Less than 33 Miniatures

Based on the textbook "Thirty-three Miniatures: Mathematical and Algorithmic Applications of Linear Algebra" by Jiri Matousek

Instructor's Handout

The appearance of linear-algebraic methods is often unexpected.
— Jiri Matousek

Miniature 1: Fibonacci Numbers, Quickly

The Fibonacci numbers $F_0, F_1, F_2, \ldots$ are defined by the relations

$$F_0 = 0, \quad F_1 = 1, \quad \text{and} \quad F_{n+2} = F_{n+1} + F_n \text{ for } n \geq 0.$$

Obviously, F_n can be calculated using roughly n arithmetic operations. Using linear algebra, can we do it more quickly?

Problem 1:
Write an algorithm that uses linear algebra to compute the n^{th} Fibonacci number in $O(\log n)$ time.

Steps for Problem 1:

- *Encode two Fibonacci numbers F_n, F_{n+1} as a vector $v_n = \begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix}$.*
- *Write down a matrix M that returns the next vector v_{n+1} given the previous vector v_n; that is, find M such that $Mv_n = v_{n+1}$.*
- *Write a formula for v_n given $v_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.*
- *Describe an algorithm that computes v_n (and hence finds F_{n+1}) using only $O(\log n)$ matrix multiplications.*

Solution

- $M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$
- $v_n = Mv_{n-1} = M^n v_0$.
- Same as for a scalar, to compute M^n, we need to square M $\log_2(n)$ times. Hence $O(\log(n))$ matrix multiplications.

Miniature 2: Fibonacci Numbers, the Formula

Problem 2:
Derive an explicit formula for the n^{th} Fibonacci number F_n.

Steps for Problem 2:

- *Let W be the vector space of all sequences $(u_0, u_1, u_2, \dots)$ of real numbers — with coordinate-wise addition and multiplication by real numbers — which satisfy the Fibonacci recursion relationship:*

$$W = \big\{(u_0, u_1, u_2, \dots) \subset \mathbb{R} \;\big|\; u_{n+2} = u_{n+1} + u_n\big\}.$$

- *What is the dimension of this vector space? Write down a basis.*
- *Find all possible values of τ such that $v_n = \tau^n$ is a sequence in W.*
- *Verify that these special sequences form a basis for W.*
- *Write the Fibonacci sequence $F = (F_0, F_1, F_2, F_3, \dots) = (0, 1, 1, 2, \dots)$ as a linear combination of these special sequences. Then find an explicit formula for the n^{th} Fibonacci number F_n.*

Solution

The possible values of τ satisfy $\tau^2 = \tau + 1$ which gives

$$\tau_\pm = \frac{1 \pm \sqrt{5}}{2}.$$

Then we want to write F as a linear combination of the two sequences $(\tau_\pm^0, \tau_\pm, \tau_\pm^2, \tau_\pm^3, \dots)$. A little algebra gives

$$F_0 = 0 = \frac{1}{\sqrt{5}}\tau_+^0 - \frac{1}{\sqrt{5}}\tau_-^0$$
$$F_1 = 1 = \frac{1}{\sqrt{5}}\tau_+ - \frac{1}{\sqrt{5}}\tau_-$$

and so

$$F_n = \frac{1}{\sqrt{5}}(\tau_+^n - \tau_-^n) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

Miniature 3: The Clubs of Oddtown

There are n citizens living in Oddtown. Their main occupation was forming various clubs, which at some point started threatening the very survival of the city. In order to limit the number of clubs, the city council decreed the following innocent-looking rules:

- Each club has to have an odd number of members.
- Every two clubs must have an even number of members in common.

Problem 3:
Under these rules, show that it is impossible to form more than n clubs.

