Math 6014 - Homework 1

Caitlin Beecham

August 29, 2018

1. Let G be a graph with n vertices and m edges. Show that $\sum_{v \in V(G)} d(v)^2 \geq 4m^2/n$.
Proof:
Lemma 1 (Cauchy Schwarz Inequality):
For lists of numbers $(u_1, u_2, ..., u_n)$ and $(v_1, v_2, ..., v_n)$, the following holds:
$(\sum_{i \in [n]} u_i v_i)^2 \leq (\sum_{i \in [n]}(u_i^2))(\sum_{i \in [n]}(v_i^2))$.
Proof of Lemma 1:
Think of these as vectors. This statement is equivalent to the statement that $(\mathbf{u} \cdot \mathbf{v})^2 \leq \|\mathbf{u}\|^2 \|\mathbf{v}\|^2$. Now, let $w = proj_v(u) = \frac{\mathbf{u} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}} \mathbf{v}$. Let $y = u - w$. Now, by construction, y and w are orthogonal and form a right triangle with u as the hypotenuse, which means that the pythagorean theorem applies to their norms. Specifically, $\|\mathbf{u}\|^2 = \|\mathbf{y}\|^2 + \|\mathbf{w}\|^2 = \|\mathbf{y}\|^2 + (\frac{\mathbf{u} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}} \mathbf{v}) \cdot (\frac{\mathbf{u} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}} \mathbf{v}) = \|\mathbf{y}\|^2 + \frac{(\mathbf{u} \cdot \mathbf{v})^2}{(\mathbf{v} \cdot \mathbf{v})^2} \mathbf{v} \cdot \mathbf{v} = \|\mathbf{y}\|^2 + \frac{(\mathbf{u} \cdot \mathbf{v})^2}{(\|\mathbf{v}\|^2)^2} \|\mathbf{v}\|^2 = \|\mathbf{y}\|^2 + \frac{(\mathbf{u} \cdot \mathbf{v})^2}{(\|\mathbf{v}\|^2)} \geq \frac{(\mathbf{u} \cdot \mathbf{v})^2}{(\|\mathbf{v}\|^2)}$.
Lemma 2:
For a list of positive integers $(a_1, a_2, ..., a_n)$, the following holds: $(\sum_{i \in [n]} a_i)^2 \leq n(\sum_{i \in [n]}(a_i^2))$.
Proof of Lemma 2:
We apply Lemma 1 to the vectors $\mathbf{u} = (a_1, a_2, ..., a_n)$ and $\mathbf{v} = (\frac{1}{n}, \frac{1}{n}, ..., \frac{1}{n})$. We get that $(\mathbf{u} \cdot \mathbf{v})^2 = (\sum_{i \in [n]} \frac{1}{n} a_i)^2 = \frac{1}{n^2}(\sum_{i \in [n]} a_i)^2 \leq \|\mathbf{u}\|^2 \|\mathbf{v}\|^2 = (\sum_{i \in [n]}(\frac{1}{n})^2)(\sum_{i \in [n]}(a_i)^2) = \frac{1}{n^2} n(\sum_{i \in [n]}(a_i)^2) = \frac{1}{n}(\sum_{i \in [n]}(a_i)^2)$. So that gives us $\frac{1}{n^2}(\sum_{i \in [n]} a_i)^2 \leq \frac{1}{n}(\sum_{i \in [n]}(a_i)^2)$, which implies $(\sum_{i \in [n]} a_i)^2 \leq n(\sum_{i \in [n]}(a_i)^2)$.
Now, by the Handshake Lemma we know that $2m = \sum_{v \in V(G)} d(v)$, which implies that $(2m)^2 = 4m^2 = (\sum_{v \in V(G)} d(v))^2$. By Lemma 2, $(\sum_{v \in V(G)} d(v))^2 \leq n(\sum_{v \in V(G)}(d(v)^2))$ and we are done.

2. Let G be a connected graph with minimum degree $k \geq 2$. Prove that there is a path P in G on k vertices such that $G - P$ is connected.

