Linear Algebra in Combinatorics

Hugo Eberhard

August 2023

Combinatorics is a field which doesn't really have much deep theory (this doesn't mean there aren't deep theorems, though). Many big theorems are fairly independent from each other, and the proofs often borrow machinery from other parts of maths, such as linear algebra! In this spirit, today's lecture is mostly a collection of a couple of, in my opinion, very nice problems which (somewhat surprisingly) have quite simple solutions using tools from linear algebra. Most of the problems I present here will be more or less independent from each other, but each of them will present some ideas or techniques which can be used to solve many other problems in combinatorics of a similar flavour. I have tried to compile some such problems in the pset.

The problems covered in the lecture and the pset are collected from various different sources, some of which I don't remember. Many of them are covered in the book "Thirty-three Miniatures: Mathematical and Algorithmic Applications of Linear Algebra" by Jiřì Matoušek. Others I got from lectures or examples sheets in courses in Graph Theory (lectured by Julian Sahasrabudhe, Michaelmas 2021), Combinatorics (lectured by Béla Bollobás, Michaelmas 2022), and Computational Complexity (lectured by Timothy Gowers, Lent 2023) at University of Cambridge.

1 Oddtown

There are n people living in Oddtown. They really like forming clubs, but they don't like to do it just randomly. Instead, they have a set of rules which they enforce without any exceptions. The rules are as follows:

(a) Any club must have an odd number of members.

(b) Any two clubs must have an even number of members in common.

Since the people in Oddtown really like clubs, they would like to form as many clubs as possible while following these rules. What is the largest number of clubs they could form?

How do we determine this number? It's not hard to see that we could have n clubs. For example, each person could have their own club, with them as the only member:

$$\{1\},\ \{2\},\ \{3\},\ ...,\ \{n\}$$

Then every club has one member (an odd number) and any two clubs have zero members in common (an even number). But can we do better than this? It turns out that the answer is no, and we will present two proofs of this.

As you might have guessed, both solutions will use some linear algebra. But it doesn't look at all like a linear algebra problem at first glance. For example, there is no mention of any vectors or matrices. Instead the problem seems to be about sets. Indeed, we can think of the people in Oddtown as the set $\{1, 2, ..., n\}$ (which we will denote by $[n]$) and the clubs as subsets of people, i.e as subsets $A_1, ..., A_m \subset [n]$. Hence the first step of our proof is to find some way of rewriting the information in the problem in terms of some vectors.

We use a clever, and very common trick. Let's consider the indicator vectors of the sets $A_1, ..., A_m$, call them $\mathbf{v}_1, ..., \mathbf{v}_m$. These are defined to be vectors of length n where each entry is either 0 or 1 depending on whether the corresponding person is in the set or not. For example, if $n = 5$ and one of the clubs is $A = \{2, 5\}$ the corresponding vector would be $\mathbf{v} = (0, 1, 0, 0, 1)$. We can then interpret the conditions on $A_1, ..., A_m$ in terms of dot products as follows:

- $|A_i|$ is odd $\iff$ $\mathbf{v}_i$ has an odd number of ones, i.e $\langle \mathbf{v}_i, \mathbf{v}_i \rangle = 1 \pmod 2$
- $|A_i \cap A_j|$ is even $\iff$ $\mathbf{v}_i, \mathbf{v}_j$ have an even number of common ones, i.e $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0 \pmod 2$

where $\langle \mathbf{v}, \mathbf{w} \rangle = \sum_{i=1}^{n} v_i w_i$ for any two vectors $\mathbf{v} = (v_1, ..., v_n)$ and $\mathbf{w} = (w_1, ..., w_n)$. We now have two ways to finish the proof.

