Linear algebra methods in combinatorics

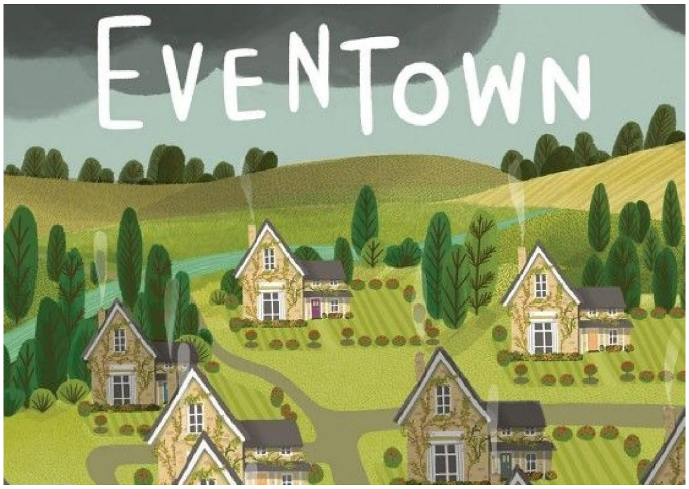
Henk D.L. Hollmann

email: henk.hollmann@ut.ee

(For hints and further help with the problems, you may contact the author)

18 March 2022

1 Introduction: Eventown and Oddtown



The small town Eventown has precisely 2014 inhabitants, half of which are male. They are quite a social bunch and like to form clubs, however, they have to obey the rules for club forming set by the Major of Eventown, which are

1 A club must have an *even* number of members.

2 Any two distinct clubs must share an *even* number of members.

Under these rules, many clubs can be formed. Any idea what is the maximum possible number of (distinct) clubs?

The towners felt great social pressure to form the maximum possible number of clubs, and to be active in them. After many socially very taxing years, the inhabitants (still the same number, since they had been too busy to make children) revolted. They wanted FEWER clubs! After a short trial, the major was executed, and the town was renamed Oddtown. Then the club-forming rules were slightly amended, in particular, rule 1 was replaced by the rule

$1'$ A club must have an *odd* number of members.

(Rule 2 was still supposed to hold.) This new rules made the social lives of the remaining 2013 inhabitants of the town now named Oddtown much less stressful. Do you know *how* less stressful exactly, that is, can you say how many clubs could now maximally be formed?

In due time, the new club rules were boring everybody to dead, and so new rules were sought to form clubs while keeping social life on an acceptable level. Another drawback of both the old and the new club rules was that different clubs often had no idea of each others activities. So after some experimentation, the following rule was adopted.

(a) Any two distinct clubs must share *precisely two* members;

(Rule (a) is now supposed to be the only rule; however no two clubs have exactly the same members.) Can you now guarantee the inhabitants that under this new club-forming rule, their lives will not get more involved as before?

In the next sections, we will develop some linear algebraic tools to solve combinatorial problems like those above.

2 Basics on linear algebra

Let $\mathbb{F}$ be a field, for example $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or a finite field such as $\mathbb{F}_p$, the field of integers molulo a prime p. We write $\mathbb{F}^n$ to denote the vector space of dimension n over $\mathbb{F}$; we denote the set of $n \times m$ matrices with entries from $\mathbb{F}$ by $\mathcal{M}_{\mathbb{F}}(n, m)$.

For $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}^n$, their *inner product* (or *dot-product*) $(\boldsymbol{x}, \boldsymbol{y})$ is defined as

$$(\boldsymbol{x}, \boldsymbol{y}) = \boldsymbol{x}^\top \boldsymbol{y} = \sum_{i=1}^{n} x_i y_i.$$

If V is a subspace of $\mathbb{F}^n$, then the *orthogonal complement* $V^\perp$ is defined as

$$V^\perp = \{\boldsymbol{x} \in \mathbb{F}^n \mid (\boldsymbol{x}, \boldsymbol{v}) = 0 \text{ for all } \boldsymbol{v} \in V\}.$$

the *orthogonal complement* of V. If V is a subspace of a vector space U, then

$$V^{\perp_U} = \{\boldsymbol{x} \in U \mid (\boldsymbol{x}, \boldsymbol{v}) = \boldsymbol{0} \text{ for all } \boldsymbol{v} \in V\}$$

If V, W are two subspaces of $\mathbb{F}^n$, then

$$V + W = \{\boldsymbol{v} + \boldsymbol{w} \mid \boldsymbol{v} \in V, \boldsymbol{w} \in W\}.$$

We will write $\boldsymbol{0}_n$ is the all-zero vector $(0, \ldots, 0)^\top$, and $\boldsymbol{O}_n$ or $\boldsymbol{O}_{n,m}$ to denote the $n \times n$ or $n \times m$ all-zero matrix. Similarly, we write $\boldsymbol{j}_n$ to denote the all-one vector $(1, 1, \ldots, 1)^\top$ of size n, and $\boldsymbol{J}_n$ or $\boldsymbol{J}_{n,m}$ to denote the all-one matrix of size $n \times n$ or size $n \times m$. We let $\boldsymbol{I}_n$ denote the identity matrix $\operatorname{diag}(\boldsymbol{j}_n)$ of size $n \times n$. We simply write $\boldsymbol{0}$, $\boldsymbol{j}$, $\boldsymbol{O}$, $\boldsymbol{J}$, and $\boldsymbol{I}$ if the dimensions are clear from the context.