Steps for problem 3:

- *Encode the club participation of Oddtown in a matrix: Suppose there are m clubs and n citizens. Define an $m \times n$ matrix A where $A_{ij} = 1$ if citizen j is in club i and $A_{ij} = 0$ if citizen j is not in club i. For the remainder of this problem, treat this as a matrix with entries in $\mathbb{F}_2$.*
- *Look at the matrix product AA^T. What do the rules of Oddtown tell you about AA^T?*
- *What is the rank of the matrix AA^T? How does this compare to the number of clubs?*
- *How does the rank of AA^T compare to the rank of A? Use this to conclude that the maximal number of clubs is n.*

Solution

Let us call the citizens $1, 2, \ldots, n$ and the clubs $C_1, C_2, \ldots, C_m$. We define an $m \times n$ matrix A by

$$a_{ij} = \begin{cases} 1 & \text{if } j \in C_i, \\ 0 & \text{otherwise.} \end{cases}$$

(Thus clubs correspond to rows and citizens to columns.)
Let us consider the matrix A over the two-element field $\mathbb{F}_2$. Clearly, the rank of A is at most n. Next, we look at the product AA^T. This is an $m \times m$ matrix whose entry at position (i, k) equals $\sum_{j=1}^{n} a_{ij}a_{kj}$, and so it counts the number of citizens in $C_i \cap C_k$. More precisely, since we now work over $\mathbb{F}_2$, the entry is 1 if $|C_i \cap C_k|$ is odd, and it is 0 if $|C_i \cap C_k|$ is even.
Therefore, the rules of the city council imply that $AA^T = I_m$, where I_m denotes the identity matrix. So the rank of AA^T is at least m. Since the rank of a matrix product is no larger than the minimum of the ranks of the factors, we have $\operatorname{rank}(A) \geq m$ as well, and so $m \leq n$.

Miniature 6: Odd Distances

Problem 4:
Show there are no 4 points in the plane such that the distance between each pair is an odd integer.

Steps for problem 4:

- *Let* $\mathbf{0}$ *be one of the points and* a, b, c *the other three. Suppose that the distance between each pair of points is odd. Write down this condition in terms of* a, b, c*. We will be showing that this creates a contradiction.*
- *Show that if* m *is an odd integer, then* $m^2 = 1 \pmod 8$*.*
- *Derive the polarization identity*

$$\|u+v\|^2 = \|u\|^2 + \|v\|^2 + 2\langle u, v\rangle$$

and use it to show that

$$2\langle a, b\rangle = 2\langle a, c\rangle = 2\langle b, c\rangle = 1 \pmod 8.$$

.

- *Define a matrix* A *with columns* a, b, c*. What is the maximum rank of* A*?*
- *Write a formula for the product* $B = A^T A$ *in terms of* $\|a\|^2, \langle a, b\rangle, \langle a, c\rangle, \ldots$ *etc. Using your previous results, compute* $2B \pmod 8$*.*
- *What is the determinant of* $2B \pmod 8$*? What does this tell you about the rank of* B*? Use this to find a contradiction.*

Solution

We observe that if m is an odd integer, then $m^2 \equiv 1 \pmod 8$ (here $\equiv$ denotes congruence; $x \equiv y \pmod k$ means that k divides $x - y$). Hence the squares of all the considered distances are congruent to 1 modulo 8. From the cosine theorem we also have

$$2\langle a, b\rangle = \|a\|^2 + \|b\|^2 - \|a-b\|^2 \equiv 1 \pmod 8,$$

and the same holds for $2\langle a, c\rangle$ and $2\langle b, c\rangle$. If B is the matrix

$$B = \begin{pmatrix} \langle a, a\rangle & \langle a, b\rangle & \langle a, c\rangle \\ \langle b, a\rangle & \langle b, b\rangle & \langle b, c\rangle \\ \langle c, a\rangle & \langle c, b\rangle & \langle c, c\rangle \end{pmatrix},$$

then $2B$ is congruent to the matrix

$$R := \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$$

modulo 8. Since $\det(R) = 4$, we have $\det(2B) \equiv 4 \pmod 8$. (To see this, we consider the expansion of both determinants according to the definition, and we note that the corresponding terms for $\det(2B)$ and for $\det(R)$ are congruent modulo 8.) Thus $\det(2B) \neq 0$, and so $\det(B) \neq 0$. Hence, $\operatorname{rank}(B) = 3$.
On the other hand, $B = A^T A$, where