Method 1: The above two conditions look a lot like saying that the vectors are orthonormal, except that the dot products are not actually 0 and 1 since the conditions are stated modulo 2. We can fix this by viewing the vectors as living in the vector space $\mathbb{F}_2^n$ over the field $\mathbb{F}_2 = \{0, 1\}$ instead of over the reals, i.e we consider everything modulo 2. Since this is a field (meaning that we can add and multiply numbers within $\mathbb{F}_2$, that addition and multiplication work as we expect and that every non-zero number has a multiplicative inverse), linear algebra works as usual. We can then prove that the vectors are linearly independent over $\mathbb{F}_2$ the same way we would usually prove this for orthonormal vectors. Indeed, assume that $\sum \lambda_i \mathbf{v}_i = 0$ for some constants $\lambda_i \in \mathbb{F}_2$. Then we get

$$\sum \lambda_i \mathbf{v}_i = 0 \quad \implies \quad \sum \lambda_i \langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0 \quad \implies \quad \lambda_j = 0$$

where we have taken the dot product of the sum with the vector $\mathbf{v}_j$. This shows that $\lambda_j = 0$ for every j, so in particular there is no way of writing any of the vectors $\mathbf{v}_i$ as a linear combination of the other vectors. Hence they are linearly independent, so since they live inside the $n-$dimensional space $\mathbb{F}_2^n$, there can be at most n of them. This finishes the proof.

Method 2: The above proof is probably the simplest one, but I will show another one as well since it uses a technique which generalises to many other problems. Let M be the $n \times m$ matrix with columns $\mathbf{v}_1, ..., \mathbf{v}_m$:

$$M = \begin{bmatrix} | & | & & | \\ \mathbf{v}_1 & \mathbf{v}_2 & ... & \mathbf{v}_m \\ | & | & & | \end{bmatrix}$$

Then we consider the matrix $M^T M$:

$$M^T M = \begin{bmatrix} - & \mathbf{v}_1 & - \\ - & \mathbf{v}_2 & - \\ & ... & \\ - & \mathbf{v}_n & - \end{bmatrix} \begin{bmatrix} | & | & & | \\ \mathbf{v}_1 & \mathbf{v}_2 & ... & \mathbf{v}_m \\ | & | & & | \end{bmatrix} = \begin{bmatrix} \langle \mathbf{v}_1, \mathbf{v}_1 \rangle & \langle \mathbf{v}_1, \mathbf{v}_2 \rangle & ... & \langle \mathbf{v}_1, \mathbf{v}_m \rangle \\ \langle \mathbf{v}_2, \mathbf{v}_1 \rangle & \langle \mathbf{v}_2, \mathbf{v}_2 \rangle & ... & \langle \mathbf{v}_2, \mathbf{v}_m \rangle \\ \langle \mathbf{v}_3, \mathbf{v}_1 \rangle & \langle \mathbf{v}_3, \mathbf{v}_2 \rangle & ... & \langle \mathbf{v}_3, \mathbf{v}_m \rangle \\ ... & & & ... \\ \langle \mathbf{v}_m, \mathbf{v}_1 \rangle & \langle \mathbf{v}_m, \mathbf{v}_2 \rangle & ... & \langle \mathbf{v}_m, \mathbf{v}_m \rangle \end{bmatrix} = I_m$$

where I_m is the $m \times m$ identity matrix and the last equality holds modulo 2, i.e over $\mathbb{F}_2$. Hence the matrix $M^T M = I_m$ has full rank. So we get

$$m = rank(M^T M) \leq rank(M) \leq n$$

where we use that multiplying a matrix by another matrix can only reduce the rank (this is a fact which is proven in most undergraduate linear algebra courses, but as a reminder I have also put it on the pset). This finishes the proof. ■

Here is a quick summary of the important ideas and takeaways:

- We can view subsets of $[n]$ as $n-$dimensional vectors with entries in $\{0, 1\}$. The dot product of two such vectors is equal to the size of the intersection of the corresponding sets.
- Linear algebra works over all fields, including $\mathbb{F}_2$ (modulo 2) and in general over $\mathbb{F}_p$ (modulo p). This means that if we are working with vectors or matrices with integer entries, we can reduce them modulo p, and still use results from linear algebra such as "the largest number of linearly independent vectors is at most the dimension of the space they live in" and "the rank of a product of two matrices is at most the minimum of the ranks of the factors". However we sometimes have to take extra care when reducing modulo p. In particular, the dot product is no longer technically an inner product since $\langle \mathbf{v}, \mathbf{v} \rangle = 0 \pmod p$ does not necessarily imply that $\mathbf{v} = 0$.
- This being said, we have now seen that if $\mathbf{v}_1, ..., \mathbf{v}_m$ is a set of orthonormal vectors in a vector space over $\mathbb{F}_p$, we can still conclude that they are linearly independent.

