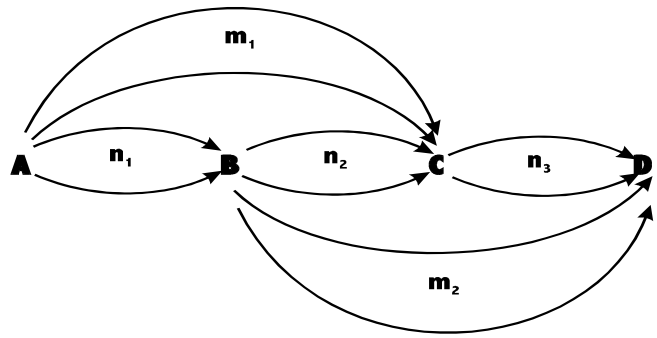
Final Examination Solutions

1. a [5] Consider this directed multigraph having n_1 edges from vertex A to vertex B, n_2 edges from vertex B to vertex C, etc. . How many different paths are there from vertex A to vertex D*?*



Paths from vertex A to vertex D either pass through vertices B and C, B but not C, or C but not B. There are $n_1 n_2 n_3$ paths passing through vertices B and C, $n_1 m_2$ paths passing through vertex B but not C, and $m_1 n_3$ paths passing through vertex C but not B. The total is $n_1 n_2 n_3 + n_1 m_2 + m_1 n_3$ paths from vertex A to vertex D

b [5] Given that the length of any shortest path along gridlines from *(0,0)* to *(m, n)* is *m+n,* how many such shortest length paths are there. ?

A shortest path from *(0,0)* to *(m, n)* has exactly m steps in which the first coordinate increases by one and exactly n steps in which the second coordinate increases by one. There are $\binom{m+n}{m}$ ways to insert the m steps in which the first coordinate increases by one into the sequence of $m+n$ steps, thus there are $\binom{m+n}{m}$ such paths.

2. [10] For $n \geq 1$, consider sequences on length *n* composed of *a*'s, *b*'s, *c*'s, *d*'s and *e*'s. How many of the sequences are in alphabetical order (i.e., all *a*'s precede all *b*'s, all *b*'s precede all *c*'s, …, etc.)?

Consider a string of n dots and four bars. There are $\binom{n+4}{4}$ such strings. If we replace all dots prior to the first bar with *a*'s, all dots between the first bar and the second bar with *b*'s, all dots between the second bar and the third bar with *c*'s, all dots between the third bar and the fourth bar with *d*'s and all dots following the fourth bar with *e*'s, we obtain exactly the set of all alphabetized sequences. Thus, there are $\binom{n+4}{4}$ such sequences..

3. a. [10] Using a combinatorial argument, prove that for $n \geq 2$ and $m \geq 2$:

$$\binom{n+m}{2} = n \cdot m + \binom{n}{2} + \binom{m}{2}$$

Let A and B be disjoint sets of cardinalities n and m, respectively. We seek to determine how many subsets of two elements there are in $A \cup B$. Since the cardinality of $A \cup B$ is $n+m$, there are $\binom{n+m}{2}$ such subsets. Alternatively, we could obtain such a subset by selecting one element from each of A and B, by selecting both elements from A, or by selecting both elements from B. There are $nm + \binom{n}{2} + \binom{m}{2}$ ways of doing this and, therefore $\binom{n+m}{2} = nm + \binom{n}{2} + \binom{m}{2}$.

b. [10] Using a combinatorial argument, prove that for integers $m, n, p \geq 1$:

$$(n+m)^p = \sum_{k=0}^{p} \binom{p}{k} n^k \, m^{p-k}$$

Let A and B be disjoint sets of cardinalities n and m, respectively. We seek to determine how many strings of length p there are consisting of elements of $A \cup B$. Since the cardinality of $A \cup B$ is $n+m$, there are $n+m$ options for each of p positions in the sequence, so there are $(n+m)^p$ such sequences. Alternatively, let k denote the number of positions in the sequence occupied by elements of A. The value of k varies from 0 to p. For a fixed value of k, there are $\binom{p}{k}$ ways to select these positions and then n options for each of the k positions. For each of the

$p-k$ positions occupied by elements of B, there are m options, thus $\binom{p}{k} n^k m^{p-k}$ for the fixed value of k and $\sum_{k=0}^{p} \binom{p}{k} n^k m^{p-k}$ overall. This must equal $(n+m)^p$.