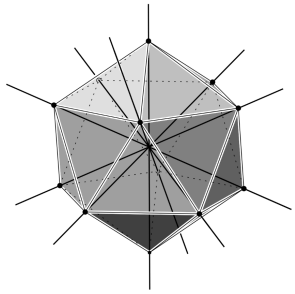
$$A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}.$$

We have $\operatorname{rank}(A) \leq 2$ and, as it is well known, the rank of a product of matrices is no larger than the minimum of the ranks of the factors. Thus, $\operatorname{rank}(B) \leq 2$, and this contradiction concludes the proof.

Miniature 9: Equiangular Lines

What is the largest number of lines in $\mathbb{R}^3$ such that the (nonzero) angle between every two of them is the same?

Everybody knows that in $\mathbb{R}^3$ there cannot be more than three mutually orthogonal lines, but the situation for angles other than 90 degrees is more complicated. For example, the six longest diagonals of the regular icosahedron (connecting pairs of opposite vertices) are equiangular:



As we will prove, this is the largest number one can get.

Problem 5:
Show that the largest number of equiangular lines in $\mathbb{R}^3$ is 6, and in general, there cannot be more than $\binom{d+1}{2}$ equiangular lines in $\mathbb{R}^d$.

Steps for problem 5:

- *Suppose that you have a configuration of n lines with unit directions $v_1, \dots, v_n \in \mathbb{R}^d$. Suppose that the angle between any two distinct lines is a fixed θ, with $0 < \theta < \frac{\pi}{2}$. What does this condition tell you about $\langle v_i, v_j \rangle$ for $i \neq j$?*
- *Consider the $d \times d$ matrices $M_i = v_i v_i^T$. Show that M_i is symmetric for each i.*
- *Show that the vector space of symmetric $d \times d$ matrices has dimension $\binom{d+1}{2}$.*
- *If we can show that the matrices M_i are linearly independent, then we are done. (Why?) To show this, suppose that we have a linear combination of M_i such that*

$$\sum_i a_i M_i = 0.$$

Multiply this sum on the left by v_j^T and on the right by v_j. Write this sum entirely in terms of the coefficients a_i and $\cos^2\theta$.
- *Using the fact that $\cos^2\theta < 1$, show that $a_i = 0$ for all i. (This is challenging. Feel free to ask your instructor.)*

Solution

Let us consider a configuration of n lines, where each pair has the same angle $\vartheta \in (0, \frac{\pi}{2}]$. Let v_i be a unit vector in the direction of the ith line (we choose one of the two possible orientations of v_i arbitrarily). The condition of equal angles is equivalent to

$$|\langle v_i, v_j \rangle| = \cos\vartheta, \quad \text{for all } i \neq j.$$

Let us regard v_i as a column vector, or a $d \times 1$ matrix. Then $v_i^T v_j$ is the scalar product $\langle v_i, v_j \rangle$, or more precisely, the 1×1 matrix whose only entry is $\langle v_i, v_j \rangle$. On the other hand, $v_i v_j^T$ is a $d \times d$ matrix.
We show that the matrices $v_i v_i^T$, $i = 1, 2, \dots, n$, are linearly independent. Since they are elements of the vector space of all real symmetric $d \times d$ matrices, and the dimension of this