- Finally, it turns out that this is not the only problem where bounding the rank of some cleverly chosen matrix essentially solves the problem! In particular, the fact that

$$rk(AB) \leq \min\{rk(A),\ rk(B)\}$$

will often come in useful.

2 Equilateral Sets

Can we find three points A, B, C in the plane, such that all pairwise distances are the same? Of course the answer is yes, just take an equilateral triangle. More generally, in $\mathbb{R}^n$, we can find $n+1$ points such that all pairwise distances are the same (say such a set of points is *equilateral*). For example we can pick the points

$$(1,0,0,...,0),(0,1,0,...,0),(0,0,1,...,0),...,(0,0,0,...,1),(t,t,t,...,t)$$

where we have to choose t such that the distance to any of the other points is $\sqrt{2}$. Another way to find $n+1$ points is to temporarily allow one extra dimension. Clearly the points

$$(1,0,0,...,0),(0,1,0,...,0),...,(0,0,0,...,1) \in \mathbb{R}^{n+1}$$

are all equidistant. But they also all live in the hyperplane $x_1 + ... + x_{n+1} = 1$, which is just a copy of $\mathbb{R}^n$.

So we can find an equilateral set with $n+1$ points in $\mathbb{R}^n$. Can we find more? The answer is no, which shouldn't come as a surprise. How do we prove it? I will talk about two ways in which one might prove this. Each of them will introduce some ideas.

Method 1: We might as well assume that one of our points is 0 by translating the whole set of points. Let's say that the remaining points are $\mathbf{v}_1, ..., \mathbf{v}_m$, so that we have $m+1$ points in total, and consider these as vectors in $\mathbb{R}^n$. They must all be at the same distance from 0, say at distance 1. Then we have that

- $1 = ||\mathbf{v}_i||^2 = \langle \mathbf{v}_i, \mathbf{v}_i \rangle$
- $1 = ||\mathbf{v}_i - \mathbf{v}_j||^2 = \langle \mathbf{v}_i - \mathbf{v}_j, \mathbf{v}_i - \mathbf{v}_j \rangle = \langle \mathbf{v}_i, \mathbf{v}_i \rangle - 2\langle \mathbf{v}_i, \mathbf{v}_j \rangle + \langle \mathbf{v}_j, \mathbf{v}_j \rangle = 2(1 - \langle \mathbf{v}_i, \mathbf{v}_j \rangle)$

$$\implies \langle \mathbf{v}_i, \mathbf{v}_j \rangle = \tfrac{1}{2}$$

As in our second method from the Oddtown problem, we define the matrix

$$M = \begin{bmatrix} | & | & & | \\ \mathbf{v}_1 & \mathbf{v}_2 & ... & \mathbf{v}_m \\ | & | & & | \end{bmatrix}$$