4. a. [10] For $n \geq 5$, consider strings of length n using elements of $\{a,b,c\}$. Assume all such strings are equally likely. What is the probability that a string has at least one a?

There are 3^n strings of length n using elements of $\{a,b,c\}$ and 2^n strings of length n using elements of $\{b,c\}$, therefore there are $3^n - 2^n$ such strings with at lest one a. The probability of such a string is $\frac{3^n - 2^n}{3^n}$.

b. [5] What is the probability that such a string has at least one b given that it has at least one a?

If a string fails to have at least one b and at least one a, then it either has no b at all or no a at all. There are 2^n stings with no b at all, the same number of strings with no a at all, and one string with neither. Thus there are $2^{n+1} - 1$ strings either having no b at all or no a at all. Complementing this, we have $3^n - 2^{n+1} + 1$ strings having at least one b and at least one a. The probability of such a string is $\frac{3^n - 2^{n+1} + 1}{3^n}$ and probability that such a string has at least one b given that it has at least one a is $\frac{3^n - 2^{n+1} + 1}{3^n - 2^n}$.

5. [10] Using definition 2' (and no cardinality theorems) prove that $\mathrm{N} \times \mathrm{N}$, the set of ordered pairs of natural numbers, is infinite.

Consider the mapping $f : \mathrm{N} \times \mathrm{N} \to \mathrm{N} \times \mathrm{N}$ defined by $f(i,j) = (i+1, j)$. If $(i,j) \in \mathrm{N} \times \mathrm{N}$ then $(i+1, j) \in \mathrm{N} \times \mathrm{N}$. For $(i_1, j_1) \in \mathrm{N} \times \mathrm{N}$ and $(i_2, j_2) \in \mathrm{N} \times \mathrm{N}$ with $(i_1, j_1) \neq (i_2, j_2)$ then either $i_1 \neq i_2$ or $j_1 \neq j_2$ and thus either $i_1 + 1 \neq i_2 + 1$ or $j_1 \neq j_2$. In either case $f(i_1, j_1) = (i_1 + 1, j_1) \neq (i_2 + 1, j_2) = f(i_2, j_2)$, so f is one-to-one. However, for no element $(i,j) \in \mathrm{N} \times \mathrm{N}$ is $f(i,j) = (0,0)$ since that would imply that $i = -1$. We conclude that f maps $\mathrm{N} \times \mathrm{N}$ one-to-one into a proper subsets of itself, and thus is infinite.

6. a. [10] Let A be a nonempty set. Prove that $\mathcal{P}(A)$, the power set of A, cannot be put into one-to-one correspondence with A (i.e., there exists no function $f : A \xrightarrow[onto]{1-1} \mathcal{P}(A)$). (Hint you may want to employ the set $C = \{a \mid a \subseteq A \text{ and } a \notin f(a)\}$.)

Suppose there exists no function $f : A \xrightarrow[onto]{1-1} \mathcal{P}(A)$. Let $C = \{a \mid a \subseteq A \text{ and } a \notin f(a)\}$ and notice that $C \subseteq A$ so $C \in \mathcal{P}(A)$. Since f is onto there exists some $\bar{a} \in A$ so that $f(\bar{a}) = C$. We must then either have that $\bar{a} \in C$ or $\bar{a} \notin C$. If $\bar{a} \in C$ we have a contradiction since $\bar{a} \in C$ implies that $\bar{a} \notin f(\bar{a}) = C$. But if $\bar{a} \notin C$ we also have a contradiction since in that case $\bar{a} \in f(\bar{a}) = C$. Since both assuming that $\bar{a} \in C$ and $\bar{a} \notin C$ result in contradictions, we conclude that no function $f : A \xrightarrow[onto]{1-1} \mathcal{P}(A)$.

b. [5] Use the above result to conclude that for any nonempty set A, its power set cannot be countably infinite.

