CS 173, Spring 2009
Homework 10 Solutions

(Total point value: 50 points.)

---

1. **[10 points] Paths and Circuits in Graphs**

   (a) Under what conditions does the graph $K_{m,n}$ have an Eulerian circuit? What has to be true about m and n?

   [Solution]
   m and n must both be even and greater than zero, which we can see by the theorem for Eulerian circuits from lecture (every vertex has to have even degree). Since $K_{m,n}$ is a complete bipartite graph, any vertex in the size m partition is connected to (exactly) every vertex in the size n partition. Thus n must be even. The same reasoning holds for any vertex in the n partition, so m must be even as well. This only holds if neither m nor n is zero; otherwise, there would be no edges in the graph to form a circuit from.

   (b) Under what conditions does the graph Q_n have an Eulerian circuit? What has to be true about n?

   [Solution]
   Each vertex must have even degree, so n must be even and greater than zero. Q_2 is degree 2 at each vertex and has a clear Eulerian circuit since it is isomorphic to C_4. The degree of each vertex increases by one as n increases by one, so the degree will be even exactly when n is even. Also note that Q_0 does not contain any cycles by the textbook definition (looping paths of length greater than zero, p.623), so n cannot equal zero.

   (c) Consider the complete graph K_n. Suppose we pick two vertices u and v. A path of length k between u and v is a sequence of k edges starting at u and ending at v. **Consider a path in which no vertex or edge is visited more than once.** How many different such paths of length 4 are there between u and v, assuming $n \geq 5$? Can you generalize this result and give a formula for the number of such paths of length k in K_n when $n > k$?

   [Solution]
   Since every vertex is adjacent to every other vertex, we can build a path by choosing a sequence of distinct vertices that represents four edges: u, x_1, x_2, x_3, v. Note that if we never repeat vertices, we will never reuse edges. Starting at u, there are $n-2$ possible choices for x_1. Once we visit x_1, we have $n-3$ possible choices for x_2. and then $n-4$ possible candidates for x_3. At this point, the path completes by going directly to v. Using the formula for permutations, there are $(n-2)(n-3)(n-4)$ ways to choose a path of length 4.

   We can generalize this to find the number of possible paths of length k: $(n-2)(n-3)(n-4)...(n-k+1)(n-k)$.

2. **[10 points] Graph Diameters**
   On a connected simple graph G we can measure the distance between two distinct vertices v_i and v_j as the number of edges on the shortest path between them. The *diameter* of a graph G is the maximum distance between any two distinct vertices in G.

(a) What are the diameters of the following graphs: K_n, C_n, and W_n?

[Solution]

Since every vertex has an edge to every other vertex of K_n, the diameter is 1.

The maximum distance in C_n is halfway around the circuit, which is $\lfloor \frac{n}{2} \rfloor$.

For W_n, consider any two vertices. They are either adjacent or there is a path of length 2 between them through the center. Thus the diameter is 2.

(b) Prove by induction that the diameter of the n-dimensonal hypercube Q_n is n.

[Solution]

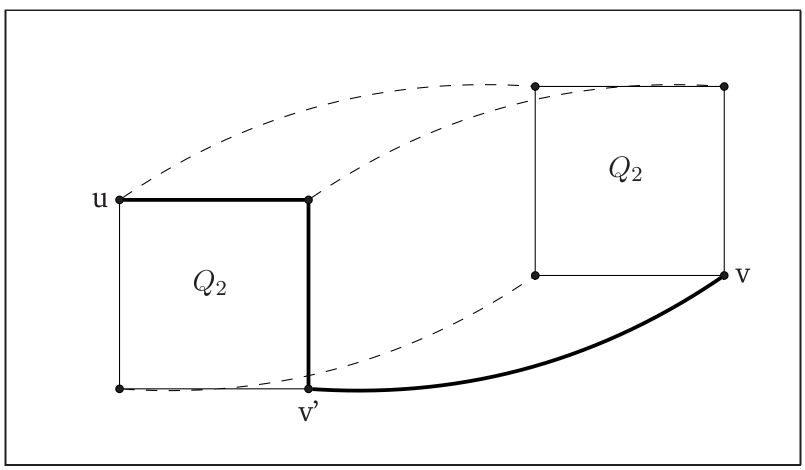
Base: Q_1 has one edge, so the diameter is 1.

Inductive step: Assume that the claim is true for the $n = k$ case: the diameter of Q_k is k. We will now show that it is true for $n = k + 1$.