   We consider the Depth First Search tree of G. As stated in class, this tree is normal, which for a spanning tree means that for all edges in G, its ends are comparable in the partial order defined in class. In particular this means that for any leaf of the DFS tree its neighbors, of which there are at least k, lie on the path from the leaf to the root. First we define a branch of the DFS tree. A branch is a path that includes a leaf as one end, whose internal vertices have degree 2 in the DFS tree and whose other end of is either a leaf or a vertex of degree ≥ 3 in the DFS tree. We consider two cases: there exists some branch with $\geq k+1$ vertices or there does not. If there exists such a branch, we delete the leaf and the next consecutive k-1 vertices. Then, the DFS tree is still connected which means that G is still connected. If all branches have $\leq k$ vertices, then we do the following. For all leaves consider the unique path from that leaf to the root. Then, for each of these paths look at the subpath with k vertices that starts at the leaf and goes toward the root, each ending with a vertex we'll call x_l. Pick an x_i that is farthest from the root and the corresponding leaf i and subpath that go with it. Then, we know that for all other leaves, l, their subpaths with k vertices reach closer (or at least as close) to the root than x_i. Now, since for all leaves the degree of l is $\geq k$ and all neighbors of l lie on the path from l to the root, we observe that at least one neighbor of our arbitrary leaf lies closer to the root than its subpath with k vertices. Because we are deleting $T[i, x_i]$ with x_i maximally far from r, this means that for all leaves l other than i, there is at least one neighbor of l not in $T[i, x_i]$ which means that it is still in $T' = T - T[i, x_i]$. Hence, T' is still connected which implies that $G' = G - T[i, x_i]$ is

still connected.
(A picture is attached for clarity on this last page. In this example, we delete $T[x_4, 4]$. One might worry this will disconnect branches 2,3, or 5. However, because each of 2,3, and 5 has some neighbor that is closer to r than x_4, T' is still connected).

3. Let F be a finite field with p (prime) elements and consider the vector space F^3. Define the graph G as follows. The vertices of G are the 1-dimensional subspaces of F^3, and two vertices are adjacent in G if and only if they are orthogonal in F^3. Let A denote the adjacency matrix of G, with A_{ii} corresponding to the number of loops at vertex i. Find A^2. (Optional: What can you say about the eigenvalues of A.)

   What is $(A^2)^i_j$? It is the number of walks of length 2 from vertex i to vertex j in G.

   One first asks what is $(A^2)^i_i$? Well it is the degree of vertex i in G, since all length two walks from a vertex to itself are exactly the walks going away on some edge and then coming back. What is the degree of a vertex i in G? It is the number of one dimensional subspaces orthogonal to it. We have two subspaces S_1 and S_2. Since these are 1 dimensional subspaces they can each be generated by one non-identity element. Let the ith vertex be S_1. We want to find S_2 orthogonal to it. Say $S_1 =< (u, v, w) >$ and $S_2 =< (a, b, c) >$. S_1 is orthogonal to S_2 if and only if (u,v,w) is orthogonal to (a,b,c). This is true iff $ua + vb + wc = 0$ iff (($u \neq 0$ and $a = \frac{-vb-wc}{u}$ (b and c can be anything)) or ($u = 0$ and $v \neq 0$ and $b = \frac{-wc}{v}$ (a and c can be anything)) or ($u = v = 0$ and $w \neq 0$ and $c = 0$ (a and b can be anything))).

   So, let's look at the case where $u \neq 0$. Then, for (a,b,c) to be orthogonal to (u,v,w), we need $(a, b, c) = (\frac{-vb-wc}{u}, b, c)$, with $((a, b, c) \neq (0, 0, 0))$ iff $((b, c) \neq (0, 0))$. That gives us $p^2 - 1$ degrees of freedom for choosing b and c.

   What about the case where $u = 0, v \neq 0$? Then, $(a, b, c) = (a, \frac{-wc}{v}, c)$, with $((a, b, c) \neq (0, 0, 0))$ iff $((a, c) \neq (0, 0))$. That gives us $p^2 - 1$ degrees of freedom for choosing a and c.

   What about the case where $u = v = 0, w \neq 0$? Then, $(a, b, c) = (a, b, 0)$, with $((a, b, c) \neq (0, 0, 0))$ iff $((a, b) \neq (0, 0))$. That gives us $p^2 - 1$ degrees of freedom for choosing a and b.

   So, we see that in any of these cases we have $p^2 - 1$ degrees of freedom in finding our orthogonal vector. However, this is finding individual orthogonal vectors. Some of these vectors may belong to the same one dimensional subspace. We go through each of our three cases and examine when two of the orthogonal vectors are in the same subspace.

