METHODS OF LINEAR ALGEBRA IN COMBINATORICS

K. N. RAGHAVAN
THE INSTITUTE OF MATHEMATICAL SCIENCES

CONTENTS

These are notes of three lectures given at the TEACHERS' ENRICHMENT WORKSHOP at IMSc held during 27 November–02 December, 2017. Comments are solicited and may please be sent to the author at knr.imsc@gmail.com.

1. Clubs in odd town and even town

1.1. **Statement of the odd town club problem.** Once upon a time, in the city state of *Odd Town*, there lived n residents. They formed clubs, subject to the following (admittedly odd) rules:

- Each club consists of an odd number of residents.
- The number of members common to two different clubs is always even.

Note that the second condition allows two clubs to be disjoint (after all, zero is an even number). Note also that the two conditions together imply that two different clubs cannot have the same set of members.

The question is: what is the maximum number of clubs that they could form?

1.2. **Examples of clubs in odd town.** Let us identify the set of residents with $[n]$, the set of all positive integers not exceeding n. Taking the clubs to be all singleton subsets of $[n]$, the residents of odd town could obviously have formed n clubs. For n even, they could also have taken the clubs to be all subsets of cardinality $n-1$. For $n=6$ for instance, here is yet another way in which they could have formed 6 clubs:

$$\{1,2,3\},\ \{1,2,4\},\ \{1,2,5\},\ \{1,2,6\},\ \{1,3,4,5,6\},\ \{2,3,4,5,6\} \tag{1}$$

1.3. **The odd town club theorem.** While there seem to be many different ways in which the n residents of odd town could have formed n clubs, is it possible that they could have done better and formed more than n clubs? It turns out that it is not:

Theorem 1. *No more than n clubs can be formed under the odd town rules in §1.1.*

1.4. **The set up and idea of the proof.** We represent subsets of $[n]$ as n-tuples ($n\times 1$ column matrices): the j^{th} entry is either 1 or 0 depending upon whether or not j is an element of the subset. The six clubs in (1) are, for instance, represented as columns of the following matrix:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Towards the proof of the theorem, let us suppose that we have formed m clubs according to the rules of §1.1. We want to show that $m\le n$. Choosing $\mathbb{F}$ to be an arbitrary field, we may think of the clubs as elements of $\mathbb{F}^n$, where $\mathbb{F}^n$ is the vector space consisting of all $n\times 1$ column vectors with entries in $\mathbb{F}$. If we can show that the m elements of $\mathbb{F}^n$ corresponding to the m clubs are linearly independent (for an appropriate choice of $\mathbb{F}$), it would follow that $m\le n$, since the dimension of $\mathbb{F}^n$ as a vector space is n.

1.5. **The standard bilinear form.** We have a natural symmetric bilinear form on $\mathbb{F}^n$:

$$(a, b) := a_1b_1 + \cdots + a_nb_n = a^tb = b^ta \quad \text{for } a \text{ and } b \text{ in } \mathbb{F}^n$$

where we've denoted by a_j, $1 \leq j \leq n$, the entries of a, by a^t the transpose of a, and by a^tb the usual matrix product of a^t and b.

For a in $\mathbb{F}^n$, let φ_a denote the linear functional on $\mathbb{F}^n$ given by $b \mapsto (a, b)$.

1.6. **Proof of the odd town theorem.** We choose $\mathbb{F}$ to be the field of two elements. Let $c_1, \ldots, c_m$ be the $n \times 1$ column vectors (elements of $\mathbb{F}^n$) corresponding to the m clubs, and let $\lambda_1c_1 + \cdots + \lambda_mc_m = 0$ be a linear dependence relation among them. Fix j, $1 \leq j \leq m$, and apply the linear functional $\varphi_j := \varphi_{c_j}$ to both sides of this relation. We observe that $\varphi_j(c_j) = 1$ (since each club has an odd number of members) and $\varphi_j(c_i) = 0$ for $i \neq j$ (since between two distinct clubs there are evenly many members in common). Applying φ_j thus gives $\lambda_j = 0$. Since j was arbitrary, this proves the linear independence of c_j, $1 \leq j \leq m$, and the proof of Theorem 1 is complete. □

1.7. **The even town club problem.** There lived n residents in the city state of *Even Town*. Like their neighbours in Odd Town, they too formed clubs. But, true to their name, each of their clubs had evenly many members. Here are the rules they followed:

- Each club has evenly many members. (Being mathematically minded, the residents of this strange town even allowed a club to have no members at all!)
- The number of members common to two different clubs is always even. In particular, the clubs could be disjoint.
- Two different clubs cannot have the same set of members.