Basics on linear algebra - part 1

Some useful properties of matrices and vector spaces, valid for **all** fields, are the following.

- The *dimension* $\dim(V)$ of a vector space V is the largest number n for which there is a collection of n (linearly) independent vectors in V. A set of $\dim(V)$ independent vectors in V is called a *basis* of V. Any set of $n+1$ vectors $\boldsymbol{v}_0, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ in an n-dimensonal vector space over a field $\mathbb{F}$ is *dependent*, that is, there are $\lambda_0, \dots, \lambda_n$ in $\mathbb{F}$, *not all zero*, such that $\lambda_0\boldsymbol{v}_0 + \cdots + \lambda_n\boldsymbol{v}_n = \mathbf{0}$. If there are k independent vectors in an n-dimensional vector space, then $k \leq n$.

  Note that the dimension cannot go down by enlarging the field (see the later item on determinants).

- Let V be a (finite) vector space over some finite field $\mathbb{F} = \mathbb{F}_p$. Let $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ be a basis for V. Then $\dim(V) = n$, and V consists of all vectors of the form

  $$\lambda_1\boldsymbol{e}_1 + \cdots + \lambda_n\boldsymbol{e}_n$$

  with $\lambda_1, \dots, \lambda_n \in \mathbb{F}$; in particular, $|V| = |\mathbb{F}|^{\dim(V)} = q^n$ if $\mathbb{F} = \mathbb{F}_q$ is a finite field of size q.

Incidence vectors

Important method: If we have $n+1$ vectors in an n-dimensional vector space, then these vectors must be *dependent*.

This method has many applications. We give some examples.

Problem 1 Let $M_1, \dots, M_{n+1}$ be $n+1$ non-empty subsets of $\{1, \dots, n\}$. Show that there are disjoint non-empty sets $I, J \subseteq \{1, \dots, n+1\}$ of indices such that

$$\bigcup_{k\in I} M_k = \bigcup_{k\in J} M_k.$$

In order to apply the method, we need vectors and a vector space. In the next section, we explain how these are obtained.

Given a finite set V and a subset $S \subseteq V$, we can encode the information which elements of V are contained in S and which are not with the aid of a vector, in the following way. First, we *number* the elements of V, say $V = \{v_1, \dots, v_n\}$. Now, we define a vector $\boldsymbol{\chi}_S$ by letting

$$\boldsymbol{\chi}_S(i) = \begin{cases} 1, & \text{if } v_i \in S; \\ 0, & \text{if } v_i \notin S. \end{cases}$$

In other words, the positions in the 0-1 vector $\boldsymbol{\chi}_S$ are indexed with the set V, and there is a 1 in the positions whose index is contained in S. The vector $\boldsymbol{\chi}$ is called the *characteristic vector* or *incidence vector* of S. We may consider these vectors as *real* or *complex* vectors, but also as vectors over a *finite* field $\mathbb{F}_p$ if we like; indeed, *every* field $\mathbb{F}$ contains 0 and 1! Let us use incidence vectors to solve Problem 1.

Solution: Let $\boldsymbol{\chi}_i$ $(1 \leq i \leq n+1)$ denote the incidence vector of the subset $M_i \subseteq \{1, \dots, n\}$, considered as rational vectors. Since we have $n+1$ vectors $\boldsymbol{\chi}_i$ in the n-dimensional vector space $\mathbb{Q}^n$, these vectors must be dependent. So there are are rational numbers $\lambda_i, \dots, \lambda_{n+1}$ in $\mathbb{Q}$ such that

$$\lambda_1\boldsymbol{\chi}_1 + \lambda_2\boldsymbol{\chi}_2 \cdots + \lambda_{n+1}\boldsymbol{\chi}_{n+1} = 0.$$

As often, this reformulation in terms of vectors is half of the work, but some work remains! Here comes the trick: let $I = \{i_1, \dots, i_r\}$ denote the set of indices i for which $\lambda_i > 0$ and let $J = \{j_1, \dots, j_s\}$ denote the set of indices j for which $\lambda_j < 0$ (we forget about indices for which $\lambda_i = 0$). Then we have that

$$\lambda_{i_1}\boldsymbol{\chi}_{i_1} + \cdots + \lambda_{i_r}\boldsymbol{\chi}_{i_r} = (-\lambda_{j_1})\boldsymbol{\chi}_{j_1} + \cdots + (-\lambda_{j_s})\boldsymbol{\chi}_{j_s}.$$

Now, for every $v \in V$, the vector on the left-hand side of the above equation is nonzero (hence positive!) in position v if and only if one of the vectors $\boldsymbol{\chi}_i$ is 1 in position v, that is , if and only if $v \in \cup_{i \in I} S_i$; similarly, the vector on the right-hand side is nonzero in position v if and only if $v \in \cup_{i \in J} S_j$. We conclude that $\cup_{i \in I} S_i = \cup_{i \in J} S_j$. □

(For a slightly more complicated case, see Problem 15.)