Suppose there was a set A such that $\mathcal{P}(A)$ were countably infinite. A could not be finite since then $\#(\mathcal{P}(A)) = 2^{\#A}$ and so $\mathcal{P}(A)$ would be finite as well. A could not be uncountably infinite since the mapping $f : A \to \mathcal{P}(A)$ defined by $f(a) = \{a\}$ maps A one-to-one into $\mathcal{P}(A)$, so $\mathcal{P}(A)$ must be uncountably infinite. Lastly, A could not be countably infinite, since if there exists $f : \mathrm{N} \xrightarrow[onto]{1-1} A$ and $g : \mathrm{N} \xrightarrow[onto]{1-1} \mathcal{P}(A)$, we would have $g \circ f^{-1} : A \xrightarrow[onto]{1-1} \mathcal{P}(A)$ contrary to what was proved above.

7. [10] Prove that $1 + 2n + 3n^2 + 4n^3 = \mathrm{O}(n^3)$.

By Theorem 6, we have that $1 = \mathrm{O}(n^3)$, $n = \mathrm{O}(n^3)$, $n^2 = \mathrm{O}(n^3)$, and $n^3 = \mathrm{O}(n^3)$. By Theorem 1, we have that $2n = \mathrm{O}(n^3)$, $3n^2 = \mathrm{O}(n^3)$, and $4n^3 = \mathrm{O}(n^3)$. Finally, by Corollary 3.2 we have that $1 + 2n + 3n^2 + 4n^3 = \mathrm{O}(n^3)$.

8. [10] .Prove that if $f_1 = \mathrm{o}(g)$ and $f_2 = \mathrm{o}(g)$, then $f_1 + f_2 = \mathrm{o}(g)$.

Given any $\varepsilon > 0$, since $f_1 = \mathrm{o}(g_1)$ there exists an N_1 so that $n \geq N_1 \Rightarrow |f_1(n)| \leq \frac{\varepsilon}{2} |g(n)|$ and there exists an N_2 so that $n \geq N_2 \Rightarrow |f_2(n)| \leq \frac{\varepsilon}{2} |g(n)|$. Combining these, we have $n \geq \max\{N_1, N_2\} \Rightarrow |f_1(n) + f_2(n)| \leq |f_1(n)| + |f_2(n)| \leq (\frac{\varepsilon}{2} + \frac{\varepsilon}{2}) |g(n)| = \varepsilon |g(n)|$, so $f_1 + f_2 = \mathrm{o}(g)$.

9. [10] Prove the following code is correct with respect to precondition "***true***" and postcondition "$((z = w) \vee (z = x)) \wedge (z \geq w) \wedge (z \geq x)$":

```
z := w
if x > z then
    z := x
```

______________________true

z := w

______________________ $z = w$

if x > z **then**

    ________________ $(z = w) \wedge (x > z)$

    z := x

    ________________ $(z = x) \wedge (z' = w) \wedge (x > z')$

    ________________ $(z = x) \wedge (z > w)$

______________________ $((x \le z) \wedge (z = w)) \vee ((z = x) \wedge (z > w))$

______________________ $((z \le x) \wedge (z = w)) \vee ((z = x) \wedge (z \ge w))$

______________________ $((z = w) \vee (z = x)) \wedge (z \ge w) \wedge (z \ge x)$

10. a. [10] Prove the following code is partially correct with respect to precondition "$m \ge 1$ and $n \ge 1$" and postcondition "$c = \binom{m}{n}$" (assume c, m, n, and k are integer variables.):

```
c := 1
k := 1
while k≤n do
        c := (c*(m-k+1))/k
        k := k+1
endwhile
```

Be explicit about your loop invariant. (You may use the following axiom:

$$\text{for } m \ge 1 \text{ and } k \ge 1: \binom{m}{k-1} \cdot \frac{m-k+1}{k} = \binom{m}{k},$$

and you may assume that integer division of $c*(m-k+1)$ by k is done exactly. That can be easily proved but do not waste the time.)