The question once again is: What is the maximum number of clubs that they could form?

1.8. **Examples of clubs in even town.** Perhaps surprisingly, the slight alteration in the rules allows for far many more clubs to be formed in even town (compared to the situation in odd town). Suppose that n is even. Put $n = 2k$, and imagine the n residents to consist of k couples. For every subset of k, we form a club consisting of all the couples belonging to that subset. It is easy to see that these clubs satisfy the required conditions. Thus we have formed $2^k = 2^{\frac{n}{2}}$ clubs. If n is odd, by excluding one resident from all clubs and following the previous construction with the remaining $n - 1$ residents, we can form $2^{\frac{n-1}{2}}$ clubs.

1.9. **The even town club theorem.** For k a real number, let $\lfloor k \rfloor$ denote the greatest integer not exceeding k.

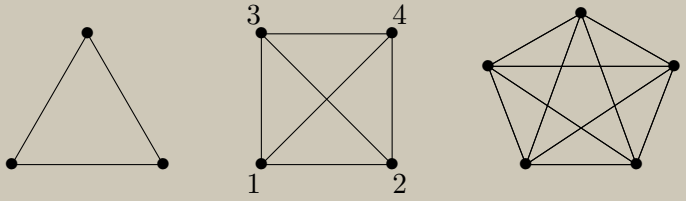
Theorem 2. *No more than $2^{\lfloor \frac{n}{2} \rfloor}$ clubs can be formed under the even town rules in §1.7.*

PROOF: As in the proof of Theorem 1, we identify clubs with elements of $\mathbb{F}^n$, where $\mathbb{F}$ is the field of two elements. Suppose that we have formed m clubs according to the rules in §1.7. We will prove that $m \leq 2^{\lfloor \frac{n}{2} \rfloor}$.

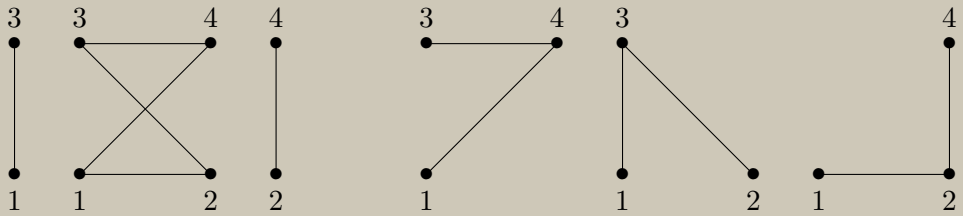
The key observation is the following: the even town rules imply that for any two clubs c and c' (including the case when $c = c'$) we have $(c, c') = 0$ (where (c, c') is the standard bilinear product of c and c' as in §1.5). Thus the clubs span an isotropic subspace of $\mathbb{F}^n$ (with respect to the standard bilinear form). (See items (2) and (3) in §4 for review of the definition of isotropic subspaces and the basic fact about how large they can be that is used in this proof.) The standard form being non-degenerate, the maximal dimension of an isotropic subspace is $\lfloor \frac{n}{2} \rfloor$. The cardinality of the space spanned by the clubs (and hence that of the clubs themselves) is thus bounded above by $2^{\lfloor \frac{n}{2} \rfloor}$. □

2. THE GRAHAM-POLLAK THEOREM

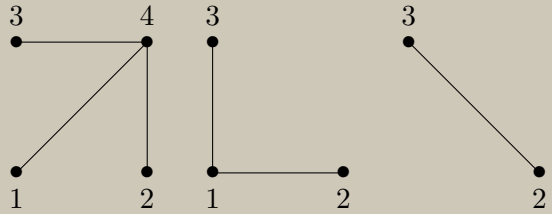
2.1. **The complete graph K_n.** Let K_n denote the *complete graph* on n vertices. Complete graphs on three, four, and five vertices are depicted below:



2.2. **Decompositions of the complete graph.** A *decomposition* of K_n is a "partition" into complete bipartite subgraphs: the set of edges of K_n is partitioned into those of the subgraphs; the same vertex could be part of more than one subgraph. Here are two examples of such partitions of K_4:



Here is a third example:

