Spring, 2004 CIS 511

Introduction to the Theory of Computation

Warm-up Homework

January 6, 2004

These problems do not have to be turned in, but I **urge** you to solve as many as you can! The goal of this homework is to give you some practice with proof techniques, especially induction. You will also have the opportunity to review elementary properties of graphs and trees.

Problem B1 (20 pts). For any natural number $n \geq 0$, prove that

$$1 + 3 + 5 + \cdots + 2n + 1 = \sum_{k=0}^{n} (2k + 1) = (n + 1)^2.$$

Prove that

$$\sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k \right)^2.$$

Problem B2 (40 pts). Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ denote the set of natural numbers. Given any set S, a *finite multiset M over S* is any function $M\colon S \to \mathbb{N}$ such that $M(a) \neq 0$ only for finitely many $a \in S$. If $M(a) = k > 0$, we say that *a appears with mutiplicity k in M*. For example, if $S = \{a, b, c\}$, we may use the notation $\{a, a, a, b, c, c\}$ for the multiset where a has multiplicity 3, b has multiplicity 1, and c has multiplicity 2. The *cardinality* $|M|$ of a (finite) multiset is the number

$$|M| = \sum_{a \in S} M(a).$$

Note that this is well-defined since $M(a) = 0$ for all but finitely many $a \in S$. For example

$$|\{a, a, a, b, c, c\}| = 6.$$

Assume that S has $n \geq 1$ elements. Recall that

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

(a) Prove that the number $A(m, n)$ of multisets of cardinality m over S is

$$A(m, n) = \binom{m + n - 1}{m}.$$

Hint. This has to do with the number of multisets $\{j_1, \ldots, j_n\}$ of natural numbers j_k such that $j_1 + \cdots + j_n = m$.

(b) Let $B(m, n)$ be the number of multisets over S of cardinality at most m. Prove that

$$A(m, n) = B(m, n - 1),$$

and that

$$B(m, n) = B(m, n - 1) + B(m - 1, n).$$

Conclude that

$$B(m, n) = \binom{m + n}{m}.$$

What's the connection with the number of monomials $X_1^{j_1} \cdots X_n^{j_n}$ of total degree m in n variables and the number of monomials $X_1^{j_1} \cdots X_n^{j_n}$ of total degree at most m?

Problem B3 (40 pts). Let $n \geq 1$ be any natural number. Prove that any subset S of $\{1, 2, \ldots, 2n\}$ consisting of $n + 1$ elements contains two (distinct) numbers p, q such that p divides q.

Problem B4 (50 pts). A *graph (undirected)* is a pair $G = (V, E)$, where V is a set of *nodes* (or *vertices*), and E is a set of two-element subsets $e = \{u, v\} \subseteq V$ (where $u \neq v$) called *edges*. We say that a node v *belongs to an edge* e if $v \in e$, i.e., e is of the form $e = \{v, w\}$ for some $w \in V$. An *endpoint* is a node that belongs to a single edge. A graph is finite if V is finite.

Prove that a graph with n nodes has at most $n(n - 1)/2$ edges.

Given any two nodes $v_0, v_n \in V$, a *path from* v_0 *to* v_n is a sequence $(e_1, e_2, \ldots, e_n)$ of edges $e_i \in E$ such that $v_0 \in e_1$, $v_n \in e_n$, and $e_i \cap e_{i+1} \in V$ for all i, $1 \leq i \leq n - 1$ (where $n \geq 1$). Letting $v_i = e_i \cap e_{i+1}$, $1 \leq i \leq n - 1$, we can write the path as

$$(v_0,\, e_1,\, v_1,\, e_2,\, \ldots,\, v_{n-1},\, e_n,\, v_n),$$

where $e_i = \{v_{i-1}, v_i\}$ $(1 \leq i \leq n)$, and $e_i \neq e_{i+1}$ $(1 \leq i \leq n - 1)$.

Remarks: (1) Our definition rejects

$$(\{u, v\},\, \{u, v\})$$

as a path from u to u (or a path from v to v).