The loop invariant is $m \ge 1 \wedge c = \binom{m}{k-1} \wedge k \le n+1$. This is the verification:

______________________ $m \ge 1 \wedge n \ge 0$

c := 1

______________________ $m \ge 1 \wedge n \ge 0 \wedge c = 1$

k := 1

______________________ $m \ge 1 \wedge n \ge 0 \wedge c = 1 \wedge k = 1$

______________________ $m \ge 1 \wedge c = \binom{m}{k-1} \wedge k \le n+1$

while k≤n **do**

    ________________ $m \ge 1 \wedge c = \binom{m}{k-1} \wedge k \le n+1 \wedge k \le n$

$\_\_\_\_\_\_\_\_\_\_ m \geq 1 \wedge c = \binom{m}{k-1} \wedge k \leq n$

c := (c*(m-k+1))/k

$\_\_\_\_\_\_\_\_\_\_ m \geq 1 \wedge c' = \binom{m}{k-1} \wedge k \leq n \wedge c = \frac{c' \cdot (m-k+1)}{k}$

$\_\_\_\_\_\_\_\_\_\_ m \geq 1 \wedge c = \binom{m}{k} \wedge k \leq n$

k := k+1

$\_\_\_\_\_\_\_\_\_\_ m \geq 1 \wedge c = \binom{m}{k'} \wedge k' \leq n \wedge k = k'+1$

$\_\_\_\_\_\_\_\_\_\_ m \geq 1 \wedge c = \binom{m}{k-1} \wedge k \leq n+1$

endwhile

$\_\_\_\_\_\_\_\_\_\_\_\_\_\_ m \geq 1 \wedge c = \binom{m}{k-1} \wedge k \leq n+1 \wedge k > n$

$\_\_\_\_\_\_\_\_\_\_\_\_\_\_ c = \binom{m}{k-1} \wedge k = n+1$

$\_\_\_\_\_\_\_\_\_\_\_\_\_\_ c = \binom{m}{n}$

…b. [5] Prove that the loop terminates.

while k≤n **do**
c := (c*(m-k+1))/k
k := k+1
$\_\_\_\_\_\_\_\_\_\_ k = k'+1$
$\_\_\_\_\_\_\_\_\_\_ n-k < n-k'$
endwhile

Therefore the value of the integer expression $n-k$ strictly decreases at each step until $n-k<0$, at which point $k>n$ and the loop terminates.

11. [10] Determine the weakest precondition with respect to the postcondition "$z \geq 6$" for the following code (assume *z*, *y*, and *x* are integer variables and that y is defined):

