CS 103X: Discrete Structures
Midterm

February 7, 2008

THE STANFORD UNIVERSITY HONOR CODE

- The Honor Code is an undertaking of the students, individually and collectively:
  - that they will not give or receive aid in examinations; that they will not give or receive unpermitted aid in class work, in the preparation of reports, or in any other work that is to be used by the instructor as the basis of grading;
  - that they will do their share and take an active part in seeing to it that others as well as themselves uphold the spirit and letter of the Honor Code.
- The faculty on its part manifests its confidence in the honor of its students by refraining from proctoring examinations and from taking unusual and unreasonable precautions to prevent the forms of dishonesty mentioned above. The faculty will also avoid as far as practicable, academic procedures that create temptations to violate the Honor Code.
- While the faculty alone has the right and obligation to set academic requirements, the students and faculty will work together to create optimal conditions for honorable academic work.

Exams are to be done individually and must represent original work—it is a violation of the honor code to copy or derive exam question solutions from other students or anyone at all, textbooks, or previous instances of this course.

I acknowledge and accept the honor code:

Signature: ____

Name (print): ____

EXAM RULES

- You have two hours to complete this exam.
- Do not include your scratch work with your exam. Please work the solutions out on another sheet of paper and then write your solutions neatly on the exam.
- You may use Prof. Koltun's lecture notes (Chapters 1 through 7) and one double-sided cheat-sheet. You may *not* use any other material, such as your own course notes, homeworks, distributed homework solutions, other sets of lecture notes, books, computers, cell phones, crystal balls, Tarot cards, etc.
- Write clearly and neatly.
- Stagger your seats.

GOOD LUCK!

Exercise 1 (20 points). Prove or disprove:

(a) If a and b are irrational, so is $a + b$.

Solution. False. Consider $a = \sqrt{2}$, $b = -\sqrt{2}$.

(b) If a and b are two coprime integers and c is an integer, the *linear Diophantine equation*

$$ax + by = c$$

always has an integer solution x, y.

Solution. True. By Bezout's theorem, for some choice of integers s and t

$$sx + ty = 1$$

$$\Rightarrow csx + cty = c$$

$$\Rightarrow ax + by = c$$

by setting $a = cs$ and $b = ct$.

(c) If R and S are equivalence relations on A,

$$R \cap S$$

is also an equivalence relation on A.

(d) For a function $f : X \to Y$,

$$f(A \cap B) = f(A) \cap f(B)$$

for any $A, B \subseteq X$.

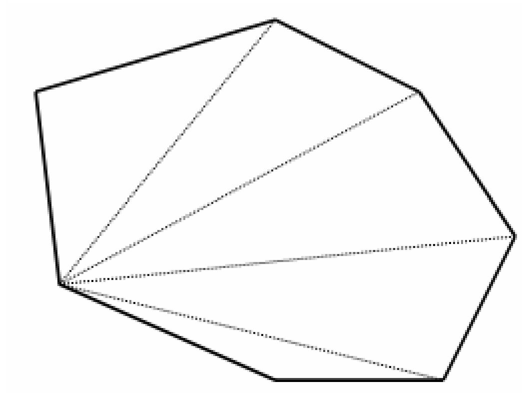
Solution. False. Let $f(n) = n^2$. Then consider $A = \{1\}$, $B = \{-1\}$.

$$\Rightarrow f(A) = \{1\} \text{ and } f(B) = \{1\} \Rightarrow f(A) \cap f(B) = \{1\}$$

$$\text{However, } A \cap B = \emptyset \Rightarrow f(A \cap B) = \emptyset$$

Exercise 2 (20 points)**.** A *diagonal* of a polygon is a straight line joining two non-adjacent vertices of the polygon. A *convex* polygon is a polygon such that any diagonal lies in its interior. What is the maximum number of non-intersecting diagonals that may be drawn in a convex polygon with n vertices? Prove.