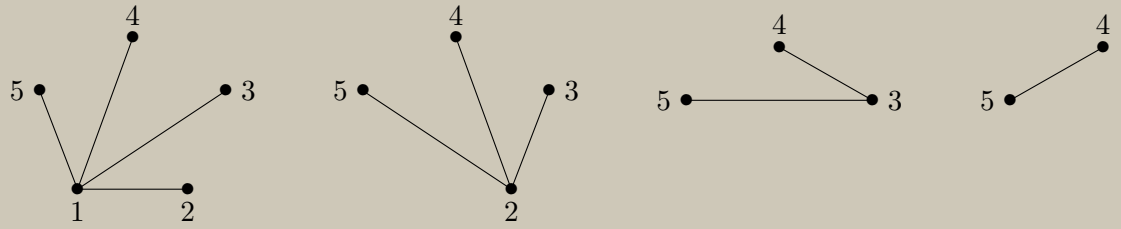


Partitioning the edge set into singletons is also a valid decomposition.

2.3. **Statement of the theorem.** The following question about decompositions is motivated by applications to networks and communications:

> What is the least number of complete bipartite subgraphs into which the complete graph K_n on n vertices can be decomposed?

Note that we have a special decomposition of K_n into $n-1$ complete bipartite subgraphs as follows. Identify the vertex set of K_n with $[n]$. For every j, $1 \leq j < n$, let B_j be the subgraph consisting of all edges (j,k) with $k > j$. For $n = 5$, here is how the B_j look:



Can we somehow manage to obtain a decomposition of K_n with fewer than $n-1$ complete bipartite subgraphs? No, we cannot:

Theorem 3. (GRAHAM-POLLAK, 1972) *In any decomposition of K_n, the complete graph on n vertices, there are at least $n-1$ complete bipartite subgraphs.*

We discuss three proofs in the three subsections below, all based on linear algebra. First we fix some notation to be used commonly in the proofs.

2.4. **Notation to be used in the proofs.** Let G be a general graph. The notion of a *decomposition* of G into complete bipartite subgraphs is defined in the same way as is done for the complete graph K_n above. Let $G_1, \ldots, G_m$ be the complete bipartite subgraphs in a decomposition of G. Let P_j and Q_j be the two "parts" in G_j, $1 \leq j \leq m$. Let p_j and q_j be the characteristic (column) vectors of P_j and Q_j respectively in $\mathbb{R}^n$ (where we identify the vertex set of G with $[n]$ in some arbitrarily fixed way).

Let A be the adjacency matrix of G and A_j that of G_j, $1 \leq j \leq n$. We have:

- $A = A_1 + \cdots + A_m$ (because $G_1, \ldots, G_m$ form a decomposition of G)
- $A_j = p_j q_j^t + q_j p_j^t$

2.5. **Proof by Twerberg, 1982.** Take G to be the complete graph K_n on n vertices. By way of contradiction, suppose that $m < n-1$. Let p denote the element of $\mathbb{R}^n$ each of whose components is 1. Consider the subspace $V := \{v \in \mathbb{R}^n \mid p^t v = 0,\ p_j^t v = 0\ \forall\ 1 \leq j \leq m\}$. By our hypothesis on m, it follows that $V \neq 0$.

Choose $v \neq 0$ in V. Let $v_1, \ldots, v_n$ be the components of v. Then:

- On the one hand, $v^t v = v_1^2 + \cdots + v_n^2 \neq 0$ (since $v \neq 0$).

- On the other, $v^t v = (v_1 + \cdots + v_n)^2 - 2\sum_{1 \le r < s \le n} v_r v_s$. Observe that $v_1 + \cdots + v_n = p^t v$ and that $\sum_{1 \le r < s \le n} v_r v_s = \sum_{j=1}^{m} (p_j^t v) \cdot (q_j^t v)$ (since $G_1, \ldots, G_m$ form a decomposition of K_n). Since $p^t v = p_j^t v = 0$ by choice of v, we conclude that $v^t v = 0$.

We thus have a contradiction, and the proof is complete. □

2.6. **Proof by Peck, 1983.** Take G to be the complete graph K_n on n vertices. Then $I_n + A = J_n$, where I_n is the $n \times n$ identity matrix, A is the adjacency matrix of G, and J_n is the $n \times n$ matrix all of whose entries are 1. Since $A = A_1 + \cdots + A_m$ (as observed above), we have $I_n + (A_1 + \cdots + A_m) = J_n$.