In order to achieve this, we need to show that the maximum distance between all pairs of nodes is $k + 1$. Recall that Q_{k+1} is comprised of two copies of Q_k, connected at corresponding vertices. For any two u and v that we choose, there are two possibilities: either both in the same Q_k subgraph within Q_{k+1} or separated into the two Q_k subgraphs. If u and v are in the same Q_k subgraph, the distance between them is k or less by the inductive hypothesis.

If u and v are in different Q_k subgraphs, consider the vertex v' that is the corresponding copy of v in the other Q_k. By the inductive hypothesis, there is a shortest path $P_{u,v'}$ of length k or less between u and v'. We can add the edge $\{v, v'\}$ to the end of $P_{u,v'}$ to get a path $P_{u,v}$ from u to v. Note that $P_{u,v}$ is a path of length $k + 1$ or less between any u and v.

The picture below illustrates a choice of u, v', and v on Q_3. A possible $P_{u,v}$ is indicated by the bold edges.



Since distance is defined using *shortest* paths, we will now show that $P_{u,v}$ is a shortest path between u and v. We can show this by contradiction: if there was another 'shorter' path between u and v, we would be able to find a shorter path than $P_{u,v'}$ between u and v'. This is done by translating all edges of the path to the same Q_k subgraph as u,v' and removing the edges that transition between the Q_k subgraphs. Since $P_{u,v'}$ is a shortest path, this is a contradiction, so $P_{u,v}$ must also be shortest.

A remaining technicality is to show that there is at least one pair of vertices with distance $k + 1$ in Q_{k+1}. (Otherwise it could be possible that all pairs are k or less apart.) By the inductive hypothesis, there is a u and a v' that are distance k from each other. We can use the v that corresponds to v' to make a path $P_{u,v}$, which will be a shortest from u to v of length $k+1$ by the arguments above. Therefore we have found a pair of vertices that has distance $k+1$.

Thus the distance between any two vertices in Q_{k+1} is $k+1$ or less, and the diameter is $k+1$, which is what we wanted to show.

3. **[10 points] Properties of Relations**

   (a) The relation E relates intervals of the real line that abut one another. Specifically $(x,y)E(p,q)$ if and only if $y = p$ or $x = q$. E.g. $(2,3)$ and $(1.5,2)$ are related because they share the common endpoint 2. Using a specific concrete counter-example, prove that this is not an equivalence relation.

   [Solution]
   In order to be an equivalence relation, E needs to be reflexive. However, it is not reflexive, because $(1,2) \not\!E(1,2)$. Or, alternatively, it's not transitive. For example, $(1,2)E(2,3)$ and $(2,3)E(3,4)$ but it's not the case that $(1,2)E(3,4)$.

   (b) Suppose that Q is the relation on positive real numbers such that xQy if and only if $xy = 1$. Is Q reflexive, irreflexive, both, or neither? Is Q transitive? Briefly justify your answers.

   [Solution]
   Q is not reflexive, since $x \not\!Qx$ if $x = 3$. Q is not irreflexive because xQx if $x = 1$.
   Q is not transitive either. Consider $x = 2$, $y = \frac{1}{2}$, and $z = 2$: xQy and yQz but $x \not\!Qz$.

   (c) Define the relation T on the set $\mathbb{N}^3$ by saying that $(x,y,z)T(p,q,r)$ if and only if $x+y+z = p+q+r$. List three elements of $[(1,2,3)]$ and also one element of $\mathbb{N}^3$ that is not in $[(1,2,3)]$.

   [Solution]
   $(1,2,3),(2,1,3),(5,0,1) \in [(1,2,3)]$, since the sum of the coordinates is 6 for all the points.
   $(1,2,4) \notin [(1,2,3)]$, because the sums of the coordinates are different (7 vs. 6).

4. **[10 points] Proving relation properties**

   (a) Let $\ll$ be the relation on $\mathbb{Z}^2$ such that $(x,y) \ll (p,q)$ if and only if either $x < p$, or else $x = p$ and $y \leq q$. That is, when the first coordinates are different, they determine the ordering of pairs, e.g. $(0,8) \ll (1,3)$. But when the first coordinates are the same, we compare the second coordinates, e.g. $(1,3) \ll (1,8)$. Prove that $\ll$ is antisymmetric.

   [Solution]
   Using the second definition of antisymmetric from lecture 34, we need to show: $\forall (x,y),(p,q) \in \mathbb{Z}^2, (x,y) \ll (p,q)$ and $(p,q) \ll (x,y)$ implies $(x,y) = (p,q)$.
   $(x,y) \ll (p,q)$ means that either $x < p$ or both $x = p$ and $y \leq q$. Similarly, $(p,q) \ll (x,y)$ means that either $p < x$ or both $p = x$ and $q \leq y$. If both $(x,y) \ll (p,q)$ and $(p,q) \ll (x,y)$, x must equal p to be consistent between both definitions. Consequently, $y \leq q$ and $q \leq y$, so we conclude $y = q$ and $(x,y) = (p,q)$. This is what we needed to show.