Solution (continued)

space is $\binom{d+1}{2}$, we get $n \le \binom{d+1}{2}$, just as we wanted.
To check linear independence, we consider a linear combination

$$\sum_{i=1}^{n} a_i v_i v_i^T = 0,$$

where $a_1, a_2, \ldots, a_n$ are some coefficients. We multiply both sides of this equality by v_j^T from the left and by v_j from the right. Using the associativity of matrix multiplication, we obtain

$$0 = \sum_{i=1}^{n} a_i v_j^T (v_i v_i^T) v_j = \sum_{i=1}^{n} a_i \langle v_i, v_j \rangle^2 = a_j + \sum_{i \neq j} a_i \cos^2 \vartheta$$

for all j.
In other words, we have deduced that $Ta = 0$, where $a = (a_1, \ldots, a_n)$ and

$$T = (1 - \cos^2 \vartheta)\, I_n + (\cos^2 \vartheta)\, J_n.$$

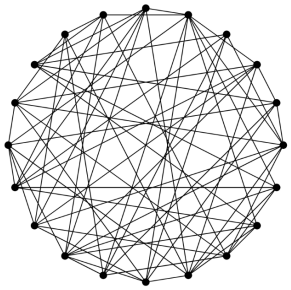
Here I_n is the identity matrix and J_n is the matrix of all 1's. It is easy to check that the matrix T is nonsingular (using $\cos \vartheta \neq 1$). Therefore, $a = 0$, the matrices $v_i v_i^T$ are linearly independent, and the theorem is proved.
Alternatively, one can let $S = \sum_i a_i$ and note that $0 < \cos^2 \theta < 1$ implies

$$0 = a_j + \cos^2\theta\big(S - a_j\big) \implies (1 - \cos^2\theta) a_j = S \cos^2 \theta \implies (1 - \cos^2\theta) S = nS \cos^2 \theta \implies S = 0.$$

Then $(1 - \cos^2 \theta) a_j = S \cos^2 \theta \implies a_j = 0$ for all j.

Miniature 10: Where is the Triangle?

Does a given graph contain a triangle, i.e., three vertices u, v, w, every two of them connected by an edge? This question is not entirely easy to answer for graphs with many vertices and edges. For example, where is a triangle in this graph?



An obvious algorithm for finding a triangle inspects every triple of vertices, and thus it needs roughly n^3 operations for an n-vertex graph (there are $\binom{n}{3}$ triples to look at, and $\binom{n}{3}$ is approximately $n^3/6$ for large n). Can we do any better with linear algebra?

Problem 6:
Given a graph G with n vertices, use the fact that an $n \times n$ matrix can be squared in $O(n^{2.371339})$ time to write an $O(n^{2.371339})$ algorithm that determines whether G contains a triangle.

Steps for problem 6:

- *Let A be the adjacency matrix of G. Consider $B = A^2$. Using the definition of matrix multiplication, what does the entry B_{ij} tell us about the graph G?*
- *In terms of the entries A_{ij} and B_{ij}, what does it mean for G to contain a triangle?*
- *Using the fast matrix multiplication as a black box, write an algorithm that checks if G contains a triangle.*

Solution

Define the adjacency matrix of G as the $n \times n$ matrix A with

$$a_{ij} = \begin{cases} 1 & \text{if } i \neq j \text{ and } \{i,j\} \in E(G), \\ 0 & \text{otherwise.} \end{cases}$$

The key insight is to understand the square $B := A^2$. By the definition of matrix multiplication we have $b_{ij} = \sum_{k=1}^{n} a_{ik}a_{kj}$, and

$$a_{ik}a_{kj} = \begin{cases} 1 & \text{if the vertex } k \text{ is adjacent to both } i \text{ and } j, \\ 0 & \text{otherwise.} \end{cases}$$

So b_{ij} counts the number of common neighbors of i and j.
Finding a triangle is equivalent to finding two adjacent vertices i, j with a common neighbor k. So we look for two indices i, j such that both $a_{ij} \neq 0$ and $b_{ij} \neq 0$.
To do this, we need to compute the matrix $B = A^2$. If we perform the matrix multiplication according to the definition, we need about n^3 arithmetic operations and thus we save nothing compared to the naive method of inspecting all triples of vertices.
However, ingenious algorithms are known that multiply $n \times n$ matrices asymptotically faster. The oldest one, due to Strassen, needs roughly $n^{2.807}$ arithmetic operations. It is based on a simple but very clever trick—if you haven't seen it, it is worth looking it up.
Newer methods get you to $O(n^{2.371339})$.

