CSE 20: Sample Final

November 29, 2005

Name: _____

Student ID:_____

No books or calculators are allowed. One double-sided 8.5x11 page of handwritten notes is allowed. If you need to make an assumption to solve a problem, state the assumption.

1. *8 pts.* We intend to prove that, for all integers $k \geq 1$,

$$\sqrt{k} \leq \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{k}}.$$

It is clearly true for $k = 1$. Assume the Induction Hypothesis (IH) that $\sqrt{n} \leq \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}}$. What is a correct way of concluding this proof by induction?

(a) By IH, $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n+1}} \geq \sqrt{n} + \frac{1}{\sqrt{n}} \geq \frac{\sqrt{n}\sqrt{n}+1}{\sqrt{n}} \geq \frac{n+1}{\sqrt{n+1}} = \sqrt{n+1}$.

(b) By IH, $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n+1}} \geq \sqrt{n} + \frac{1}{\sqrt{n+1}} = \frac{\sqrt{n}\sqrt{n+1}+1}{\sqrt{n+1}} \geq \frac{\sqrt{n}\sqrt{n}+1}{\sqrt{n+1}} = \frac{n+1}{\sqrt{n+1}} = \sqrt{n+1}$.

(c) By IH, $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n+1}} \geq \sqrt{n} + \frac{1}{\sqrt{n+1}} = \sqrt{n+1} + 1 \geq \sqrt{n+1}$.

(d) By IH, $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n+1}} \geq \sqrt{n+1} + \frac{1}{\sqrt{n+1}} \geq \sqrt{n+1}$.

(e) By IH, $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n+1}} \geq \sqrt{n} + 1 \geq \sqrt{n+1}$.

Solution: (a) is incorrect because the first inequality loses the $\frac{1}{n+1}$ term.

(b) is correct. The first inequality is due to the inductive hypothesis. Successive operations are algebraically correct. The final result shows the needed inequality.

(c) is incorrect because the equality is incorrect.

(d) is incorrect because the first inequality incorrectly utilizes the inductive hypothesis (the $\sqrt{n+1}$ should be a $\sqrt{n}$).

(e) is incorrect because it assumes what is to be proven (*begging the question*) in the first inequality.

2. Show that in any set of n integers, $n \geq 3$, there always exists a pair of numbers whose difference is divisible by $n-1$.

Solution: Consider the mapping $f(a) = a \bmod (n-1)$. Since f maps from a set of size n to a set of size $n-1$, by the pigeonhole principle, at least two items in the domain map to the same item in the codomain.

If any two integers i, j have the same mapping, then:

$$\begin{aligned} f(i) &= f(j) \\ i \bmod (n-1) &= j \bmod (n-1) \\ i - j &= 0 \bmod (n-1) \\ &\rightarrow (n-1) | (i-j) \end{aligned}$$

Thus, in any set of n integers, there are at least two integers whose difference is divisible by $n-1$.

3. Let $A = \{1,2,3,4,5\}$ and define a binary relation R on A as follows:

   $R = \{(1,1),(2,2),(3,3),(4,4),(5,5),(1,4),(4,1),(1,5),(5,1),(4,5),(5,4),(2,3),(3,2)\}$

   What are the distinct equivalence classes of B?

   Solution: The distinct equivalence classes of B are: $\{\{1,4,5\},\{2,3\}\}$.

4. Let A be the set of all straight lines in the Cartesian plane. Define a relation $\perp$ on A as follows:
   For all l_1 and l_2 in A, $l_1 \perp l_2$ iff l_1 is perpendicular to l_2.

   Is $\perp$ an equivalence relation? Prove or disprove.

   Solution:

   Reflexive: l_1 is not $\perp l_1$. No.

   Symmetric: $l_1 \perp l_2 \rightarrow l_2 \perp l_1$. Yes.

   Transitive: If $l_1 \perp l_2$ and $l_2 \perp l_3$, then $l_1 \parallel l_2$. No.

   Thus, $\perp$ is *not* an equivalence relation.

5. *5 pts.* Assume that R is a binary relation defined on a set A. Which of the following are correct *(circle all correct answers)*:

   (a) R is a partial order relation on A if, and only if, R is reflexive, symmetric, and transitive.

   (b) If R is an equivalence relation on A, then R is reflexive and transitive.

   (c) In order for R to be a total order relation on A, it is necessary that R be a partial order relation on A.

   (d) If R is a partial order relation on A, then each pair of elements is comparable.

