Oddtown and Eventown: Linear algebra methods in combinatorics

Henk D.L. Hollmann

Tartu, 18 March, 2022

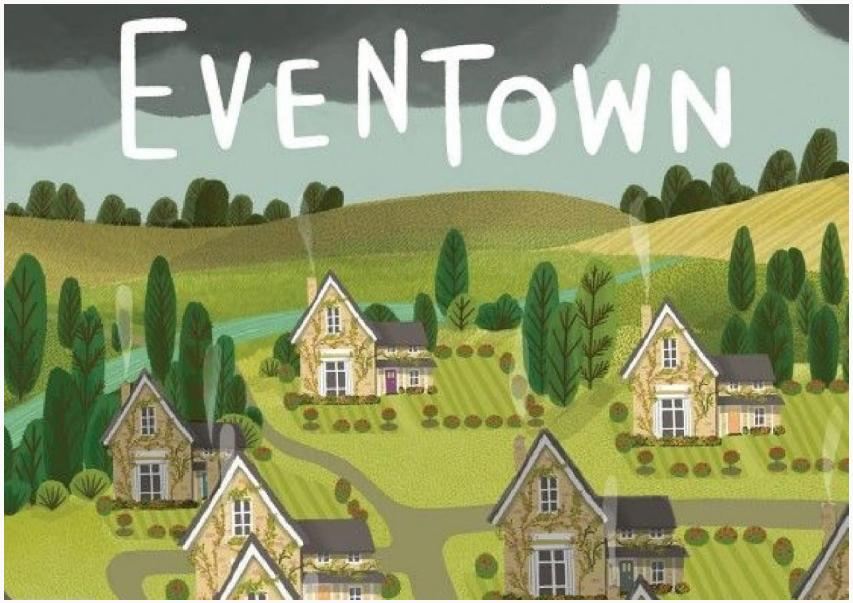
University of Tartu, Taru, Estonia
Email: henk.hollmann@ut.ee, hdlh@xs4all.nl

Content

Contents of this talk:

- Introduction: Eventown and Oddtown
- Basics of linear algebra
- Some vector space examples
- Incidence and adjacency matrics
- The town problems revisited
- Some more linear algebra problems
- Conclusions

Introduction



The small town Eventown has precisely 2022 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.

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

(Rule 2 was still supposed to hold.) This new rules made the social lives of the remaining 2021 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.

- Any two distinct clubs must share *precisely two* members;

(This rule is now supposed to be the *only* rule; however no two clubs can 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.

Basics of linear algebra

Notation:

$\mathbb{F}$ is 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.

$\mathbb{F}^n$ is the vector space of dimension n over $\mathbb{F}$.

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

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

For V a subspace of $\mathbb{F}^n$:

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

the *orthogonal complement* of V.

For subspaces V, W of $\mathbb{F}^n$:

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

$\mathbf{0}_n$ is the all-zero vector $(0, \ldots, 0)^\top$.

$\boldsymbol{j}_n$ is the all-one vector $(1, 1, \ldots, 1)^\top$ of size n,

$\boldsymbol{J}_n$ or $\boldsymbol{J}_{n,m}$ is the all-one matrix of size $n \times n$ or size $n \times m$.

$\boldsymbol{O}_n$ or $\boldsymbol{O}_{n,m}$ is the $n \times n$ or $n \times m$ all-zero matrix.

$\boldsymbol{I}_n$ is the identity matrix $\mathrm{diag}(\boldsymbol{j}_n)$ of size $n \times n$.

Simply $\mathbf{0}$ and $\boldsymbol{j}$ and $\boldsymbol{J}$ and $\boldsymbol{I}$ and $\boldsymbol{O}$ if dimensions clear from context.

Useful properties of matrices and vector spaces, valid for **all** fields:

- *Dimension* $\dim(V)$ of a vector space V: the largest size of a collection of n (linearly) independent vectors in V.
- A *basis* of V: a set of $\dim(V)$ independent vectors in V.
- Any $n+1$ vectors $\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ in an n-dimensonal vector space over a field $\mathbb{F}$ are *dependent*:
  there are $\lambda_0, \lambda_1, \ldots, \lambda_n$ in $\mathbb{F}$, *not all zero*, such that

$$\lambda_0 \boldsymbol{v}_0 + \lambda_1 \boldsymbol{v}_1 + \cdots + \lambda_n \boldsymbol{v}_n = 0.$$

- Given k independent vectors in an n-dimensional vector space, then $k \leq n$.
- The dimension cannot go down by enlarging the field (see the later item on determinants).