Miniature 12: Tiling a Rectangle by Squares

Problem 7:
Show that a rectangle R with side lengths 1 and x, where x is irrational, cannot be tiled by finitely many squares.

Steps for problem 7:

- *Suppose that a tiling exists consisting of squares $Q_1, \ldots, Q_n$. Let s_i be the side length of Q_i.*
- *Consider the real numbers $\mathbb{R}$ as a vector space over the field $\mathbb{Q}$. Let $V \subset \mathbb{R}$ be the subspace generated by $x, s_1, s_2, \ldots, s_n$.*
- *We can define a linear function f such that $f(1) = 1$ and $f(x) = -1$. (This is possible because $x, 1$ are linearly independent over $\mathbb{Q}$).*
- *For a rectangle A with side lengths a and b, define $v(A) = f(a)f(b)$. Using the linearity of f, prove that*
$$v(R) = \sum_{i=1}^{n} v(Q_i).$$
(This is the most challenging part. Draw a picture and don't be afraid to ask your instructor for help.)
- *Using the definition of v, f, Q_i, and R, find a contradiction.*

Solution

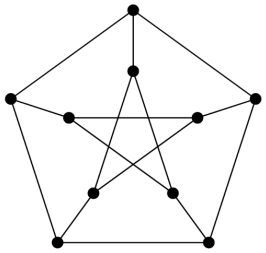
For contradiction, let us assume that a tiling exists, consisting of squares $Q_1, Q_2, \ldots, Q_n$, and let s_i be the side length of Q_i.
We need to consider the set $\mathbb{R}$ of all real numbers as a vector space over the field $\mathbb{Q}$ of rationals. This is a rather strange, infinite-dimensional vector space, but a very useful one.
Let $V \subseteq \mathbb{R}$ be the linear subspace generated by the numbers x and $s_1, s_2, \ldots, s_n$, in other words, the set of all rational linear combinations of these numbers.
We define a linear mapping $f : V \to \mathbb{R}$ such that $f(1) = 1$ and $f(x) = -1$ (and otherwise arbitrarily). This is possible, because 1 and x are linearly independent over $\mathbb{Q}$. Indeed, there is a basis $(b_1, b_2, \ldots, b_k)$ of V with $b_1 = 1$ and $b_2 = x$, and we can set, e.g., $f(b_1) = 1$, $f(b_2) = -1$, $f(b_3) = \cdots = f(b_k) = 0$, and extend f linearly on V.
For each rectangle A with edges a and b, where $a, b \in V$, we define a number $v(A) := f(a)f(b)$.
We claim that if the $1 \times x$ rectangle R is tiled by the squares $Q_1, Q_2, \ldots, Q_n$, then

$$v(R) = \sum_{i=1}^{n} v(Q_i).$$

This leads to a contradiction, since $v(R) = f(1)f(x) = -1$, while $v(Q_i) = f(s_i)^2 \geq 0$ for all i.
To check the claim just made, we extend the edges of all squares Q_i of the hypothetical tiling across the whole of R. This partitions R into small rectangles, and using the linearity of f, it is easy to see that $v(R)$ equals the sum of $v(B)$ over all these small rectangles B. Similarly $v(Q_i)$ equals the sum of $v(B)$ over all the small rectangles lying inside Q_i. Thus, $v(R) = \sum_{i=1}^{n} v(Q_i)$.

Miniature 13: Three Petersens Are Not Enough

The famous Petersen graph



has 10 vertices of degree 3. The complete graph K_{10} has 10 vertices of degree 9. Yet, it is not possible to cover all edges of K_{10} by three copies of the Petersen graph.