x := 5
z := x+y
if *y>0* **then**
z := 3+x
else
z := 3*z
endif

$wp($**if** y>0 **then** z := 3+x **else** z := 3*z **endif**$, z \geq 6)$
$= (y > 0 \Rightarrow wp($z := 3+x$, z \geq 6)) \wedge (y \leq 0 \Rightarrow wp($z := 3*z$, z \geq 6))$
$= (y > 0 \Rightarrow 3 + x \geq 6) \wedge (y \leq 0 \Rightarrow \ 3z \geq 6)$
$= (y > 0 \Rightarrow x \geq 3) \wedge (y \leq 0 \Rightarrow \ z \geq 2)$
$= (y \leq 0 \vee x \geq 3) \wedge (y > 0 \vee \ z \geq 2).$
$wp($z:=x+y$, (y \leq 0 \vee x \geq 3) \wedge (y > 0 \vee \ z \geq 2))$
$= (y \leq 0 \vee x \geq 3) \wedge (y > 0 \vee \ x + y \geq 2).$
$wp($x:=5$, (y \leq 0 \vee x \geq 3) \wedge (y > 0 \vee \ x + y \geq 2))$
$= (y \leq 0 \vee 5 \geq 3) \wedge (y > 0 \vee \ 5 + y \geq 2)$
$= (y \leq 0 \vee true) \wedge (y > 0 \vee \ y \geq -3)$
$= true \wedge \ (y \geq -3)$
$= \ (y \geq -3).$
Therefore,
$wp($x:=5;z:=x+y;**if** y>0 **then** z := 3+x **else** z := 3*z **endif**$, z \geq 6) = (y \geq -3)$

12. [10] Prove that the weakest precondition with respect to the postcondition “ $post(c)$ ” for the following code

b : = 1
c := $\exp_1(a,b)$
if $test(a,b,c)$ **then**
  c := $\exp_2(a,b,c)$
else
  c := $\exp_3(a,b,c)$
endif

is:
$(test(a,1,exp_1(a,1)) \wedge post(exp_2(a,1,exp_1(a,1)))) \vee (\neg test(a,1,exp_1(a,1)) \wedge post(exp_3(a,1,exp_1(a,1))))$

(Hint: You may want to use the logical identity:
$((p \Rightarrow r) \wedge (\neg p \Rightarrow q)) \equiv ((p \wedge r) \vee (\neg p \wedge q))$

$$wp(\textbf{if } test(a,b,c) \textbf{ then } \text{c:} = exp_2(a,b,c) \textbf{ else } \text{c:} = exp_3(a,b,c) \textbf{ endif}, post(c))$$
$$= (test(a,b,c) \Rightarrow wp(\text{c:} = exp_2(a,b,c), post(c)) \wedge (\neg test(a,b,c) \Rightarrow wp(\text{c:} = exp_3(a,b,c), post(c))$$
$$= (test(a,b,c) \Rightarrow post(exp_2(a,b,c)) \wedge (\neg test(a,b,c) \Rightarrow post(exp_3(a,b,c))$$
$$= (test(a,b,c) \wedge post(exp_2(a,b,c)) \vee (\neg test(a,b,c) \wedge post(exp_3(a,b,c))$$
$$wp(\text{c:=}exp_1(a,b),(test(a,b,c) \wedge post(exp_2(a,b,c))) \vee (\neg test(a,b,c) \wedge post(exp_3(a,b,c))))$$
$$= (test(a,b,exp_1(a,b)) \wedge post(exp_2(a,b,exp_1(a,b)))) \vee (\neg test(a,b,exp_1(a,b)) \wedge post(exp_3(a,b,exp_1(a,b))))$$
$$wp(\text{b:=}1,(test(a,b,exp_1(a,b)) \wedge post(exp_2(a,b,exp_1(a,b)))) \vee (\neg test(a,b,exp_1(a,b)) \wedge post(exp_3(a,b,exp_1(a,b)))))$$
$$= (test(a,1,\text{exp}_1(a,1)) \wedge post(exp_2(a,1,\text{exp}_1(a,1)))) \vee (\neg test(a,1,\text{exp}_1(a,1)) \wedge post(exp_3(a,1,\text{exp}_1(a,1))))$$

Thus,

$$wp(\text{b:=1;c:=}exp_1(a,b); \textbf{if } test(a,b,c) \textbf{ then } \text{c:} = exp_2(a,b,c) \textbf{ else } \text{c:} = exp_3(a,b,c) \textbf{ endif}, post(c))$$
$$= (test(a,1,\text{exp}_1(a,1)) \wedge post(exp_2(a,1,\text{exp}_1(a,1)))) \vee (\neg test(a,1,\text{exp}_1(a,1)) \wedge post(exp_3(a,1,\text{exp}_1(a,1))))$$