For $\boldsymbol{M}$ an $n \times m$ matrix over some field $\mathbb{F}$:

- *Rowspace* $\mathrm{row}(M)$: the subspace of $\mathbb{F}^m$ spanned by the *rows* of M.
- *Columnspace* $\mathrm{col}(M)$: the subspace of $\mathbb{F}^n$ spanned by the *columns* of $\boldsymbol{M}$.
- The *null space* $\mathrm{null}(M)$ (or *kernel*) of M is the collection of all $x \in \mathbb{F}^m$ such that $Mx = 0$.

- $\mathrm{row}(M)$ and $\mathrm{col}(M)$ have the *same* dimension, called the *rank* of M, denoted by $\mathrm{rank}(M)$.
- $\mathrm{rank}(M^\top) = \mathrm{rank}(M)$ and $\mathrm{rank}(M) \leq \min(m, n)$.
- Obviously, $\mathrm{null}(M) = \mathrm{row}(M)^\perp$.

For V is a subspace of $\mathbb{F}^n$:

- $\dim(V) + \dim(V^\perp) = n$.
  Watch out:
  if $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, then $x^\top x = 0$ implies $x = 0$, so
  $V \cap V^\perp = \{0\}$.
  Not always true: in particular, in *finite fields* this is *false*.
  For example, over a field of characteristic 2 such as $\mathbb{F}_2 = \mathbb{Z}_2$,
  we have for $\boldsymbol{v} = (1, 1)^\top$ that $\boldsymbol{v}^\top \boldsymbol{v} = 2 = 0$.
  So for $V = \{\mathbf{0}, (1, 1)^\top\} \subseteq \mathbb{F}_2^2$, we have $V^\perp = V$, both of dimension 1.
- $\mathrm{col}(A + B) \subseteq \mathrm{col}(A) + \mathrm{col}(B)$, so
  $\mathrm{rank}(A + B) \leq \mathrm{rank}(A) + \mathrm{rank}(B)$.
- An $m \times n$ matrix M is *invertible* if and only if
  $m = n = \mathrm{rank}(M)$.

Very important:

V, W vector spaces; **linear** map $f : V \to W$.

$\mathrm{null}(f) = \ker(f) = \{x \in v \mid f(v) = 0\}$, $\mathrm{nullity}(f) := \dim(\ker(f))$.

$\mathrm{range}(f) = \{f(\mathbf{x}) \mid \mathbf{x} \in V\}$, $\mathrm{rank}(f) = \dim(\mathrm{range}(f))$.

Dimension Theory, Rank-nullity Theorem:

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

or

$$\dim(V) = \mathrm{nullity}(f) + \mathrm{rank}(f).$$

Corollary: if $\dim(V) = \dim(W)$, then conditions

(i) f is onto;
(ii) f is 1-1;
(iii) $\mathrm{rank}(f) = \dim(W)$;

are all equivalent.

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

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

Other consequences:

- A square matrix $\boldsymbol{M}$ over a field $\mathbb{F}$ is invertible if and only if $\boldsymbol{M}\boldsymbol{x} = \mathbf{0}$ implies that $\boldsymbol{x} = \mathbf{0}$.

Theorem

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: 1. $\text{range}(\boldsymbol{AB}) \subseteq \text{range}(\boldsymbol{A})$, hence $\text{rank}(\boldsymbol{AB}) \leq \text{rank}(\boldsymbol{A})$.

2. $\text{null}(\boldsymbol{B}) \subseteq \text{null}(\boldsymbol{AB})$, hence $\text{nullity}(\boldsymbol{B}) \leq \text{nullity}(\boldsymbol{AB})$.
$\text{nullity}(\boldsymbol{B}) + \text{rank}(\boldsymbol{B}) = \text{nullity}(\boldsymbol{AB}) + \text{rank}(\boldsymbol{AB}) = n$, so
$\text{rank}(\boldsymbol{AB}) \leq \text{rank}(\boldsymbol{B})$. $\square$

S_n: all permutations of $\{1, \ldots, n\}$.