Next, another example. A *simple graph* is a pair $G = (V, E)$ and consists of a (finite) set V of *vertices* and a set of *edges* $E \subseteq \binom{V}{2}$; so every edge $e \in E$ is a pair $e = \{v, w\}$ of two vertices $v, w \in V$; we say that e *joins* the vertices v and w. Vertices joined by an edge are called *neighbours* and are said to be *adjacent*. A vertex v and an edge e are said to be *incident* if v is contained in e. The *degree* $d(v)$ of a vertex v is the number of edges that contain v. A *subgraph* of G is a pair $(U, F$ with $U \subseteq V$, $F \subseteq E$ such that if $e = \{v, w\} \in F$, then $v, w \in U$. the subgraph *induced* by a set of vertices $U \subseteq V$ is the pair (U, F) where F is the set of all edges joining two vertices in U; similarly, the subgraph induced by a set of edges $F \subseteq E$ is the pair (U, E) where U is the set of vertices incident with edges in'F. A *cycle* in G is a set of edges $e_0 = \{v_0, v_1\}, e_1 = \{v_1, v_2\}, \dots, e_{m-1} = \{v_{m-1}, v_0\}$ where $v_0, \dots, v_{m-1}$ are distinct vertices.

With every edge e, considered as a subset of V, we associate its incidence vector $\boldsymbol{\chi}_e$. Now we think of the vectors $\boldsymbol{\chi}_e$ as being vectors *in* $\mathbb{F}_2$, so (the vectors associated with) edges are elements in $\mathbb{F}_2^{|V|}$. In what follows, we do not distinguish between an edge e and the corresponding vector $\boldsymbol{\chi}_e \in \mathbb{F}_2^{|V|}$, that is, we identify an edge e with its corresponding vector $\boldsymbol{\chi}_e$. If C is a cycle, then every vertex on the cycle is contained in precisely two edges; so the edges in a cycle are *dependent* in $\mathbb{F}_2^{|V|}$. Obviously, if F is a set of edges that sum to the zero vector, then the subgraph induces by F forms an *even* subgraph, that is, all of its vertices are incident with an *even* number of edges in F. Such a subgraph obviously contains a cycle. Briefly, the edges of G span a subspace of $\mathbb{F}_2^{|V|}$ called the *cycle space*, a subspace of dimension $|V| - 1$; the minimal dependent sets are the cycles; every spanning tree is a basis for the cycle space, and every set of edges of size $|V|$ is dependent and therefore contains a cycle.

We can use these graph dimension ideas to solve the next problem.

Problem 2 Consider an $n \times m$ array. A subset S of the nm cells is called *even* if every row and every column contains an even number of cells of S. Find the smallest positive integer k with the property that every set of k cells contains an even subset.

Solution: With the array, we associate the complete bipartite graph $G = K_{n,m}$: the set of vertices consists of the union of the set of rows and the set of columns of the array, and a cell in position (r, c) corresponds to an edge between row r and column c. Now a set S of cells consists of a number of edges in the graph G, and S is even precisely when each vertex (rows and columns) contain an even number of edges (cells) from S. A subset of the cells is even precisely when the sum of the incidence vectors of the edges corresponding to S sum to the zero vector. In other words, using the terminology and ideas above, if a subset S is even, then it is dependent, and the number k such that every set S contains an even subset is just 1 plus the dimension of the cycle space of the graph G. Since G has $n + m$ vertices, the dimension is $n = m - 1$ and so the answer is $k = n + m$. □

Basics on linear algebra - part 2

In what follows, we list some further useful properties of matrices and vector spaces that are valid for all fields (with one exception).

- If $\boldsymbol{M}$ is an $n \times m$ matrix over some field $\mathbb{F}$, then the *rowspace* row$(\boldsymbol{M})$ of $\boldsymbol{M}$, the subspace of $\mathbb{F}^m$ spanned by the *rows* of $\boldsymbol{M}$, and the *columnspace* col$(\boldsymbol{M})$ of $\boldsymbol{M}$, the subspace of $\mathbb{F}^n$ spanned by the *columns* of $\mathbb{F}$, have the *same* dimension. This common dimension is called the *rank* of $\boldsymbol{M}$, and is denoted by rank$(\boldsymbol{M})$. In particular, rank$(\boldsymbol{M}^\top) =$ rank$(\boldsymbol{M})$ and rank$(\boldsymbol{M}) \leq \min(m, n)$.

  Equality of row rank and column rank is usually shown with the aid of the reduced row-echelon form. The following very short proof is also valid for every field: If $\boldsymbol{M} = \boldsymbol{O}$, then the row and column rank of $\boldsymbol{M}$ are both 0; otherwise, let r be the smallest positive integer such that there is an $n \times r$ matrix $\boldsymbol{A}$ and an $r \times m$ matrix $\boldsymbol{B}$ satisfying $\boldsymbol{M} = \boldsymbol{AB}$. Thus the r rows of $\boldsymbol{B}$ form a minimal spanning set of the row space of $\boldsymbol{M}$ and the r columns of $\boldsymbol{A}$ form a minimal spanning set of the column space of M. Hence, row and column ranks are both r. (Homework: supply the missing details.)

- The *null space* null($\boldsymbol{M}$) (or *kernel*) of $\boldsymbol{M}$ is the collection of all $\boldsymbol{x} \in \mathbb{F}^m$ such that $\boldsymbol{Mx} = 0$. Obviously, $\text{null}(\boldsymbol{M}) = \text{row}(\boldsymbol{M})^\perp$.