Here is an example of such a maximal set of non-intersecting diagonals for a convex polygon with 7 vertices:



Solution.
Claim: $n-3$ is maximal non-intersection diagonals for polygons having $n \geq 3$ vertices. Proof by strong induction:
Base case: $n = 3$. Every vertex in a triangle does not have non-adjacent vertices (the are all adjacent to each other). Therefore, there is $n - 3 = 3 - 3 = 0$ diagonals.
Induction hypothesis: Let us assume that the claim holds true for $n = 3, 4, 5, \ldots, k$. We now need to show that the claim holds for $n = k + 1$.
Proof for $n = k + 1$. Draw any diagonal in our $k + 1$-gon. This separates the polygon into a m-gon and a $k + 1 - m + 2$-gon, with $m \leq k$ since at least 1 of the original vertices lives in the other polygon. Notice also that $k+1-m+2 \leq k$ since $m \geq 3$ since m represents the number of vertices in another polygon. Also note that there can be no diagonals from the m-gon to the $k + 1 - m + 2$-gon since they are separated by a diagonal. Now by the induction hypothesis, our m-gon has $m - 3$ diagonals, and our $k + 1 - m + 2$ has $k+1-m+2-3$ diagonals, which brings us to a grand total of $m-3+k+1-m+2-3 = (k+1)-4$ diagonals. However, we also have the original diagonal that we had used to separate into these two polygons, so we have a total of $(k + 1) - 3$ diagonals in the entire $k + 1$-gon.

Exercise 3 (20 points)**.** Given distinct primes p and q, prove:

(a) $\sqrt{pq}$ is irrational.

(b) $\sqrt{p/q}$ is irrational.

Solution.

(a) We will prove that $\sqrt{pq}$ is irrational by contradiction.

Assume that $\sqrt{pq}$ is rational $\Rightarrow \sqrt{pq} = \frac{a}{b}$ where $a,b \in \mathbb{Z}$ and a,b co-prime. Therefore, $b^2pq = a^2$. Since a and b co-prime $\Rightarrow$ a and b do not share any factors, $pq|a^2$, and more specifically, $p|a^2$. Since p is prime, $p|a$. We can rewrite $a = kp$ for some $k \in \mathbb{Z}$. Thus, $b^2pq = k^2p^2 \Rightarrow b^2q = k^2p$. Since p and q are co-prime (since they are primes), $p|b^2$, and since p is prime, $p|b$. This means that a and b share the common factor p. This is a contradiction $\Rightarrow \sqrt{pq}$ irrational.

(b) We will prove that $\sqrt{p/q}$ is irrational by contradiction.

Assume that $\sqrt{p/q}$ is rational $\Rightarrow \sqrt{p/q} = \frac{a}{b}$ where $a,b \in \mathbb{Z}$ and a,b co-prime. Therefore, $b^2p = a^2q$. Since p and q are primes, they are co-prime. This means that $p|a^2$. Since p is prime, this also means $p|a$. We can rewrite $a = kp$ for some $k \in \mathbb{Z}$. Thus, $b^2p = k^2p^2q \Rightarrow b^2 = k^2pq$. This implies that $p|b^2$ and consequently since p is prime, $p|b$. a and b share the common factor p. This is a contradiction $\Rightarrow \sqrt{p/q}$ irrational.

Exercise 4 (20 points)**.** Let

$$S_k = \sum_{i=1}^{p-1} i^k$$

where p is prime and k is a positive multiple of $p-1$. Use Fermats Little Theorem to prove that $S_k \equiv_p -1$.

Solution. Fermats little theorem says that $x^{p-1} \equiv_p 1$ when $1 \leq x \leq p-1$. Since k is a multiple of $p-1$, raising each side to a suitable power proves that $x^k \equiv_p 1$. Thus:

$$1^k + 2^k + ... + (p-1)^k \equiv_p 1 + 1 + ... + 1 \quad (p-1 \text{ terms})$$

$$\equiv_p p - 1$$

$$\equiv_p -1$$

Exercise 5 (20 points)**.** Show that if p, q, and r are distinct primes, there exist integers a, $b$and c, such that

$$a(pq) + b(qr) + c(rp) = 1$$

Solution. Since $gcd(pq, qr) = q$, there exist integers s and t such that:

$$s(pq) + t(qr) = q$$

Now $gcd(q, rp) = 1$, so there exist integers u and v such that:

$$uq + v(rp) = 1$$

Therefore:

$$u(s(pq) + t(qr)) + v(rp) = (us)(pq) + (ut)(qr) + v(rp) = 1$$