Write $A_j = p_j q_j^t + q_j p_j^t = 2 p_j q_j^t + S_j$, where $S_j := q_j p_j^t - p_j q^t$. Note that S_j is real skew-symmetric. Substituting for A_j into $I_n + (A_1 + \cdots + A_m) = J_n$, and rewriting we obtain:

$$I_n + (S_1 + \cdots + S_m) = J_n - 2\sum_{j=1}^{m} p_j q_j^t$$

The left hand side is an invertible matrix since $S_1 + \cdots + S_m$ is real skew-symmetric (see item (3) in §5). Each of the $m + 1$ terms on the right hand side has rank 1. Thus a necessary condition for the ranks of the two sides to be equal is that $m + 1 \ge n$, or $m \ge n - 1$ (see item (1) in §5).

2.7. **Proof via Witsenhausen's theorem, 1980s.** The following theorem about decompositions of a general graph contains the Graham-Pollak theorem as a special case:

Theorem 4. (WITSENHAUSEN, 1980S) *The number of complete bipartite graphs in any decomposition of a graph G is at least the number of positive eigenvalues of the adjacency matrix of G. (It is also at least the number of negative eigenvalues.)*

The eigenvalues of the adjacency matrix of the complete graph K_n are $n - 1$ and -1, the latter repeated $n - 1$ times (see item (4) in §5). Thus the Graham-Pollak theorem follows as an immediate consequence.

PROOF: (OF THEOREM 4) We introduce two subspaces U and W of $\mathbb{R}^n$:

- U is the span of all eigenspaces of the adjacency matrix A of G corresponding to positive eigenvalues. The dimension of U equals the number of positive eigenvalues of A, since A being real symmetric is diagonalizable over the reals by the spectral theorem.
- We define $W := \{w \in \mathbb{R}^n \mid p_j^t w = 0 \ \forall\ 1 \le j \le m\}$. Clearly $\dim W \ge n - m$.

The key observation of the proof is the following claim: $U \cap W = 0$. Before we prove the claim, let us see how the proof is finished once we have it. It follows from the claim that $\dim U + \dim W \le n$, which means $n - m \le \dim W \le n - \dim U$, or $m \ge \dim U$, which gives us the theorem.

It only remains to prove the claim that $U \cap W = 0$. This in turn follows from the following two claims:

- $u^t A u > 0$ for $u \in U$: Write $u = \lambda_1 u_1 + \cdots + \lambda_s u_s$, where the u_i are pairwise orthogonal eigenvectors corresponding to positive eigenvalues λ_i (respectively) for A. (Such vectors u_i exist by the spectral theorem.) We have $u^t A u = \lambda_1 u_1^t u_1 + \cdots + \lambda_s u_s^t u_s > 0$.
- $w^t A w = 0$ for $w \in W$: It is enough to show $w^t A_j w = 0$ for $w \in W$ and $1 \leq j \leq n$ (since $A = A_1 + \cdots + A_m$). But $w^t A_j w = w^t (p_j q_j^t + q_j p_j^t) w = (p_j^t w)^t q_j + q_j (p_j^t w) = 0$. □

3. (Balanced Incomplete) Block Designs and Fisher's Inequality

The theory of *block designs* was developed by Fisher and Yates in the 1930s motivated by applications to the design of experiments in agriculture. It has since found other uses, e.g., in software testing.

3.1. **Definition of a BIBD.** A *balanced incomplete block design*, *BIBD* for short, consists of the following data:

- A finite set called the *vertex set*, whose elements are called *vertices*; the cardinality of this set is denoted v.
- A collection of subsets of vertices, each subset being called a *block*; the blocks all have the same cardinality, denoted k. (Caveat: blocks could be *repeated*, that is, the same subset of the vertex set may appear as a block multiple times.) We assume that $k \geq 2$.
- (*Axiom of balancedness*) For every pair of vertices, the number of blocks containing both is the same, this being denoted λ. Note that $\lambda \geq 1$ since $k \geq 2$.
- (*Axiom of incompleteness*) $v > k$, or, in other words, the whole vertex set is not a block.

To draw attention to the integers v, k, and λ, the above data set is also called a (v, k, λ)-BIBD.

3.2. **Some examples of BIBDs.** An easy example of a BIBD is obtained by taking all subsets of the vertex set of a given cardinality $k \geq 2$ to be blocks. The λ in this case is $\binom{v-2}{k-2}$.