   (e) if A is the empty set, then R is a total order relation on A.

   Solution: (a) is incorrect, in order to have a partial order relation, R must be *anti*-symmetric.

   (b) is correct, if R is an equivalence relation, then it is reflexive and transitive. It is, of course, also symmetric as well.

   (c) is correct. A total order relation is a partial order relation with an additional condition.

   (d) is incorrect. Total order relations require that each pair of elements is comparable.

   (e) is correct. Since A is empty, R is empty as well. Trivially, it is reflexive, transitive, anti-symmetric, and each pair of elements is comparable.

6. Note: the overflow bit is sometimes called the carry-out bit. A twos-complement signed addition of $c = a + b$ overflows if, and only if *(circle one)*:

   (a) the addition causes the overflow bit to be set,

   (b) the addition causes the overflow bit to be set and the sign bit of c is set,

(c) the sign bits of a and b are equal, but don't match the sign bit of c,

(d) the addition causes the overflow bit to be set and the sign bits of a and b are equal.

Solution: (a) is incorrect. For example, $-1 + -1$ causes the overflow bit to be set, but doesn't overflow (since $c = -2$).

(b) is incorrect. For example, if a is the maximum value, and b is 1, then, adding them will overflow, resulting in a negative number, but the overflow bit won't be set.

(c) is correct. Adding a positive and negative number can't result in overflow. The only overflow is if adding two positives results in a negative or vice-versa.

(d) is incorrect. See reasoning in (b).

7. Let S be the set of composite integers n, $4 \leq n \leq 20$. Order S with the divides relation. Let $x_1, x_2, \ldots, x_{11}$ be a topological sort of this poset. A pair (i, j) where $i < j$ and the integer x_i is smaller than the integer x_j will be called an "in-order pair." Find a topological sort where the number of in-order pairs is less than or equal to 26.

   Hint: First draw the Hasse diagram.

   Solution: Here's a topological sort that meets the condition. It's found by always choosing the *largest* minimal element from the set:

   $$10, 20, 15, 9, 6, 18, 14, 4, 12, 8, 16$$

   There are 22 in-order pairs: (10, 20), (10, 18), (10, 14), (10, 12), (10, 16), (15, 18), (15, 16), (9, 18), (9, 14), (9, 12), (9, 16), (6, 18), (6, 14), (6, 12), (6, 8), (6, 16), (14, 16), (4, 12), (4, 8), (4, 16), (12, 16), (8, 16)

8. Which grows faster, $2n^{.01} + 3n - 1$, or $\ln n$? Prove.

   Solution:

   Let's consider $\lim_{n\to\infty} \frac{\ln n}{2n^{.01}+3n-1}$. If that converges to 0, then the denominator grows faster than the numerator.

   The limit of the numerator and the denominator both diverge to ∞, so L'Hopital's rule can be used. Let's consider the limit of the derivative

of the numerator divided by the derivative of the denominator

$$\begin{aligned}
&\lim_{n\to\infty} \frac{\frac{1}{n}}{.02n^{-.99}+3} \\
&\qquad = \lim_{n\to\infty} \frac{1}{n(.02n^{-.99}+3)} \\
&\qquad = \lim_{n\to\infty} \frac{1}{.02n^{.01}+3n} \\
&\qquad = 0
\end{aligned}$$

9. *8 pts.* Given any function, f, which of the following are true about the domain, codomain, image, and coimage of f *(circle one)*?

   (a)

   $$\begin{aligned} |\text{Coimage}(f)| &\leq |\text{Image}(f)| \\ \text{Image}(f) &\subseteq \text{Codomain}(f) \\ |\text{Coimage}(f)| &\leq |\text{Domain}(f)| \end{aligned}$$

   (b)

   $$\begin{aligned} |\text{Coimage}(f)| &= |\text{Image}(f)| \\ \text{Coimage}(f) &\subseteq \text{Domain}(f) \\ |\text{Image}(f)| &\leq |\text{Codomain}(f)| \end{aligned}$$

   (c)

   $$\begin{aligned} |\text{Coimage}(f)| &\geq |\text{Image}(f)| \\ \text{Coimage}(f) &\subseteq \text{Domain}(f) \\ |\text{Image}(f)| &\leq |\text{Codomain}(f)| \end{aligned}$$

   (d)

   $$\begin{aligned} |\text{Coimage}(f)| &= |\text{Image}(f)| \\ \text{Image}(f) &\subseteq \text{Domain}(f) \\ |\text{Codomain}(f)| &\leq |\text{Coimage}(f)| \end{aligned}$$

   Solution:

   (a) is correct. The first part is less exact than it could be, since the size of the coimage is equal to the size of the image.

