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, $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n+1}} \geq \sqrt{n} + 1 \geq \sqrt{n+1}$.

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

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?

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.

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.

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.

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.

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

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)

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

10. Give a closed form for the following sum.

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

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

11. Circle all of the following that are correct.

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

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

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

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

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

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.