and consider the matrix

$$\begin{aligned} M^T M &= \begin{bmatrix} - & \mathbf{v}_1 & - \\ - & \mathbf{v}_2 & - \\ & ... & \\ - & \mathbf{v}_m & - \end{bmatrix} \begin{bmatrix} | & | & & | \\ \mathbf{v}_1 & \mathbf{v}_2 & ... & \mathbf{v}_m \\ | & | & & | \end{bmatrix} \\ &= \begin{bmatrix} \langle \mathbf{v}_1, \mathbf{v}_1 \rangle & \langle \mathbf{v}_1, \mathbf{v}_2 \rangle & ... & \langle \mathbf{v}_1, \mathbf{v}_m \rangle \\ \langle \mathbf{v}_2, \mathbf{v}_1 \rangle & \langle \mathbf{v}_2, \mathbf{v}_2 \rangle & ... & \langle \mathbf{v}_2, \mathbf{v}_m \rangle \\ \langle \mathbf{v}_3, \mathbf{v}_1 \rangle & \langle \mathbf{v}_3, \mathbf{v}_2 \rangle & ... & \langle \mathbf{v}_3, \mathbf{v}_m \rangle \\ ... & & & ... \\ \langle \mathbf{v}_m, \mathbf{v}_1 \rangle & \langle \mathbf{v}_m, \mathbf{v}_2 \rangle & ... & \langle \mathbf{v}_m, \mathbf{v}_m \rangle \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1/2 & ... & 1/2 \\ 1/2 & 1 & ... & 1/2 \\ 1/2 & 1/2 & ... & 1/2 \\ ... & & & ... \\ 1/2 & 1/2 & ... & 1 \end{bmatrix} \end{aligned}$$

We now want to show that this matrix has full rank, i.e that the columns span the entire vector space $\mathbb{R}^m$. The sum of the columns is $\frac{m+1}{2}(1,1,...,1)$, and so in particular the vector $(1,1,...,1)$ is in the column space. Hence we also get that

$$(1,0,...,0) = 2\left((1, \frac{1}{2}, ..., \frac{1}{2}) - \frac{1}{2}(1,1,...,1) \right)$$

is in the column space, i.e the first standard basis vector. Similarly, all the standard basis vectors are in the column space, and so the matrix $M^T M$ has rank m. We conclude that

$$m = rank(M^T M) \leq rank(M) \leq n \qquad \implies \qquad m + 1 \leq n + 1$$

as required.

Note that it's also possible to show that the vectors $\mathbf{v}_1, ..., \mathbf{v}_m$ are linearly independent directly, which would also allow us to conclude that $m \leq n$. However this takes a bit of work.

Method 2: This method is more technical and arguably trickier, and will only give us a bound of $n + 2$ for the maximum number of points that are all at pairwise equal distance. However, it generalises to the problem of bounding the maximum number of points we can pick such that they only determine *two* distances (this problem will be an exercise in the pset). It will also give us an opportunity to consider certain sets of polynomials as vector spaces, which turns out to sometimes be very useful.

Assume that we have m points $\mathbf{v}_1, ..., \mathbf{v}_m$ in $\mathbb{R}^n$, all pairs of which are at distance 1 from each other. For each of these points we define an associated polynomial in the variables $x_1, ..., x_n$ (we think of $x_1, ..., x_n$ as coordinates of a point in $\mathbb{R}^n$):

$$f_i(x_1, ..., x_n) = ||\mathbf{x} - \mathbf{v}_i||^2 - 1 = \langle \mathbf{x} - \mathbf{v}_i, \mathbf{x} - \mathbf{v}_i \rangle - 1$$

These polynomials have the important property that

- $f_i(\mathbf{v}_j) = 0 \qquad$ if $i \neq j$
- $f_i(\mathbf{v}_j) = 1 \qquad$ if $i = j$

This means that if we view the set of polynomials in the variables $x_1, ..., x_n$ as a vector space over $\mathbb{R}$ (we can do this: it's easy to check that they satisfy all the axioms of a vector space), we can easily prove that they are all linearly independent. Indeed, if $\sum \lambda_i f_i(\mathbf{x}) = 0$, then by evaluating this expression at $\mathbf{x} = \mathbf{v}_j$ we get that

$$\sum \lambda_i f_i(\mathbf{v}_j) = 0 \qquad \implies \qquad \lambda_j = 0$$

by using the property of f_i that we observed above. If we could somehow find a subspace of low dimension in which all of these polynomials live, we would hence get a bound on m, which is what we want.