3.2.1. The projective planes. Here is a more interesting family of examples, called the *projective planes*. Let $\mathbb{F}$ be a finite field and T the $\mathbb{F}$-vector space formed by 3-tuples of elements of $\mathbb{F}$. Take the vertex set V to consist of lines (i.e., 1-dimensional subspaces) of T. The blocks are parametrized by 2-dimensional subspaces of T. A vertex belongs to a block if the line it represents belongs to the 2-dimensional subspace the block is indexed by.

Denoting by q the number of elements of $\mathbb{F}$, we have in this case:

$$v = \frac{q^3 - 1}{q - 1} = q^2 + q + 1, \qquad k = q + 1, \qquad \lambda = 1. \tag{2}$$

3.2.2. The Fano plane. Consider the special case of the above construction when $\mathbb{F}$ is the field of 2 elements. Called the FANO PLANE, it is a $(7, 3, 1)$-BIBD. Each line of T has in this case a unique non-zero element and so we may identify the vertices with the non-zero elements of T. A picture of the Fano plane is drawn below. The six straight lines and the circle represent the blocks.

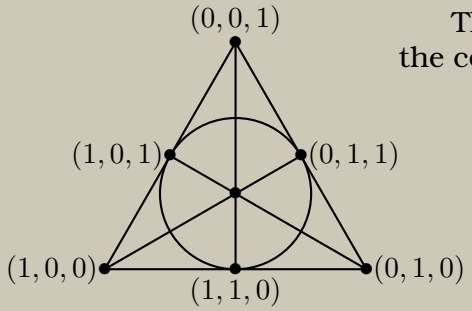


FIGURE 3.1. The Fano plane

3.3. **The incidence matrix M.** It is convenient to associate an *incidence matrix* M to a BIBD. The rows of M are indexed by the vertices, the columns by the blocks. Each entry of M is either 1 or 0 depending upon whether or not the vertex corresponding to the row of the entry belongs to the block corresponding to column of the entry.

Each column-sum of M is clearly k (by the second item in the definition above of BIBD). As we will presently show, the row-sums of M are all the same and equal to the "replication number".

3.4. **The replication number r.** Given a vertex x, let r_x denote the number of blocks to which x belongs. Consider the set

$$R_x := \{(y, A) \mid \quad y \text{ vertex}, y \neq x; \quad A \text{ block}; \quad \text{both } x, y \text{ belong to } A\}$$

What is the cardinality of R_x? We can reckon it in two different ways:

- there are $v - 1$ choices for y and, for each such choice, there are λ choices for A.
- there are r_x choices for A and, for each such choice, there are $k - 1$ choices for y.

Equating the resulting two expressions for the cardinality of R_x, we obtain:

$$r_x(k - 1) = \lambda(v - 1) \qquad \text{or} \qquad r_x = \frac{\lambda(v - 1)}{k - 1} \tag{3}$$

Thus r_x is the same for all vertices x. It is denoted r and called the *replication number*. Each row-sum of the incidence matrix M clearly equals r.

3.5. **The number b of blocks.** We denote by b the number of blocks in a BIBD. Equating the sum of the row-sums with the sum of the column-sums of the incidence matrix M, we obtain $vr = bk$. Substituting for r from (3) we get:

$$b = \frac{\lambda v(v-1)}{k(k-1)} \tag{4}$$

3.6. **Constraints on (v, k, λ).** The fact that r and b, given respectively by (3) and (4), are integers obviously imposes two constraints on the possible values of (v, k, λ) of BIBDs (see item (2) in §6). Fisher's inequality, discussed in §3.7 below, imposes yet another constraint: $b \geq v$.

These three constraints are however not sufficient to guarantee that a triplet (v, k, λ) arises from a BIBD. For instance, $(43, 7, 1)$ satisfies all three—we get $r = 7$ and $b = 43$—but nevertheless it is known that there is no $(43, 7, 1)$-BIBD (see item (7) in §6).

A characterization of the set of values (v, k, λ) of BIBDs is not yet known. It is a basic and difficult open problem. We don't even know whether or not there exists a $(22, 8, 4)$-BIBD.