   Case where $u \neq 0$: Assume we have (a,b,c) and (a',b',c') both orthogonal to (u,v,w) and in the same one dimensional subspace. Since both are orthogonal we know they have the form $(a, b, c) = (\frac{-vb-wc}{u}, b, c)$ and $(a', b', c') = (\frac{-vb'-wc'}{u}, b', c')$. The fact that they are in the same one dimensional subspace means that there exists g in our finite field such that $g(a, b, c) = (a', b', c')$ iff ($gb = b'$ and $gc = c'$ and $ga = a'$). In fact ($gb = b'$ and $gc = c'$) imply that $ga = a'$. Why? Well, $ga = g(\frac{-vb-wc}{u}) = \frac{-v(gb)-w(gc)}{u} = \frac{-vb'-wc'}{u} = a'$. So, if we have (a,b,c) orthogonal to (u,v,w), we can generate (a',b',c') also orthogonal to (u,v,w) and in the same one dimensional subspace as (a,b,c) by multiplying (b,c) by any non-zero element of g to get $g(b, c) = (b', c')$. We do so in $p - 1$ ways (it may be that g = 1 and (b,c)=(b',c')). As stated, these choices of (b',c') then determine a'. So, within the $p^2 - 1$ non-zero vectors orthogonal to (u,v,w), they are divided into groups of size $p - 1$. This means that there are $p + 1$ such groups. So, in this case the degree of $< (u, v, w) >$ in G is p+1.

   Case where $u = 0, v \neq 0$: Assume we have (a,b,c) and (a',b',c') both orthogonal to (u,v,w) and in the same one dimensional subspace. Since both are orthogonal we know they have the form $(a, b, c) = (a, \frac{-wc}{v}, c)$ and $(a', b', c') = (a', \frac{-wc'}{v}, c')$. The fact that they are in the same one-dimensional subspace means that there exists g in our finite field such that $g(a, b, c) = (a', b', c')$ iff ($gb = b'$ and $gc = c'$ and $ga = a'$). In fact ($ga = a'$ and $gc = c'$) imply that $gb = b'$. Why? Well, $gb = g(\frac{-wc}{v}) = \frac{-w(gc)}{v} = \frac{-wc'}{v} = b'$. So, if we have (a,b,c) orthogonal to (u,v,w), we can generate (a',b',c') also orthogonal to (u,v,w) and in the same one dimensional subspace as (a,b,c) by multiplying (a,c) by any non-zero element of g to get $g(a, c) = (a', c')$. We do so in $p - 1$ ways (it may be that g = 1 and (a,c)=(a',c')). As stated, these choices of (a',c') then determine b'. So, within the $p^2 - 1$ non-zero vectors orthogonal to (u,v,w), they are divided into groups of size $p - 1$. This means that there are $p+1$ such groups. So, in this case the degree of $<(u,v,w)>$ in G is p+1.

Case where $u = v = 0, w \neq 0$: Assume we have (a,b,c) and (a',b',c') both orthogonal to (u,v,w) and in the same one dimensional subspace. Since both are orthogonal we know they have the form $(a,b,c) = (a,b,0)$ and $(a',b',c') = (a',b',0)$. The fact that they are in the same one-dimensional subspace means that there exists g in our finite field such that $g(a,b,c) = (a',b',c')$ iff ($gb = b'$ and $gc = c'$ and $ga = a'$). In fact ($ga = a'$ and $gb = b'$) are all we need since $0 = 0$. So, if we have (a,b,c) orthogonal to (u,v,w), we can generate (a',b',c') also orthogonal to (u,v,w) and in the same one dimensional subspace as (a,b,c) by multiplying (a,b) by any non-zero element of g to get $g(a,b) = (a',b')$. We do so in $p-1$ ways (it may be that g $= 1$ and (a,b)=(a',b')). So, within the p^2-1 non-zero vectors orthogonal to (u,v,w), they are divided into groups of size $p-1$. This means that there are $p+1$ such groups. So, in this case the degree of $<(u,v,w)>$ in G is p+1.

So, in all cases the degree of $<(u,v,w)>$ is p+1.