First we note that they are all degree 2 polynomials, and hence must be in the span of the polynomials

$$1, x_i, x_i x_j, x_i^2 \qquad \text{for } i, j \text{ between 1 and } n$$

This is a list of $1 + n + \binom{n}{2} + n$ polynomials, so we hence get that $m \leq \frac{n^2}{2} + \frac{3n}{2} + 1$ (because the polynomials $f_1, ..., f_m$ are m linearly independent polynomials living in a subspace of dimension $\frac{n^2}{2} + \frac{3n}{2} + 1$). However, we want to do better, and it turns out that we can.

Note that

$$f_i(x) = \langle x - v_i, x - v_i \rangle - 1 = \langle x, x \rangle - 2\langle x, v_i \rangle + \langle v_i, v_i \rangle - 1$$

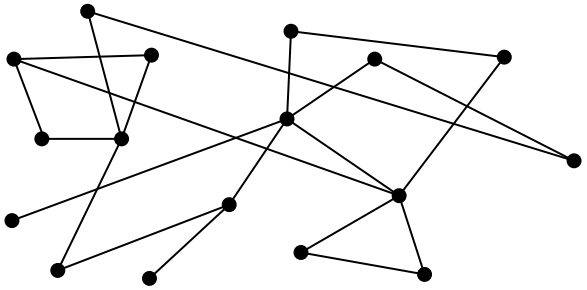
which is clearly in the span of

$$1, x_1, x_2, ..., x_n \quad \text{and} \quad \langle x, x \rangle$$

This list only contains $n + 2$ polynomials, so we get that $m \leq n + 2$. This is not quite the optimal answer, but very close. We won't try to optimise this further here.

3 Graph Theory and Linear Algebra

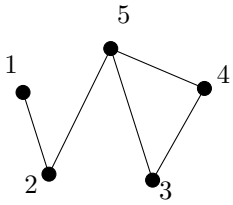
A **graph** is a collection of **vertices**, some pairs of which are connected by **edges**. For example, this is a graph:



Sometimes people talk about *directed graphs*, in which the edges have a direction so that an edge $v \to w$ is not the same thing as an edge $w \to v$. There is also a notion of *weighted graphs*, in which each edge has a number associated to it, called the *weight*. This could for example be interpreted as the distance between the two vertices. Of course, you could come up with even more ways of adding more information and structure to a graph. However, we will only consider undirected, unweighted graphs. We will also not allow any loops (edges connecting a vertex to itself).

Graph theory is the study of these objects, and it's a big part of Combinatorics. But graphs also feature in many other areas of maths, and have many real world applications. Just think of how Google maps gives you directions: that is basically about answering questions about a huge (weighted, directed) graph, specifically something like "what is the shortest path between two cities (vertices)".

There is a natural way to interpret a graph as a matrix A. We simply set the value of A_{ij} to 1 if there is an edge between i and j, and 0 otherwise. For example:



$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

This matrix is called the **adjacency matrix** of the graph. Note that it's symmetric, and hence there is an orthonormal basis of eigenvectors $v_1, ..., v_n$ corresponding to the (real) eigenvalues $\lambda_1 \geq ... \geq \lambda_n$.

Before we can get to the actual problem, let's make a few more definitions which will come in handy later.

(a) Say that a graph is **connected** if it's possible to walk between any pair of nodes following edges in the graph.

(b) For a vertex v, we say that the **degree of** v is the number of neighbours of v.

(c) Say that a graph is $k-$**regular** if every vertex has degree k.

After this rather long introduction, we can finally get to the problem that we actually care about in this section. We said that a graph is $k-$regular if all the vertices have degree k. Such graphs are pretty nice in many ways (unfortunately I don't have time to talk about reasons why this might be nice, other that the intuitive reason which is that patterns are nice). What if we can ask for even more regularity? One way of strengthening the notion of a regular graph is by also requiring that any two neighbours have some specified number of neighbours a in common, and any two non-neighbours have b neighbours in common (in addition to all vertices having degree k). Of course there might be other natural ways of strengthening the notion of regularity, but let's run with this one for now.