(2) Other authors, such as Harary, define a *walk* as an alternating sequence

$$(v_0,\, e_1,\, v_1,\, e_2,\, \ldots,\, v_{n-1},\, e_n,\, v_n)$$

such that $e_i = \{v_{i-1}, v_i\}$ for all i, $1 \leq i \leq n$, and reserve the terminology path to walks such that the sequence

$$(v_0, v_1, \ldots, v_n)$$

consists of $n+1$ distinct nodes. Our notion of path corresponds to walks without repeated consecutive edges (we must have $e_{i+1} \neq e_i$).

The path $(e_1, e_2, \ldots, e_n)$ from v_0 to v_n is a *cycle* if $v_0 = v_n$.

Remark: Other authors, such as Harary, use the terminology *closed walk* instead of cycle, and reserve the terminology cycle for a closed walk ($v_0 = v_n$) in which the nodes $v_0, \ldots, v_{n-1}$ are all distinct, and where $n \geq 3$.

A graph is *connected* if there is some path from u to v for every pair of distinct nodes $u, v \in V$ $(u \neq v)$. A graph is *acyclic* if it does not have any cycles.

A *tree* is a connected and acyclic graph.

Assume that T is a finite tree.

(a) Prove that if T has at least one edge, then T has at least two endpoints.

(b) Let r be any endpoint. Prove that there is a unique path from r to any other node.

(c) If T has n edges, prove that T has $n+1$ nodes.

(d) Is (a) still true if T is infinite? Are there infinite trees with no endpoints?

Now define a *directed graph* as a pair $G = (V, E)$, where V is a set of *nodes* (or *vertices*), and E is a subset $E \subseteq V \times V$ of pairs $e = (u, v)$ called *edges*. Note that the definition allows $u = v$. We define the functions $s, t \colon E \to V$ by

$$s((u, v)) = u, \quad \text{and} \quad t((u, v)) = v.$$

The definitions of a path, a cycle, a connected graph, an acyclic graph, are similar to the undirected case. In particular, given any two nodes $v_0, v_n \in V$, a *path from v_0 to v_n* is a sequence $(e_1, e_2, \ldots, e_n)$ of edges $e_i \in E$ such that $v_0 = s(e_1)$, $v_n = t(e_n)$, and $t(e_i) = s(e_{i+1})$ for all i, $1 \leq i \leq n-1$ (where $n \geq 1$).

A directed graph $G = (V, E)$ yields an undirected graph G_u as follows: $G_u = (V, E_u)$, where

$$E_u = \{\{u, v\} \mid (u, v) \in E,\ u \neq v\}.$$

(e) Show that if G is connected, then so is G_u. Is the converse true? If G_u is acyclic, is G also acyclic? Is the converse true?

(f) Is it reasonable to define a (finite) tree as a connected acyclic directed graph? Is there a reasonable definition of a tree in the directed case? (perhaps, use a "root" node, and require a unique path from the root to every other node).

Problem B5 (30 pts). It is well known that

$$cos 2\theta = 2\cos^2\theta - 1,$$

and

$$\sin 2\theta = 2\sin\theta\cos\theta.$$

Prove that

$$\cos n\theta = P_n(\cos\theta)$$

and

$$\sin n\theta = \sin\theta Q_{n-1}(\cos\theta),$$

where P_n is a polynomial of degree n of the form

$$P_n(X) = a_nX^n + a_{n-2}X^{n-2} + a_{n-4}X^{n-4} + \cdots$$

and Q_{n-1} is a polynomial of degree $n-1$ of the form

$$Q_{n-1}(X) = b_{n-1}X^{n-1} + b_{n-3}X^{n-3} + b_{n-5}X^{n-5} + \cdots.$$

Prove that

$$a_n = b_{n-1} = 2^{n-1}.$$

Problem B6 (40 pts). Let $f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n$ be a polynomial of degree $n \geq 1$ with coefficients in some commutative ring with unity, A. Note that A is **not** necessarily a field or even an integral domain; there may be zero divisors or nilpotent elements. For example, A could be $\mathbb{Z}/16\mathbb{Z}$, the ring of integers modulo 16, or a ring of matrices. Prove that if there is some nonzero polynomial, $g(X)$, so that $g(X)f(X) = 0$, then there is some nonzero scalar, $c \in A$, so that $cf(X) = 0$ (where 0 denotes the zero polynomial).