- If V is a subspace of a vector space U, then $\dim(V) + \dim(V^\perp) = \dim(U)$. In particular, if $V \subseteq \mathbb{F}^n$, then $\dim(V) + \dim(V^\perp) = n$. But watch out: in fields like $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, we know that since $\boldsymbol{x}^\top \boldsymbol{x} = 0$ implies $\boldsymbol{x} = \boldsymbol{0}$, we have $V \cap V^\perp = \{0\}$. But this need not be true for other fields; in particular, in *finite fields* this is *false*. For example, over a field of characteristic p such as $\mathbb{F}_p = \mathbb{Z}_p$, we have for $\boldsymbol{v} = j = (1, 1, \ldots, 1)^\top$ that $\boldsymbol{v}^\top \boldsymbol{v} = (\boldsymbol{v}, \boldsymbol{v}) = p = 0$. For $V = \{\boldsymbol{0}, (1,1)^\top\} \subseteq \mathbb{F}_2^2$, we have $V^\top = V$, both of dimension 1.

- Since $\text{null}(\boldsymbol{AB}) \supseteq \text{null}(\boldsymbol{B})$, we have that $\text{rank}(\boldsymbol{AB}) \leq \min(\text{rank}(\boldsymbol{A}), \text{rank}(\boldsymbol{B}))$, see Theorem 2.1 below for a proof. (Try for yourself first!)

- It is easily seen that $\text{col}(\boldsymbol{A} + \boldsymbol{B}) \subseteq \text{col}(\boldsymbol{A}) + \text{col}(\boldsymbol{B})$; consequently, $\text{rank}(\boldsymbol{A} + \boldsymbol{B}) \leq \text{rank}(\boldsymbol{A}) + \text{rank}(\boldsymbol{B})$.

- An $n \times m$ matrix $\boldsymbol{M}$ is invertible if and only if $m = n = \text{rank}(\boldsymbol{M})$. A square matrix $\boldsymbol{M}$ over a field $\mathbb{F}$ is invertible if and only if $\boldsymbol{Mx} = 0$ implies that $\boldsymbol{x} = \boldsymbol{0}$.

- If $\boldsymbol{M}$ is a real $n \times m$ matrix , then $\det(\boldsymbol{M}^\top \boldsymbol{M}) \geq 0$, with equality iff $\text{rank}(\boldsymbol{M}) < m$. A matrix of the form $\boldsymbol{M}^\top \boldsymbol{M}$ is called a *Gram* (or *Gramian*) matrix. (Homework: show this by using the results above.)

- [Dimension Theory, Rank-nullity Theorem] If $f : V \to W$ is a linear map from the vector space V into the vector space W, then

  $$\dim(V) = \dim(\ker(f)) + \dim(\text{range}(f)).$$

  Here $\ker(f) = \{\boldsymbol{v} \in V \mid f(\boldsymbol{v}) = 0\}$, so that $\dim(\ker(f)) = \text{nullity}(f)$. Another important result is that if $\dim(V) = \dim(W)$, then the three conditions (i) f is onto; (ii) f is 1-1; and (iii) $\text{rank}(f) = \dim(W)$; are all equivalent.

  By viewing an $n \times m$ matrix $\boldsymbol{M}$ as a linear map $\boldsymbol{M} : x \to \boldsymbol{Mx}$ from $V = \mathbb{F}^m$ to $W = \mathbb{F}^n$, we obtain the important result that

  $$\text{rank}(M) + \text{nullity}(M) = m.$$

The next result is often used

Theorem 2.1 *If $\boldsymbol{B}$ is $m \times n$ and $\boldsymbol{A}$ is $k \times m$, then* $\text{rank}(\boldsymbol{AB}) \leq \min(\text{rank}(\boldsymbol{A}), \text{rank}(\boldsymbol{B}))$.

Proof. First, $\text{range}(\boldsymbol{AB}) \subseteq \text{range}(\boldsymbol{A})$, hence $\text{rank}(\boldsymbol{AB}) \leq \text{rank}(\boldsymbol{A})$. Then $\text{null}(\boldsymbol{B}) \subseteq \text{null}(\boldsymbol{AB})$, hence $\text{nullity}(\boldsymbol{B}) \leq \text{nullity}(\boldsymbol{AB})$. Now $\text{nullity}(\boldsymbol{B}) + \text{rank}(\boldsymbol{B}) = \text{nullity}(\boldsymbol{AB}) + \text{rank}(\boldsymbol{AB}) = n$, so $\text{rank}(\boldsymbol{AB}) \leq \text{rank}(\boldsymbol{B})$. □

Incidence and adjacency matrices

Let $\mathcal{P}$ be a finite set (the elements of which will be referred to as *points*), and let $\mathcal{B}$ be a collection of subsets of $\mathcal{P}$, referred to as *blocks* or *lines*. For each $B \in \mathcal{B}$, the points in B are the points *incident* to B. We say that two points are *adjacent* if they are contained together in some block. In such a situation, we can form two matrices describing the relations between points and blocks. The *incidence matrix* is the $|\mathcal{P}| \times |\mathcal{L}|$ matrix $\boldsymbol{M}$ defined by

$$\boldsymbol{M}(P,B) = \begin{cases} 1, & \text{if } P \in B; \\ 0, & \text{otherwise.} \end{cases}$$

In other words, the columns of the incidence matrix $\boldsymbol{M}$ are the *characteristic vectors* or *incidence vectors* of the blocks.