Problem 8:
Show that there are no three subgraphs of K_{10}, each isomorphic to the Petersen graph, that together cover all edges of K_{10}.

Steps for problem 8:

- *Suppose for the sake of contradiction that K_{10} can be covered by three copies of the Petersen graph: P, Q, and R.*
- *Let A be the adjacency matrix of K_{10} and A_P, A_Q, and A_R be the adjacency matrices of the subgraphs P, Q, and R respectively. Show that*
$$A = A_P + A_Q + A_R.$$
- *Write down an adjacency matrix for the Petersen graph. Show that this adjacency matrix has eigenvalue 1 with geometric multiplicity 5. Because A_P is equivalent to any adjacency matrix of the Petersen graph, this implies that A_P has eigenvalue 1 with geometric multiplicity 5.*
- *Suppose that x is an eigenvalue of A_p with eigenvalue 1; that is, $A_p x = x$. Show that $\langle \mathbf{1}, x\rangle = 0$ where $\mathbf{1} = (1, \ldots, 1)^T$. The same is true of A_Q.*
- *Consider the subspace $\mathbf{1}^\perp = \{x : \langle \mathbf{1}, x\rangle = 0\} \subset \mathbb{R}^{10}$. What is the dimension of this subspace?*
- *Using the dimension of $\mathbf{1}^\perp$, prove that A_Q and A_P share a nonzero eigenvector v with eigenvalue 1.*
- *Prove that v is an eigenvector of A_R with eigenvalue -3. Using the fact that R is a Petersen graph, show that this is a contradiction.*

Solution

We recall that the adjacency matrix of a graph G on the vertex set $\{1, 2, \ldots, n\}$ is the $n \times n$ matrix A with
$$a_{ij} = \begin{cases} 1 & \text{if } i \neq j \text{ and } \{i, j\} \in E(G), \\ 0 & \text{otherwise.} \end{cases}$$
It means that the adjacency matrix of the graph K_{10} is $J_{10} - I_{10}$, where J_n is the $n \times n$ matrix of all 1's and I_n is the identity matrix.
Let us assume that the edges of K_{10} are covered by subgraphs P, Q, and R, each of them isomorphic to the Petersen graph. If A_P is the adjacency matrix of P, and similarly for A_Q and A_R, then
$$A_P + A_Q + A_R = J_{10} - I_{10}.$$
It is easy to check that the adjacency matrices of two isomorphic graphs have the same set of eigenvalues, and also the same dimensions of the corresponding eigenspaces.

Solution (continued)

We can use Gaussian elimination to calculate that for the adjacency matrix of the Petersen graph, the eigenspace corresponding to the eigenvalue 1 has dimension 5; i.e., the matrix $A_P - I_{10}$ has a 5-dimensional kernel.
Moreover, this matrix has exactly three 1's and one -1 in every column. So if we sum all the equations of the system $(A_P - I_{10})x = 0$, we get $2x_1 + 2x_2 + \cdots + 2x_{10} = 0$. In other words, the kernel of $A_P - I_{10}$ is contained in the 9-dimensional orthogonal complement of the vector $\mathbf{1} = (1, 1, \ldots, 1)$.
The same is true for the kernel of $A_Q - I_{10}$, and therefore, the two kernels have a common nonzero vector x. We know that $J_{10}x = 0$ (since x is orthogonal to $\mathbf{1}$), and we calculate

$$\begin{aligned} A_R x &= (J_{10} - I_{10} - A_P - A_Q)x \\ &= J_{10}x - I_{10}x - (A_P - I_{10})x - (A_Q - I_{10})x - 2I_{10}x \\ &= 0 - x - 0 - 0 - 2x = -3x. \end{aligned}$$

It means that -3 must be an eigenvalue of A_R, but it is not an eigenvalue of the adjacency matrix of the Petersen graph—a contradiction.