The *sign* of a permutation π is 1 if π can be written as a product of an *even* number of transpositions, -1 otherwise.
[Something needs a proof here! Exercise: prove it!]

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

$$\det(\boldsymbol{M}) = \sum_{\pi \in S_n} \operatorname{sign}(\pi) \prod_{i=1}^{n} M_{i,\pi(i)} \neq 0.$$

  The *permanent* $\operatorname{perm}(\boldsymbol{M})$: leave out the signs. Over $\mathbb{F}_2$, $\det(\boldsymbol{M}) = \operatorname{perm}(\boldsymbol{M})$.

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 $\boldsymbol{V} = [\boldsymbol{v}_1 \cdots \boldsymbol{v}_n]$. 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

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

- If $\boldsymbol{M}$ is a real $n \times m$ matrix , then $\det(\boldsymbol{M}^\top \boldsymbol{M}) \geq 0$, with equality iff $\operatorname{rank}(\boldsymbol{M}) < m$ [proof?].
  A matrix of the form $\boldsymbol{M}^\top \boldsymbol{M}$ is called a *Gram* (or *Gramian*) matrix.

Some vector space examples

Sometimes: consider *polynomials* or *functions* as vectors in a suitable vector space. Examples:

- $\mathcal{P}_n(\mathbb{F})$: polynomials of degree at most n with coefficients in some field $\mathbb{F}$.
  is an $(n+1)$-dimensional vector space over $\mathbb{F}$ with basis $1, x, \ldots, x^n$.
- Set of maps $f_i : X \mapsto \mathbb{F}$ for $1 \leq i \leq n$ and points $x_1, \ldots, x_n$ in X. If $f_i(x_i) \neq 0$ and $f_i(x_j) = 0$ for $i \neq j$, then $f_1, \ldots, f_n$ are independent [idea?].

Vandermonde matrix

- Set of vectors $V \subseteq \mathbb{F}^n$ is in *general position* if any n of the vectors of V are independent.
- Then the *null space* of the matrix with as columns the vectors from V is said to be an *MDS code*.
- If $|\mathbb{F}| \geq n$, then the $|\mathbb{F}|$ vectors

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

($a \in \mathbb{F}$) are in general position. Reason : the *Vandermonde determinant*

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

[Exercise: prove this!]

Incidence and adjacency matrices

- $\mathcal{P}$: finite set, elements are called *points*
- $\mathcal{B}$: finite set of *subsets* of $\mathcal{P}$ called *blocks*.
- $B \in \mathcal{B}$: points in B are *incident* to B.
- Two points $P_1, P_2 \in \mathcal{P}$ are *adjacent* if together in a block.

$B \subseteq \mathcal{P}$ and $\mathcal{P} = \{P_1, \ldots, P_n\}$, then *characteristic vector* $\chi_B \in \{0,1\}^n$ is

$$\chi_B(i) = \begin{cases} 1, & \text{if } P_i \in B; \\ 0, & \text{otherwise.} \end{cases}$$

Two matrices describing the relations between points and blocks.

- The *incidence matrix* is the $|\mathcal{P}| \times |\mathcal{L}|$ matrix $\boldsymbol{M}$ defined by

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

  Columns of the incidence matrix $\boldsymbol{M}$ are the *characteristic vectors* or *incidence vectors* of the blocks, so has the vectors χ_B for the blocks B as columns.
- 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

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

  If we consider $\boldsymbol{M}, \boldsymbol{A}$ as real matrices, then $\det(\boldsymbol{A}) \geq 0$.
- The *block intersection* matrix $\boldsymbol{N}$: here $\boldsymbol{N}(B, B') = |B \cap B'|$. Note: $\boldsymbol{N}$ is the adjacency matrix of the *dual* configuration (interchange 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. Also, if the problem is modelled 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 matrices and vectors, and then considering these matrices and vectors over a *suitable field*, sometimes $\mathbb{Q}$, sometimes a finite field $\mathbb{Z}_p$.

The town problems revisited

Consider the incidence matrix for the clubs in Even/Odd-town.

The n inhabitants are the "points"; the m clubs are the "blocks".

Incidence matrix: $n \times m$ matrix $\boldsymbol{M}$.