3.7. **Fisher's Inequality.** This basic inequality states the following:

(5) In any BIBD, the number b of blocks is at least the number v of vertices: $b \geq v$

PROOF: The columns of the incidence matrix M are elements of $\mathbb{R}^v$. There being b of these, it is enough to show that they span $\mathbb{R}^v$. We write out explicit expressions for each of the standard basis vectors e_j of $\mathbb{R}^v$, $1 \leq j \leq v$, as linear combinations of the columns of M.

Since each row-sum of M equals r, addition of all the columns of M equals

$$r(e_1 + \ldots + e_v) \tag{6}$$

Fix j, $1 \leq j \leq v$. Addition of those columns whose entry in row j is 1 equals (by the axiom of balancedness):

$$\lambda(e_1 + \cdots + e_v) + (r - \lambda)e_j \tag{7}$$

By (3) and the incompleteness axiom (and the fact that $\lambda \geq 1$), we have $r = \lambda(v-1)/(k-1) > \lambda$, and in particular $r - \lambda \neq 0$. We may thus express e_j as a linear combination of the vectors in (6) and (7):

$$e_j = \frac{1}{(r-\lambda)} \cdot ((e_1 + \cdots + e_v) + (r - \lambda)e_j) - \frac{1}{r(r-\lambda)} \cdot (r(e_1 + \cdots + e_v)) \tag{8}$$

The vectors in (6) and (7) being linear combinations of columns of M, we conclude that each e_j and hence all of $\mathbb{R}^v$ is contained in the column space of M. □

For a recasting of the above proof, see item (6) of §6.

4. Activity Set 1

(1) Let M be a matrix of size $m \times n$ each entry of which is either 0 or 1. Consider the rank of M as a matrix over the reals and its rank as a matrix over the field of two elements. What is the relationship between these two ranks?

(2) Observe that the standard bilinear form on $\mathbb{F}^n$ (where $\mathbb{F}$ is an arbitrary field) defined in §1.5 is non-degenerate. Recall that non-degeneracy of a symmetric bilinear form $(\ ,\ )$ means the following: if $(v, w) = 0$ for some $v \in \mathbb{F}^n$ and all $w \in \mathbb{F}^n$, then $v = 0$.

(3) Let V be a finite dimensional vector space with a symmetric bilinear form $(\ ,\ )$. For a subspace of W, define $W^\perp := \{v \in V \,|\, (v, w) = 0 \ \forall\ w \in W\}$. A subspace W is called *isotropic* if $W \subseteq W^\perp$.
   (a) Observe that $\dim W^\perp \geq \dim V - \dim W$ and that equality holds if the form is non-degenerate.
   (b) If the form is non-degenerate then any isotropic subspace has dimension at most $\dim V/2$ (and hence at most $\lfloor \dim V/2 \rfloor$).

(4) Construct on $\mathbb{R}^n$ various non-degenerate symmetric bilinear forms $(\ ,\ )_j$, one for each j, $1 \leq j \leq \lfloor \frac{n}{2} \rfloor$, such that the maximum dimension of an isotropic subspace with respect to $(\ ,\ )_j$ is exactly j.

(5) In a certain town there are n residents. They want to form clubs, subject to the following rules:
   - Each club has an odd number of members.
   - The number of members common to any two clubs is odd.
   - No two distinct clubs have the same set of members.

   What is the maximum number of clubs that they can form? (Hint: The answer is $2^{\lfloor (n-1)/2 \rfloor}$.)

(6) Let A_n be the $n \times n$ matrix whose diagonal entries are all 0 and off-diagonal entries are all 1. In other words, A_n is the adjacency matrix of the complete graph on n vertices. Consider A_n as a matrix over the field of 2 elements. Show that A_n is invertible for n even and of rank $n - 1$ for n odd. In which of these cases is it diagonalizable?

(7) In a certain town there are n residents. They want to form clubs, subject to the following rules:
   - Each club has an even number of members.
   - The number of members common to any two distinct clubs is odd.

   Note that it follows from these rules that no two distinct clubs have the same set of members. What is the maximum number of clubs that can be formed? (Hint: The answer is n for n odd and $n - 1$ for n even.)

(8) Let A be a $2n \times 2n$ real matrix. Suppose that all the diagonal entries of A are 0 and that every off-diagonal entry is either 1 or -1. Show that A is invertible.

5. Activity Set 2

The first three items are in the form of assertions. Prove them from first principles.

(1) $\operatorname{rank}(A_1 + \cdots + A_s) \leq \operatorname{rank} A_1 + \cdots + \operatorname{rank} A_s$ for matrices $A_1, \ldots, A_s$ of a fixed size.