   (b) is incorrect because the coimage is not a subset of the domain (it is a *partition* of the domain).

   (c) is incorrect for the same reason as (b).

   (d) is incorrect because the size of the codomain is greater than or equal to the size of the coimage.

10. Give a closed form for the following sum.

    $$S_n = \sum_{0 \leq k \leq n} \frac{1}{x^{k-n}}$$

Solution:

$$
\begin{aligned}
S_n &= \sum_{0 \le k \le n} \frac{1}{x^{k-n}} \\
&= \sum_{0 \le k \le n}^{n} x^{n-k} \\
&= \sum_{0 \le k \le n}^{n} x^{n} \qquad \text{Since } k \text{ and } n-k \text{ take on the same values, albeit in a different order} \\
&= \begin{cases} n+1 & \text{if } x = 1 \\ \frac{x^{k+1}-1}{x-1} & \text{if } x \neq 1 \end{cases} \text{ Geometric Series}
\end{aligned}
$$

For what values of x, if any, does $\lim_{n\to\infty} S_n$converge?

Solution: If $x > 1$, the numerator grows faster than the denominator, and thus the series diverges.

If $x \le -1$, we have an alternating series of positive and negative terms. Inspection shows that the negative terms diverge to infinity, as do the positive terms. Thus, the value is undefined.

If $x = 1$, $n+1$ diverges to infinity.

If $0 \le x < 1$, the closed formula converges to $\frac{1}{1-x}$.

If $-1 < x < 0$, although x^{k+1} alternates between positive and negative, each term in the series is positive. However, the numerator gets closer and closer to 1. Thus, the total series converges to $\frac{1}{1-x}$.

In summary, if $-1 < x < 1$, then the series converges.

11. Circle all of the following that are correct.

    (a) In order to prove $p \leftrightarrow q$, it is sufficient to prove $p \to q$ and $p \leftarrow q$.

    (b) In order to prove $p \leftrightarrow q$, it is sufficient to prove $p \to q$ and $\sim p \to \sim q$.

    (c) The contrapositive of $p \to q$ is $\sim q \to \sim p$.

    (d) The inverse of $p \to q$ is $q \to p$.

    (e) The converse of $p \to q$ is $\sim p \to \sim q$.

    Solution: (a) is correct. We prove from left-to-right, and then from right-to-left.

    (b) is correct. If p is true, q will be true, and if p is false, q will be false. Alternatively, the second part is just the contrapositive of the second part of (a).

    (c) is correct.

    (d) is incorrect. The inverse of $p \to q$ is $\sim p \to \sim q$.

    (e) is incorrect. The converse of $p \to q$ is $q \to p$.

12. Which of the following is a description of the RSA protocol *(circle one)*

    (a) Alice chooses two large primes d (her private key) and e (her public key) and computes $N = de$. Bob encrypts a message M to Alice by computing $C = M^e \bmod N$. Alice decrypts C by computing $C^d \bmod N$.

    (b) Alice choose two large primes p and q and computes $N = pq$. She chooses d (her private key) and e (her public key) such that $de = 1 \bmod \phi(N)$. Bob encrypts a message M ($\gcd(M,N) = 1$) to Alice by computing $C = M^e \bmod N$. Alice decrypts C by computing $C^d \bmod N$.

    (c) Given p and b, Alice chooses a random number $1 < s < p-1$, and Bob chooses a random number $1 < t < p-1$. Alice computes $S = b^s \bmod p$ and sends S to Bob. Bob computes $T = b^t \bmod p$ and sends T to Alice. Alice computes the shared key $K = T^s \bmod p$. Bob computes the shared key $K = S^t \bmod p$. Alice and Bob now encrypt future traffic using the shared secret key K.

    Solution: (a) is incorrect.

    (b) is correct. Let's look at the decryption: $C^d = (M^e)^d = M^{ed} \pmod N$. But, $de = 1 \bmod \phi(N)$, so $M^{ed} = M^{1+k\phi(N)} = M \times (M^{\phi(N)})^k$. However, since $\gcd(M,N) = 1$, M is a unit of N, and so $M^{\phi(N)} = 1 \pmod N$. This leads to $M^{ed} = M$.

    (c) is incorrect. This is an explanation of the Diffie-Hellman symmetric key exchange protocol.