Club-forming rules of Eventown: $n = 2022$, the $m \times m$ block-intersection matrix $\boldsymbol{M}^\top \boldsymbol{M}$ has *even* entries, that is, as matrix over $\mathbb{F}_2$,

$$\boldsymbol{M}^\top \boldsymbol{M} = \boldsymbol{O}_m.$$

Analysis: We have $\boldsymbol{M}^\top \boldsymbol{M} = \boldsymbol{O}_m$.

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.

$\boldsymbol{M}^\top \boldsymbol{M} = \boldsymbol{O}_m$, hence $V \subseteq V^\perp$, so $2\dim(V) \leq n$ and $\dim(V) \leq n/2$.

Available columns for $\boldsymbol{M}$: the vectors from V, and $|V| = 2^{\lfloor n/2 \rfloor}$.

So number of different clubs $m \leq 2^{\lfloor n/2 \rfloor}$.

Hence at most 2^{1011} clubs can be formed under rules 1 and 2.

This can 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).

Consider $\boldsymbol{M}$ as matrix over $\mathbb{F}_2$, then $\boldsymbol{M}^\top \boldsymbol{M} = \boldsymbol{I}_n$.

So the m columns of $\boldsymbol{M}$ are independent in an n-dimensional space $\mathbb{F}_2^n$.

So M has rank $m \leq n$.

Hence, given that $n = 2021$, at most 2021 clubs can 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 the last rule, we have $\lambda = 2$).

So for the $n \times m$ incidence matrix $\boldsymbol{M}$, now considered as **real** matrix, 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 (club).

Can we have $\boldsymbol{M}\boldsymbol{x} = \boldsymbol{0}$? For any nonzero vector $\boldsymbol{x} \in \mathbb{R}^m$, we have

$$\begin{aligned} \|\boldsymbol{M}\boldsymbol{x}\|^2 &= (\boldsymbol{M}\boldsymbol{x}, \boldsymbol{M}\boldsymbol{x}) = \boldsymbol{x}^\top \boldsymbol{M}^\top \boldsymbol{M}\boldsymbol{x} = \lambda \boldsymbol{x}^\top (\boldsymbol{J} - \boldsymbol{I})\boldsymbol{x} + \boldsymbol{x}^\top \boldsymbol{K}\boldsymbol{x} = \\ & \lambda \left(\sum_i x_i \right)^2 + \sum_i (k_i - \lambda) x_i^2. \end{aligned}$$

(Repeat)

$$\|\boldsymbol{M}\boldsymbol{x}\|^2 = \lambda\left(\sum_i x_i\right)^2 + \sum_i (k_i - \lambda)x_i^2.$$

If $\boldsymbol{M}\boldsymbol{x} = \boldsymbol{0}$, then $\|\boldsymbol{M}\boldsymbol{x}\| = 0$.

- Now $k_i \geq \lambda$ and all clubs are distinct, so at most one club can have size λ [why?].
- If $\sum_i x_i = 0$ but $\boldsymbol{x} \neq 0$, then at least two x_i are nonzero.

Conclusion: if $\boldsymbol{x} \neq 0$, then $\|\boldsymbol{M}\boldsymbol{x}\| > 0$ and hence $\boldsymbol{M}\boldsymbol{x} \neq \boldsymbol{0}$.

So M has rank m and so the number m of clubs again satisfies $m \leq n$. Hence, given that $n = 2013$, again at most 2013 clubs can be formed under the last rule.

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

Some more linear algebra problems

Problem 1. 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.

Problem 2 (Putnam 2003-B1).

Do there exists 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?

Problem 3.

Let $M_1,\ldots,M_{n+1}$ be $n+1$ 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

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

Solution: 1.

Let 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 M as a matrix over $\mathbb{F}_2$ then $M^\top M = I_{n+1}$. However, $\mathrm{rank}(M^\top M) \leq \mathrm{rank}(M) \leq n$, a contradiction. □

Solution: 2.

Suppose there are. By plugging in $y = -1, 0, 1$ we obtain that the (3-dimensional) span of the polynomials $\{1, x, x^2\}$ is contained in the (2-dimensional) span of $\{a(x), b(x)\}$, which is clearly impossible. □

Solution: 3.

Hint: Consider the $n+1$ characteristic vectors $\chi_i \in \mathbb{R}^n$ of the sets M_i. □

Conclusions

- Linear algebra is a powerful tool in combinatorics!
- But creativity may be required in applications.