A special case of this is when $a = 0$ and $b = 1$. In this case we get what's known as a *Moore graph*, i.e a graph such that:

(a) any vertex has degree k (the graph is $k-$regular)

(b) any two vertices that are connected by an edge have no common neighbours

(c) any two vertices that are *not* connected by an edge have exactly one common neighbour

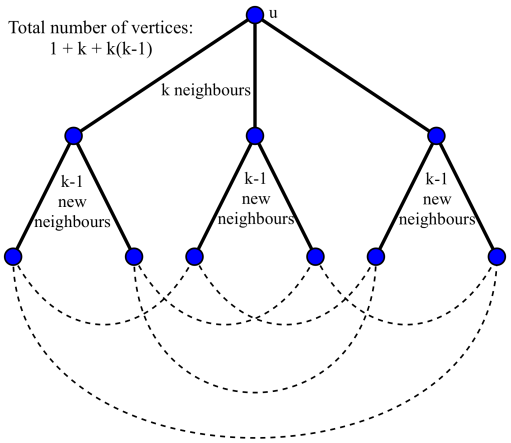
For example, in the cases $k = 2$ and $k = 3$, the following are examples of Moore graphs:

After having seen these two examples, one might think that there should exist lots of examples of Moore graphs. Maybe there is even one for every k. However, it turns out that already for $k = 4$ there is no Moore graph. In fact, as we will see soon, the only values of k for which there *might* exist a Moore graph are $k = 2, 3, 7, 57$. It is known that there are Moore graphs for $k = 2, 3$ and 7, but it is still an unsolved problem whether there exists one for $k = 57$!

We will prove this in a couple of steps. Assume that we have a Moore graph with n vertices which is $k-$regular, and that the corresponding adjacency matrix is A.

Step 1: Note that any two vertices are either neighbours (in which case they are at distance 1 from each other) or they have exactly one neighbour in common (in which case they are distance 2 from each other). In particular, it's possible to walk between any two vertices following some edges in the graph, and so it's connected.

But we can say more than that. Pick some vertex u, and let $v_1, ..., v_k$ be its neighbours. Now v_i, v_j can never be adjacent to each other, since they have u as a common neighbour. They also can't have any neighbours in common other than u, since they should have exactly one common neighbour. Since the graph is $k-$regular, each of the vertices v_i must hence have $k-1$ neighbours in addition to u, and these must all be different for different v_i. Finally, these are all the vertices in the graph, since no vertex can be at distance larger than 2 from u (then they wouldn't have any common neighbours). We conclude that the graph must look as follows:



In particular, the total number of vertices is $1 + k + k(k-1) = 1 + k^2$.

Step 2: If we compute the square of the adjacency matrix A^2, the entry $(A^2)_{ij}$ is exactly the number of common neighbours of i and j in the graph (it's the dot product of the i^{th} row with the j^{th} column). Hence in particular,

- $(A^2)_{ii} = k$ as i has exactly k neighbours in common with itself
- $(A^2)_{ij} = 0$ if $i \neq j$ and they *are* neighbours
- $(A^2)_{ij} = 1$ if $i \neq j$ and they are *not* neighbours

These observations can be summarized in the matrix equation

$$A^2 = kI + (J - A - I)$$

where J is the matrix which consists of only 1s and I is the identity matrix (note that $J-A-I$ has a 1 in entry (i,j) if and only if $i \neq j$ and i is not adjacent to j in the graph).

Step 3: Let $\mathbb{1} = (1, 1, ..., 1)$ be the vector with only 1s. Note that

$$A\mathbb{1} = \begin{bmatrix} \#1\text{s in first row of A} \\ \#1\text{s in second row of A} \\ ... \\ \#1\text{s in last row of A} \end{bmatrix} = \begin{bmatrix} k \\ k \\ ... \\ k \end{bmatrix} = k\mathbb{1}$$

since the graph is $k-$regular. In particular, $\mathbb{1}$ is an eigenvector with corresponding eigenvalue k. Conversely, if x is a vector with eigenvalue k, so that $Ax = kx$, it turns out that $x_1 = x_2 = ... = x_n$. Indeed, assume without loss of generality that $x_1 \geq x_2 \geq ... \geq x_n$. Then, by considering the first entry of Ax, we get that