Now, what is $(A^2)^i_j$ for $i \neq j$? Say vertex i is $<(a,b,c)>$ and vertex j is $<(g,h,i)>$. Then, the number of length two walks from vertex i to vertex j is the number of one dimensional subspaces that are orthogonal to both $<(a,b,c)>$ and $<(g,h,i)>$. Assume (d,e,f) is orthogonal to (a,b,c) and (q,r,s) is orthogonal to (g,h,i). Now, also assume (d,e,f) and (q,r,s) are in the same one-dimensional subspace so that $<(d,e,f)>$ is our desired one dimensional subspace that is orthogonal to both $<(a,b,c)>$ and $<(g,h,i)>$. We have 9 cases: (1) $a \neq 0$ and $g \neq 0$, (2) $a \neq 0$ and $g = 0$ and $h \neq 0$, (3) $a \neq 0$ and $g = h = 0$ and $i \neq 0$, (4) $a = 0$ and $b \neq 0$ and $g \neq 0$, (5) $a = 0$ and $b \neq 0$ and $g = 0$ and $h \neq 0$, (6) $a = 0$ and $b \neq 0$ and $g = h = 0$ and $i \neq 0$, (7) $a = b = 0$ and $c \neq 0$ and $g \neq 0$, (8) $a = b = 0$ and $c \neq 0$ and $g = 0$ and $h \neq 0$, and (9) $a = b = 0$ and $c \neq 0$ and $g = h = 0$ and $i \neq 0$.

Case 1: $a \neq 0$ and $g \neq 0$. The fact that (d,e,f) is orthogonal to (a,b,c) implies it is of the form $(d,e,f) = (\frac{-be-cf}{a}, e, f)$. Now, (q,r,s) orthogonal to (g,h,i) means that it has the form $(q,r,s) = (\frac{-hr-si}{g}, r, s)$. Since we are assuming that (d,e,f) and (q,r,s) are in the same subspace that means there is some x in our finite field such that x(d,e,f)=(q,r,s) iff (xe=r, xf = s and xd=q). Well, $xd = x(\frac{-be-cf}{a})$, and $q = \frac{-hr-si}{g}$. So, xd = q iff $xd = x(\frac{-be-cf}{a}) = \frac{-b(xe)-c(xf)}{a} = \frac{-br-cs}{a} = q = \frac{-hr-si}{g}$ iff $\frac{-b}{a}r + \frac{-c}{a}s = \frac{-h}{g}r + \frac{-i}{g}s$ iff $s = \frac{-ha+bg}{-gc+ia}r$. So, in order to determine a vector (that is to be orthogonal to both (a,b,c) and (g,h,i)) based on (a,b,c) and (g,h,i), we must make one choice: choose r in p-1 ways. Then that determines s and q. Can two such (q,r,s) exist and be in the same one-dimensional subspace? Yes, if (q,r,s) is such a pair then x(q,r,s) is such a triple for any x. Since for any nonzero r' in F, there exists some x such that r'=xr, all p-1 choices of r (and the triple (q,r,s) that they determine) all lie in the same one-dimensional subspace, so in this case, $(A^2)^i_j = 1$.

Case 2: $a \neq 0$ and $g = 0$ and $h \neq 0$. The fact that (d,e,f) is orthogonal to (a,b,c) implies it is of the form $(d,e,f) = (\frac{-be-cf}{a}, e, f)$. Now, (q,r,s) orthogonal to (g,h,i). If (d,e,f) and (q,r,s) are both in the same one-dimensional subspace, then (d,e,f) is also orthogonal to (g,h,i). This means that (d,e,f) has the form $(d,e,f) = (d, \frac{-fi}{h}, f)$. So, $(d,e,f) = (\frac{-be-cf}{a}, e, f) = (d, \frac{-fi}{h}, f) = (\frac{bfi-cfh}{ah}, \frac{-fi}{h}, f)$. This implies that the choice of non-zero f (done in p-1 ways) determines (d,e,f). Just like before all such d,e,f are in the same one-dimensional subspace, so $(A^2)^i_j = 1$.

Case 3: $a \neq 0$ and $g = h = 0$ and $i \neq 0$. The fact that (d,e,f) is orthogonal to (a,b,c) implies it is of the form $(d,e,f) = (\frac{-be-cf}{a}, e, f)$. Now, (q,r,s) orthogonal to (g,h,i). If (d,e,f) and (q,r,s) are both in the same one-dimensional subspace, then (d,e,f) is also orthogonal to (g,h,i). This means that (d,e,f) has the form $(d,e,f) = (d,e,0)$. So, $(d,e,f) = (\frac{-be-cf}{a}, e, f) = (d,e,0)$ iff $f = 0$ and $d = \frac{-be}{a}$. This implies that the choice of non-zero e (done in p-1 ways) determines (d,e,f). Just like before all such d,e,f are in the same one-dimensional subspace, so $(A^2)^i_j = 1$.