The *adjacency matrix* is the $|\mathcal{P}| \times |\mathcal{P}|$ matrix $\boldsymbol{A}$ defined by letting $\boldsymbol{A}(P,Q)$ to be the number of blocks $B \in \mathcal{B}$ for which $P, Q \in B$. We note that

$$\boldsymbol{A} = \boldsymbol{M}\boldsymbol{M}^\top,$$

hence the determinant of the adjacency matrix (considered as a real matrix) is nonnegative. Another interesting matrix to consider is the *block intersection* matrix $\boldsymbol{N} = \boldsymbol{M}^\top \boldsymbol{M}$; here for any two blocks B, B', the corresponding entry is $\boldsymbol{N}(B,B') = |B \cap B'|$, the size of the intersection of the blocks B and B'. (In fact, the block intersection matrix is the adjacency matrix of the *dual* configuration obtained by interchanging the roles of "points" and "blocks".)

Sometimes, the notion of a "block" is not present in the problem statement and has to be devised. For example, if the problem mentions a "friendship" relation (or any other binary symmetric relation), then as blocks we can take pairs of friends. If the problem is modeled as a graph, then the blocks are the edges of the graph. Also, a "club" can be a block!

Many combinatorial problems can be solved by describing the problem data in terms of suitable incidence matrices and vectors, and then considering these matrices and vectors over a *suitable field*. As an example, consider the following.

Problem 3 *Let $\mathcal{F}$ be a collection of $n+1$ distinct triples from $\{1, \ldots, n\}$, that is, $\mathcal{F} \subseteq \binom{[n]}{3}$. Show that there are two triples in $\mathcal{F}$ that intersect in precisely one element.*

Solution: Let $\boldsymbol{M}$ be the $n \times (n+1)$ incidence matrix of points versus triples. Suppose that no triples intersect in precisely one element; then any two distinct triples intersect in 0 or 2 elements. So if we consider $\boldsymbol{M}$ as a matrix over $\mathbb{F}_2$, then $\boldsymbol{M}^\top \boldsymbol{M} = \boldsymbol{I}_{n+1}$. However, $\operatorname{rank}(\boldsymbol{M}^\top \boldsymbol{M}) \le \operatorname{rank}(\boldsymbol{M}) \le n$, a contradiction. □

Often, finding the correct algebraic reformulation is only half of the work (or even only a tiny part!). To illustrate, consider this problem.

Problem 4 Show that we can color the vertices of any finite simple graph with two colors, red and blue, such that

1. Each red vertex is adjacent to an *even* number of red vertices;
2. Each blue vertex is adjacent to an *odd* number of red vertices.

I leave it as homework to find out that the correct matrix reformulation of the problem is:

> If $\boldsymbol{B}$ is an $n \times n$ symmetric matrix over $\mathbb{F}_2$ with all diagonal entries all equal to 1, then there is a vector $\boldsymbol{x} \in \mathbb{F}_2^n$ such that $\boldsymbol{Bx} = \boldsymbol{j}$, where $\boldsymbol{j}$ is the all-1 vector.

This happens to be true, but how to show this is far from evident! Howework: prove this!

Basics on linear algebra - part 3

Let S_n denote the collection of all permutations of $\{1, \ldots, n\}$. The *sign* of a permutation π is 1 or -1 depending on whether π can be written as a product of an even or an odd number of transpositions. [*Something needs a proof here!* **Exercise**: prove it! Hint: write a permutation as a product of disjoint cycles. Consider what happens if we multiply by a transposition.]

An $n \times n$ matrix $\boldsymbol{M}$ over a field $\mathbb{F}$ is invertible if and only if the determinant

$$\det(\boldsymbol{M}) = \sum_{\pi \in S_n} \operatorname{sign}(\pi) \prod_{i=1}^{n} M_{i,\pi(i)}$$

of $\boldsymbol{M}$ is nonzero. (The *permanent* $\operatorname{perm}(\boldsymbol{M})$ is the expression obtained by leaving out the signs; so over $\mathbb{F}_2$, the determinant and the permanent are equal.)

The determinant $\det(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ of a sequence of n vectors in $\mathbb{F}^n$ is the determinant of the matrix $\boldsymbol{V} = [\boldsymbol{v}_1 \cdots \boldsymbol{v}_n]$ that has the vectors as its columns. Note that the determinant is linear in each of its arguments. In particular, if $\boldsymbol{v}_i = \sum_j \lambda_{i,j} \boldsymbol{v}_{i,j}$ for $i = 1, \ldots, n$, then

$$\det(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = \sum_{j_1, \ldots, j_n} \left(\prod_k \lambda_{k,j_k} \right) \det(\boldsymbol{v}_{1,j_1}, \ldots, \boldsymbol{v}_{n,j_n}).$$

Sometimes it is possible to write the outcome of a counting problem on permutations as a determinant. Consider the following example.

Problem 5 A permutation σ on $\{1, \ldots, n\}$ is called *k-limited* if $|\sigma(i) - i| \leq k$ for all i. Show that the number of k-limited permutations on $\{1, \ldots, n\}$ is odd if and only if $n \equiv 0, 1 \bmod 2k + 1$.