$$Ax = kx \quad \Longrightarrow \quad \sum_{i \text{ adj to } 1} x_i = kx_1 \quad \Longrightarrow \quad x_i = x_1 \quad \text{for every } i \text{ adj to } 1$$

where the second implication follows from noting that the sum $\sum_{i \text{ adj to } 1} x_i$ has k terms (as the graph is $k-$regular), each of which is at most x_1 by assumption, and so they must all be exactly x_1. But now we know that for every i that is adjacent to 1, we must have $x_i = x_1 \geq x_2 \geq ... \geq x_n$. Hence we can use exactly the same argument to show that for every j which is adjacent to some neighbour i of 1, we also have $x_j = x_i = x_1$. Since the graph is connected (in fact, every vertex is at distance at most 2 from any other vertex), we can keep going like this to get that $x_1 = x_2 = ... = x_n$, as we wanted.

We can conclude that the eigenspace corresponding to the eigenvalue k has dimension 1, and so since the matrix is symmetric and has an eigenbasis, both the geometric and the algebraic multiplicity of k as an eigenvalue is 1. In particular, there must be a total of $n-1$ other eigenvalues counted with multiplicity.

Step 4: Next, consider any eigenvector v corresponding to some eigenvalue $\lambda \neq k$. By step 2, we know that $A^2 = (k-1)I + J - A$. In particular, we get that

$$A^2v = (k-1)v + Jv - Av \quad \Longrightarrow \quad \lambda^2 v = (k-1)v + (\sum_i v_i)\mathbb{1} - \lambda v$$

Since $\lambda \neq k$ and v is an eigenvector with eigenvalue λ, it can't be parallell to $\mathbb{1}$. Hence this implies that

$$\lambda^2 = k - 1 - \lambda \quad \Longrightarrow \quad \lambda_\pm = -\frac{1}{2} \pm \sqrt{k - \frac{3}{4}}$$

We hence know that the eigenvalues of A are

$$1, \lambda_+, ..., \lambda_+, \lambda_-, ..., \lambda_-$$

where the number of copies of λ_+ is t_+ and the number of copies of λ_- is t_-. On the other hand, we know that the trace of A is 0 since every entry on the diagonal is 0. This implies that

$$\begin{aligned} k + t_+\lambda_+ + t_-\lambda_- &= 0 \\ t_+ + t_- &= n - 1 \end{aligned}$$

Solving this system of equations for t_+ and t_- (plugging in the expressions for λ_+ and λ_- from above), we get that

$$t_\pm = \frac{1}{2}\Big(n - 1 \pm \frac{n-1-2k}{\sqrt{4k-3}}\Big) = \frac{1}{2}\Big(k^2 \pm \frac{k^2-2k}{\sqrt{4k-3}}\Big)$$

where we use that $n = k^2 + 1$ in the last step. But this has to be an integer, since clearly the number of copies of $\lambda_\pm$ as an eigenvalue is an integer. We have two cases:

- If $k^2 - 2k \neq 0$ we must have that $a = \sqrt{4k-3}$ is a rational number, and so an integer since $4k-3$ is an integer, giving $k = \frac{a^2+3}{4}$ for some integer a. Plugging this into the expression and putting everything on a common denominator we eventually get that a must divide 15 and so is either $1, 3, 5$ or 15. Plugging this back into the expression $k = \frac{a^2+3}{4}$ we get $k = 1, 3, 7$ or $k = 57$. Clearly $k = 1$ doesn't work.

– Otherwise $k^2 - 2k = 0$ which gives the solution $k = 2$.

Hence we are done. We have seen that for there to be any hope of finding a $k-$regular Moore graph, we must have $k = 2, 3, 7$ or 57 and the number of vertices has to be $k^2 + 1$. We have seen examples of Moore graphs for $k = 2$ and $k = 3$. There does exist a Moore graph for $k = 7$, but no one knows if there is one for $k = 57$!