Case 4: $a = 0$ and $b \neq 0$ and $g \neq 0$. The fact that (d,e,f) is orthogonal to (a,b,c) implies it is of the form $(d,e,f) = (d, \frac{-fc}{b}, f)$. Now, (q,r,s) orthogonal to (g,h,i). If (d,e,f) and (q,r,s) are both in the same one-dimensional subspace, then (d,e,f) is also orthogonal to (g,h,i). This means that (d,e,f) has the form $(d,e,f) = (\frac{-eh-fi}{g}, e, f)$. So, $(d,e,f) = (d, \frac{-fc}{b}, f) = (\frac{-eh-fi}{g}, e, f)$ iff $e = \frac{-fc}{b}$ and $d = \frac{-eh-fi}{g}$. This implies that the choice of non-zero f (done in p-1 ways) determines (d,e,f). Just like before all such d,e,f are in the same one-dimensional subspace, so $(A^2)^i_j = 1$.

Case 5: $a = 0$ and $b \neq 0$ and $g = 0$ and $h \neq 0$. The fact that (d,e,f) is orthogonal to (a,b,c) implies it is of the form $(d,e,f) = (d, \frac{-fc}{b}, f)$. Now, (q,r,s) orthogonal to (g,h,i). If (d,e,f) and (q,r,s) are both in the same one-dimensional subspace, then (d,e,f) is also orthogonal to (g,h,i). This means that (d,e,f) has the form $(d,e,f) = (d, \frac{-fi}{h}, f)$. So, $(d,e,f) = (d, \frac{-fc}{b}, f) = (d, \frac{-fi}{h}, f)$ iff $\frac{-fc}{b} = \frac{-fi}{h}$ iff $f(\frac{c}{b} + \frac{-i}{h}) = 0$ iff ($f = 0$ or $\frac{c}{b} = \frac{i}{h}$).
In the case where f = 0, this implies that the choice of non-zero d (done in $p-1$ ways) determines (d,e,f). Also, all of these p-1 elements belong in the same subspace, so $(A^2)^i_j = 1$.
In the case where $f \neq 0$ and $\frac{c}{b} = \frac{i}{h}$, then we have $p^2 - 1$ choices for d and f which determine (d,e,f) and these come in groups of $p-1$, so there are $p+1$ such groups and $(A^2)^i_j = p+1$.

Case 6: $a = 0$ and $b \neq 0$ and $g = h = 0$ and $i \neq 0$. The fact that (d,e,f) is orthogonal to (a,b,c) implies it is of the form $(d,e,f) = (d, \frac{-fc}{b}, f)$. Now, (q,r,s) orthogonal to (g,h,i). If (d,e,f) and (q,r,s) are both in the same one-dimensional subspace, then (d,e,f) is also orthogonal to (g,h,i). This means that (d,e,f) has the form $(d,e,f) = (d,e,0)$. So, $(d,e,f) = (d, \frac{-fc}{b}, f) = (d,e,0)$ iff ($f = 0$ and $e = \frac{-fc}{b} = 0$) and d can be anything non-zero. This gives us $p-1$ choices for d, all in the same linear subspace, so $(A^2)^i_j = 1$.

Case 7: $a = b = 0$ and $c \neq 0$ and $g \neq 0$. By symmetry, this is the same as case 3, and $(A^2)^i_j = 1$.

Case 8: $a = b = 0$ and $c \neq 0$ and $g = 0$ and $h \neq 0$. By symmetry, this is the same as case 6, and $(A^2)^i_j = 1$.

Case 9: $a = b = 0$ and $c \neq 0$ and $g = h = 0$ and $i \neq 0$. The fact that (d,e,f) is orthogonal to (a,b,c) implies it is of the form $(d,e,f) = (d,e,0)$. Now, (q,r,s) orthogonal to (g,h,i). If (d,e,f) and (q,r,s) are both in the same one-dimensional subspace, then (d,e,f) is also orthogonal to (g,h,i). This means that (d,e,f) has the form $(d,e,f) = (d,e,0)$. So, $(d,e,f) = (d,e,0)$. That gives us $p^2 - 1$ choices for d and e. These are in groups of $p-1$ so there are p+1 such groups (subspaces) and $(A^2)^i_j = p+1$.