Solution: First, we will work over $\mathbb{F}_2$ to get rid of the sign. Now we want to construct a matrix M such that a permutation contributes to the sum via the term $\prod_{i=1}^{n} M_{i,\sigma(i)}$ if and only if σ is k-limited, that is, if and only if $|i-\sigma(i)| \leq k$ for all i. we can achieve this by letting M be a 0-1 matrix with $M_{i,j} = 1$ precisely when $|i-j| \leq k$. So for example if $n = 5, k = 2$, we have

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

Now again, this is only half of the work. we leave it as homework to finish the solution by working out the value of the determinant. □

Basics on linear algebra - part 4

- We say that a set of vectors $V \subseteq \mathbb{F}^n$ is in *general position* if any n of the vectors of V are independent. (In that case, the null space of the matrix with as columns the vectors from V is said to be an *MDS code*.) Any collection of vectors

  $$\boldsymbol{v}(a) = (1, a, a^2, \ldots, a^{n-1})^\top$$

  ($a \in \mathbb{F}$) is in general position. This follows from the fact that the *Vandermonde determinant*

  $$\det(\boldsymbol{v}(a_1), \ldots, \boldsymbol{v}(a_n)) = \prod_{i<j} (a_j - a_i) \neq 0.$$

  (Homework: show this yourself, or look up a proof on the internet, if you do not know this. Hint: consider the a_i as variables, determine the degree of the outcome, and find out what happens if $a_i = a_j$.)

- Sometimes it can be profitable to consider polynomials or functions as vectors in a suitable vector space. For example, we may consider the collection of all polynomials of degree smaller than n with coefficients in some field $\mathbb{F}$ as a vector space over $\mathbb{F}$ with basis $1, x, \ldots, x^{n-1}$. The dimension of this vector space is n, provided that $\mathbb{F}$ is infinite or is finite of size at least n. If so, then $\mathbb{F}$ contains at least n distinct points $x_0, \ldots, x_{n-1}$, and hence $1, x, \ldots, x^{n-1}$ are indeed independent. (Homework: use a Vandermonde determinant to show this.) Note that in the field $\mathbb{F}_p$, we have that $a^p = a$ for every $a \in \mathbb{F}_p$; as a consequence, $x^p = x$ and the dimension of the space spanned by $1, x, \ldots, x^{n-1}$ is $\min(n, p)$.

> For another example, suppose that we have a set of maps $f_i : X \mapsto \mathbb{F}$ for $1 \leq i \leq n$ and distinct points $x_1, \dots, x_n$ in X. If $f_i(x_i) \neq 0$ and $f_i(x_j) = 0$ for $i \neq j$, then $f_1, \dots, f_n$ are independent. Indeed, if $s = \lambda_1 f_1 + \cdots + \lambda_n f_n = 0$, then $0 = s(x_j) = \lambda_j$ for $j = 1, \dots, n$. Again, this method requires the existence of enough distinct points in the field.

To illustrate this method, consider the following problem.

Problem 6 (Putnam 2003-B1) Do there exists (real) polynomials $a(x)$, $b(x)$, $c(x)$, $d(x)$ such that

$$1 + xy + x^2y^2 = a(x)b(y) + c(x)d(y)$$

holds identical?

Solution: The trick is to consider x as a variable, and y as some constant. If y runs through the reals, the right-hand side is contained in the at most 2-dimensional span of $a(x)$ and $b(x)$, so we are done if we can find three independent polynomials $1+xy+x^2y^2$ with $y \in \mathbb{R}$. But this is easy: taking $y = 0, 1, -1$, we get the polynomials $1, 1+x+x^2$, and $1-x+x^2$, which have the same span as $1, x, x^2$ and hence are independent. □

3 The town problems revisited

Let us consider the incidence matrix for the clubs in Even/Odd-town, considering the inhabitants as "points" and the clubs as "blocks". This incidence matrix is an $n \times m$ matrix $\boldsymbol{M}$, where n is the number of inhabitants (so $n = 2022$ here), and m is the number of clubs. It is easily seen that the club-forming rules of Eventown state that the $m \times m$ block-intersection matrix $\boldsymbol{M}^\top \boldsymbol{M}$ has even entries. In other words, if we consider the matrix $\boldsymbol{M}$ as a matrix over $\mathbb{F}_2$ (that is, modulo 2), then the condition is that over the field $\mathbb{F}_2$, we have that $\boldsymbol{M}^\top \boldsymbol{M} = \boldsymbol{O}_m$, the all-zero matrix. Let V the subspace of $\mathbb{F}_2^n$ spanned by the columns of $\boldsymbol{M}$, that is, by the characteristic vectors of the clubs. The condition $\boldsymbol{M}^\top \boldsymbol{M}$ implies that $V \subseteq V^\perp$, so we conclude that $2\dim(V) \leq n$, so that $\dim(V) \leq n/2$. The available columns for $\boldsymbol{M}$ are the vectors from V, of which there are $2^{\lfloor n/2 \rfloor}$. So we conclude that the number m of different possible clubs satisfies $m \leq 2^{\lfloor n/2 \rfloor}$ (or $2^{\lfloor n/2 \rfloor} - 1$ if we exclude the *empty* club as a possibility!). Hence with the given numbers, at most 2^{1011} clubs can be formed under rules 1 and 2. To see that this number of clubs can indeed be achieved, assume that the town inhabitants consist of $n/2$ married couples. now form clubs, but ensure that if a club has a member, the spouse is also member. In this way, we can obtain $2^{n/2}$ clubs; moreover, the intersection of any two clubs consists of a number of couples, so automatically is even.