   (b) Let $\sim$ be the relation on $\mathbb{Z}$ such that $x \sim y$ if and only if $4 \mid 3x + 5y$. Prove that $\sim$ is transitive.

   [Solution]
   We need to show $\forall x,y,z \in \mathbb{Z}, x \sim y$ and $y \sim z$ implies $x \sim z$.
   If $x \sim y$ and $y \sim z$, then we have $4|3x+5y$ and $4|3y+5z$. By the definition of divides, there are some $a,b \in \mathbb{Z}$ such that $4a = 3x+5y$ and $4b = 3y+5z$. Rearranging these equations, we know $3x = 4a - 5y$ and similarly $5z = 4b - 3y$.

Now consider $3x + 5z$. From our equations above, $3x + 5z = (4a - 5y) + (4b - 3y) = 4a + 4b - 8y = 4(a + b - 2y)$. Since $(a + b - 2y)$ is an integer, we have $4|3x + 5z$ and $x \sim z$, by the definitions of divides and $\sim$. Thus we've shown that $\sim$ is transitive.

5. **[10 points] A Probabilistic Algorithm**

In the last homework, we saw an algorithm to verify polynomial identities based on the binomial theorem. In this problem, we will consider a probabilistic algorithm to verify polynomial identities of the form:

$$(a_1x + a_2)^n = b_0x^n + b_1x^{n-1} + ... + b_{n-1}x^1 + b_n$$

where n is a positive integer and the a_i and b_i are non-negative integers. We will refer to the left-hand side of the identity as $G(x)$ and the right-hand side as $F(x)$, so we have $G(x) = (a_1x+a_2)^n$ and $F(x) = b_0x^n + b_1x^{n-1} + ... + b_{n-1}x^1 + b_n$

One way to verify the identity is to use an algorithm to test each coefficient generated by $G(x)$ and make sure it matches the corresponding coefficient in $F(x)$. This is similar to the algorithm on the last homework assignment and would require $\Theta(n^2)$ operations.

Another option would be to randomly pick a value for x and verify that the two sides of the equation yield the same answer. This would be a kind of probabilistic algorithm, in that it would yield the right answer when $G(x) = F(x)$ but not always give us the right answer when $G(x) \neq F(x)$. In analyzing this algorithm we need to consider both how many operations it will perform and the probability that it will give us an incorrect answer. Here is the pseudo-code for the algorithm:

procedure ProbablyVerify(x,a_1, a_2,n,b_0..., b_n)
$binomial := (a_1x) + a_2$
$g := binomial$
for $i := 2$ to n
begin
    $g := g \cdot binomial$
end
$f := 0$
$xpower := 1$
for $j := 0$ to n
begin
    $f := f + (b_{n-j} \cdot xpower)$
    $xpower := xpower \cdot x$
end
if $(g = f)$ **then**
    $matches :=$ **true**
else
    $matches :=$ **false**
return $matches$

(a) State a big-theta bound on the number of operations done by the procedure **ProbablyVerify** in terms of the degree of the polynomial which is given by the input n .

[Solution]

The first **for** loop runs $n-1$ times, so there are $\Theta(n)$ operations. The second loop runs $n+1$

times, which gives us another $\Theta(n)$ operations. The pseudocode outside of the loops (including the **if** statement) give some additional constant number of operations. All together, the number of operations will be $\Theta(n)$.

(b) The procedure will give an incorrect answer when we choose a specific value $x = c$ such that $G(c) = F(c)$, but it is **not true** that for all real numbers x that $G(x) = F(x)$. This happens when we accidentally choose a value c such that $G(c) - F(c) = 0$. In other words, we chose a value c that is a root of the polynomial equation $G(x) - F(x) = 0$. A degree n polynomial has at most n distinct roots. Given that fact, if we choose an integer x uniformly at random from the range 0 to m, for what value of m is the probability of selecting a root definitely at or below 0.01? Explain your answer.

[Solution]

Let's consider the worse case, which is that all n roots are non-negative integers. And that the roots are fairly small, so that when we pick our bound m, the roots are all $\leq m$.

In this case, the probability of choosing a root at random will be $\frac{n}{m+1}$. Now let's find the m where the bound holds, where p is the probability of selecting a root:

$$0.01 = \frac{1}{100} \geq \frac{n}{m+1} \geq p$$

$$\frac{m+1}{100} \geq n$$

$$m \geq 100n - 1$$

Thus when m is $100n - 1$, the probability of choosing a root is at or below 0.01.