(2) Let A be a $n \times n$ real skew-symmetric matrix.
   (a) The eigenvalues of A are all purely imaginary.
   (b) Two eigenvectors corresponding to distinct eigenvalues of A are orthogonal (with respect to the standard Hermitian inner product on $\mathbb{C}^n$).
   (c) The space of vectors orthogonal to a given eigenvector is invariant under the action of A.
   (d) There is a unitary matrix U such that U^*AU is diagonal with purely imaginary diagonal entries.

(3) If -1 is not an eigenvalue of an $n \times n$ matrix A, then $I_n + A$ is invertible (where I_n stands for the $n \times n$ identity matrix). In particular, $I_n + A$ is invertible if A is a real skew-symmetric matrix.

(4) Write down the adjacency matrix A_n of the complete graph K_n on n vertices and consider it as a matrix over the reals. What are the eigenvalues (with multiplicities) of A_n? What is the minimal polynomial of A_n? Identify a basis of $\mathbb{R}^n$ consisting of eigenvectors of A_n. (For a generalization, see (6b) in §6.)

(5) Write down the adjacency matrix of a complete bipartite graph (with p vertices in one part and q in the other). What is its rank? What are its eigenvalues (with multiplicities)? What are its characteristic and minimal polynomials? Can you find a basis for $\mathbb{R}^{p+q}$ consisting of a set of mutually orthogonal eigenvectors for it? (Compare with the statement of Witsenhausen's theorem.)

6. Activity Set 3

(1) Here is an alternate proof (without using (3)) that the number of blocks b in a BIBD is given by $b = \frac{\lambda v(v-1)}{k(k-1)}$. Consider a matrix whose rows are indexed by subsets of cardinality two of the vertex set and whose columns are indexed by the blocks, with each entry of the matrix being 1 or 0 depending upon whether the block corresponding to the column of the entry contains the subset corresponding to the row. The matrix has $\binom{v}{2}$ rows with each row-sum being λ. It also has b columns with each column-sum being $\binom{k}{2}$. Equating the sum of the row-sums to the sum of the column-sums leads to the given expression for b.

(2) Show that BIBDs with the following values of (v, k, λ) do not exist: $(8, 3, 1)$, $(19, 4, 1)$.

(3) Construct explicitly BIBDs with the following values of (v, k, λ): $(3, 2, 1)$, $(4, 2, 1)$.

(4) Show that a $(25, 10, 3)$-BIBD does not exist.

(5) Equation (2) gives the values of v, k, and λ for a projective plane in terms of the cardinality q of the finite field. Prove their correctness. Express r and b too in terms of q.

(6) The proof of Fisher's inequality in §3.7 may be recast in the following terms. Notation is as in §3.

(a) $MM^t = (r - \lambda)I_v + \lambda J_v$, where I_v is the identity matrix of size $v \times v$ and J_v is the matrix of size $v \times v$ all of whose entries are 1.

(b) $(r-\lambda)I_v + \lambda J_v$ has eigenvalues $r - \lambda$ with multiplicity $v - 1$ and $r + (v-1)\lambda$ with multiplicity one. In particular, it is non-singular.

(c) It follows from the two observations above that MM^t has rank v, and so $b \geq v$.

(7) We state without proof the following result (Bruck-Ryser-Chowla theorem) using which it can be shown that a $(43, 7, 1)$-BIBD does not exist. For a (v, k, λ)-BIBD with $v = b$ to exist, the following conditions are necessary: if v is even, then $k-\lambda$ is the square of an integer; if v is odd, then the equation $z^2 = (k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$ has a non-trivial solution in the integers. (Hint: Suppose that a $(43, 7, 1)$-BIBD exists. Then, by the theorem, there exists a non-trivial solution in the integers to $z^2 + y^2 = 6x^2$. By canceling common factors, we may assume that there is a solution in which the integers x, y, z have no common prime factor. Fix such a solution. Then $3|(z^2+y^2)$, so $3|z^2$ and $3|y^2$, and so also $3|z$ and $3|y$. Put $z = 3z'$, $y = 3y'$. We have $9z'^2 + 9y'^2 = 6x^2$, or $3z'^2 + 3y'^2 = 2x^2$, so $3|x$. Thus 3 divides each of x, y, z, a contradiction to our choice of x, y, z.)