After the revolution, the Oddtown club-forming rules state that $\boldsymbol{M}^\top \boldsymbol{M} = \boldsymbol{I}_n$ (modulo 2); so $\boldsymbol{M}$ has rank m and the number m of clubs satisfies $m \leq n$ (the columns of $\boldsymbol{M}$ must be independent in an n-dimensional space). Hence, given that $n = 2021$, at most 2021 clubs can now be formed. A possible solution is to form all 2021 possible *single-member* clubs.

Finally, suppose that any two clubs share exactly λ members (under rule (a), we have $\lambda = 2$). This problem is trickier, but can again be solved using incidence matrices for book-keeping, in combination with a bit of creativity! In terms of the $n \times m$ incidence matrix $\boldsymbol{M}$, now considered as a matrix over the *reals*, we have $\boldsymbol{M}^\top \boldsymbol{M} = \lambda(\boldsymbol{J}_m - \boldsymbol{I}_m) + \boldsymbol{K}$, where $\boldsymbol{K} = \mathrm{diag}(k_1, \ldots, k_m)$ with $k_i = |B_i|$, the size of the i-th block. Hence for any nonzero vector $\boldsymbol{x} \in \mathbb{R}^m$, we have

$$\|\boldsymbol{Mx}\|^2 = (\boldsymbol{Mx}, \boldsymbol{Mx}) = \boldsymbol{x}^\top \boldsymbol{M}^\top \boldsymbol{Mx} = \lambda \boldsymbol{x}^\top (\boldsymbol{J} - \boldsymbol{I}) + \boldsymbol{x}^\top \boldsymbol{K} x = \lambda \bigg(\sum_i x_i\bigg)^2 + \sum_i (k_i - \lambda) x_i^2.$$

Assume that there are at least two clubs. Then $k_i \geq \lambda$ for all i and since all clubs are supposed to be distinct, at most one club can have size λ [*why?*]; also, if $\sum_i x_i = 0$ but $\boldsymbol{x} \neq \boldsymbol{0}$, then at least two x_i are nonzero. We conclude that $\|\boldsymbol{Mx}\| > 0$, hence $\boldsymbol{Mx} \neq \boldsymbol{0}$ if $x \neq 0$; so $\boldsymbol{M}$ has rank m (no linear combination of the m columns of $\boldsymbol{M}$ is equal to $\boldsymbol{0}$) and so the number m of clubs again satisfies $m \leq n$. Hence, given that $n = 2021$, again at most 2021 clubs can be formed under rule (a).

[**Remark**: this proves *Fisher's inequality* for "block designs" with unequal blocksizes!]

4 More linear algebra problems

Problem 7 A town has $n \geq 1$ inhabitants, and by coincidence also has n clubs, each having an even number of members, with the additional property that every two distinct clubs have an odd number of common members. Show that the number of inhabitants is odd, and that for every odd number n such a town can exist. What can you say when the number of clubs m is not equal to n?

Problem 8 Let $X = \{1, 2, \ldots n\}$ and let $A_1, A_2, \ldots, A_n$ be distinct subsets of X. Show that there exists $x \in X$ such that the n sets $A_i \setminus \{x\}$ are again all distinct.

Problem 9 Students in a school go for ice cream in groups of at least two. After $k > 1$ groups have gone, every two students have gone together exactly once. Prove that the number of students in the school is at most k.

Problem 10 Let $A = (a_{k,\ell})_{k,\ell=1,\ldots,n}$ be an $n \times n$ complex matrix such that for each $m \in \{1, \ldots, n\}$ and $1 \leq j_1 < j_2 \cdots < j_m \leq n$ the determinant of the matrix $(a_{j_k, j_\ell})_{k,\ell=1,\ldots,m}$ is zero. Prove that $A^n = 0$ and that there exists a permutation $\sigma \in S_n$ such that the matrix $(a_{\sigma(k),\sigma(\ell)})_{k,\ell=1,\ldots,n}$ has all of its nonzero elements above the diagonal.

Problem 11 Consider an $n \times m$ array. A subset S of the nm cells is called *balanced* if every row and every column contains an even number of cells of S. Find the smallest positive integer k with the property that every set of k cells contains a balanced subset.

Problem 12 Let G be a complete graph on $2n$ vertices (a simple graph with an edge between every pair of distinct vertices). Suppose that $H_1, \ldots, H_k$ are subgraphs of G with the following properties.

1. Every H_i is a *complete bipartite subgraph* of G (there are disjoint sets A_i, B_i of the $2n$ vertices such that H_i is the graph with vertices $A_i \cup B_i$ with an edge between every pair of vertices $a \in A_i$ and $b \in B_i$).
2. Every edge of G is contained in an *odd* number of the H_i's.

Show that $k \geq n$.

Problem 13 The complete graph K_n cannot be decomposed into fewer than $n-1$ disjoint complete bipartite subgraphs.

Problem 14 A permutation σ on $\{1, \ldots, n\}$ is called *k-limited* if $|\sigma(i) - i| \leq k$ for all i. Show that the number of k-limited permutations on $\{1, \ldots, n\}$ is odd if and only if $n \equiv 0, 1 \bmod 2k + 1$.

Problem 15 Let $M_1, \ldots, M_{n+2}$ be $n + 2$ non-empty subsets of $\{1, \ldots, n\}$. Show that there are disjoint non-empty sets $I, J \subseteq \{1, \ldots, n + 1\}$ of indices such that

$$\bigcup_{k \in I} M_k = \bigcup_{k \in J} M_k \quad \text{and} \quad \bigcap_{k \in I} M_k = \bigcap_{k \in J} M_k.$$

Problem 16 In a town every two residents who are not friends have a friend in common, and no one is a friend of everyone else. Let us number the residents from 1 to n and let a_i be the number of friends of the i-th resident. Suppose that $\sum_{i=1}^{n} a_i^2 = n^2 - n$. Let k be the smallest number of residents (at least three) who can be seated at a round table in such a way that any two neighbors are friends. Determine all possible values of k.

Problem 17 In a party with n people, it is known that for every nonempty subset S of people, there is at least one person, inside or outside S, such that this person has an odd number of friends in S. Prove that n is even.

Problem 18 (Tricky) Let A be an $m \times m$ symmetric matrix over the field $\mathbb{F}_2$ with $\operatorname{diag}(A) = 0$. Show that for every $n \geq 1$, each column of A^n contains a 0.

Problem 19 (Tricky) Show that we can color the vertices of any finite simple graph with two colors, red and blue, such that

1. Each red vertex is adjacent to an *even* number of red vertices;
2. Each blue vertex is adjacent to an *odd* number of red vertices.

5 Mixed problems

Problem 20 Given 2015 rational numbers, suppose that if you remove any of them, then the remaining 2014 numbers can be partitioned into two sets of 1007 numbers that have the same sum. Show that all numbers have to be equal.

Problem 21 Consider an $n \times m$ array. A subset S of the nm cells is called *balanced* if every row and every column contains an even number of cells of S. Find the smallest positive integer k with the property that every set of k cells contains a balanced subset.

Problem 22 Let $\mathcal{F}$ be a finite collection of finite subsets of some set U. We say that a set $A \subseteq U$ is *fully tested* by $\mathcal{F}$ if each of the $2^{|A|}$ subsets X of A can be written as $X = A \cap F$ for some $F \in \mathcal{F}$. Show that there exist at least $|\mathcal{F}|$ sets that are fully tested by $\mathcal{F}$.

Question 1* (Problems with a * are quite tricky) Let $A_1, \ldots, A_m$ be sets of size r and let $B_1, \ldots, B_m$ be sets of size s such that

(i) A_i and B_i are disjoint for $i = 1, \ldots, m$;

(ii) A_i and B_j intersect whenever $i \neq j$.

Then

$$m \leq \binom{r+s}{r}.$$

Question 2 Suppose that $2n$ points of an $n \times n$ grid are marked. Show that for some $k > 1$ one can select $2k$ distinct marked points, say $a_1, \ldots, a_{2k}$, such that a_1 and a_2 are in the same row, a_2 and a_3 are in the same column, $\ldots$, a_{2k-1} and a_{2k} are in the same row, and a_{2k} and a_1 are in the same column.

Question 3 Two hundred students participated in a mathematical contest. They had 6 problems to solve. It is known that each problem was correctly solved by at least 120 participants. Prove that there must be two participants such that every problem was solved by at least one of these two students.

Question 4 Let $f : \mathbb{N}^2 \mapsto \mathbb{N}$. Suppose that each integer in $\mathbb{N}$ is image of exactly 2012 pairs in $\mathbb{N}^2$. Show that there is a pair $(n, m) \in \mathbb{N}^2$ such that $f(n, m) > mn$.

Question 5 An alien race has three genders: male, female, and emale. A married triple consists of three persons, one from each gender, who all like each other. Any person is allowed to belong to at most one married triple. A special feature of this race is that feelings are always mutual — if x likes y, then y likes x. The race is sending an expedition to colonize a planet. The expedition has n males,

n females, and n emales. It is known that every expedition member likes at least k persons of each of the two other genders. The problem is to create as many married triples as possible to produce healthy offspring so the colony could grow and prosper.
a) Show that if n is even and $k = n/2$, then it might be impossible to create even one married triple.
b) Show that if $k \geq 3n/4$, then it is always possible to create n disjoint married triples, thus marrying all of the expedition members.

Question 6 Let S_n denote the set of all permutations of the numbers $1, 2, \ldots, n$. For $\pi \in S_n$, let $\sigma(\pi) = 1$ if π is an even permutation and $\sigma(\pi) = -1$ if π is an odd permutation. Also, let $\nu(\pi)$ denote the number of fixed points of π. Show that

$$\sum_{\pi \in S_n} \frac{\sigma(\pi)}{\nu(\pi) + 1} = (-1)^{n+1} \frac{n}{n+1}.$$

Question 7 Let $A_1, A_2, \ldots, A_n$ be finite, nonempty sets. Define the function

$$f(t) = \sum_{k=1}^{n} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} (-1)^{k-1} t^{|A_1 \cup A_2 \cup \cdots \cup A_k|}.$$

Prove that f is nondecreasing on $[0, 1]$. ($|A|$ denotes the number of elements in A.)