Spring 2024 CIS 515

Fundamentals of Linear Algebra and Optimization
Jean Gallier

Homework 1

January 18, 2024; Due February 6, 2024

Problem B1 (30 pts). (i) Prove that the axioms of vector spaces imply that

$$\begin{aligned}\alpha \cdot 0 &= 0\\ 0 \cdot v &= 0\\ \alpha \cdot (-v) &= -(\alpha \cdot v)\\ (-\alpha) \cdot v &= -(\alpha \cdot v),\end{aligned}$$

for all $v \in E$ and all $\alpha \in K$, where E is a vector space over K.

(ii) For every $\lambda \in \mathbb{R}$ and every $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, define λx by

$$\lambda x = \lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n).$$

Recall that every vector $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ can be written uniquely as

$$x = x_1 e_1 + \cdots + x_n e_n,$$

where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, with a single 1 in position i. For any operation $\cdot\colon \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$, if $\cdot$ satisfies the axiom (V1) of a vector space, then prove that for any $\alpha \in \mathbb{R}$, we have

$$\alpha \cdot x = \alpha \cdot (x_1 e_1 + \cdots + x_n e_n) = \alpha \cdot (x_1 e_1) + \cdots + \alpha \cdot (x_n e_n).$$

Conclude that $\cdot$ is completely determined by its action on each of the one-dimensional subspaces of $\mathbb{R}^n$ spanned by e_i $(1 \leq i \leq n)$.

(iii) Use (ii) to define operations $\cdot\colon \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$ that satisfy the axioms (V1–V3), but for which axiom V4 fails.

(iv) **Extra credit (20 pts)**. For any operation $\cdot\colon \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$, prove that if $\cdot$ satisfies the axioms (V2–V3), then for every rational number $r \in \mathbb{Q}$ and every vector $x \in \mathbb{R}^n$, we have

$$r \cdot x = r(1 \cdot x).$$

In the above equation, $1 \cdot x$ is some vector $(y_1, \ldots, y_n) \in \mathbb{R}^n$ not necessarily equal to $x = (x_1, \ldots, x_n)$, and

$$r(1 \cdot x) = (ry_1, \ldots, ry_n),$$

as in part (ii).

Use (iv) to conclude that any operation $\cdot\colon \mathbb{Q}\times\mathbb{R}^n \to \mathbb{R}^n$ that satisfies the axioms (V1–V3) is completely determined by the action of 1 on the one-dimensional subspaces of $\mathbb{R}^n$ spanned by $e_1, \ldots, e_n$.

Problem B2 (45 pts). (In solving this problem, **do not use determinants**). (1) Let $(u_1, \ldots, u_m)$ and $(v_1, \ldots, v_m)$ be two families of vectors in some vector space E. Assume that each v_i is a linear combination of the u_js, so that

$$v_i = a_{i\,1}u_1 + \cdots + a_{i\,m}u_m, \quad 1 \leq i \leq m,$$

and that the matrix $A = (a_{i\,j})$ is an upper-triangular matrix, which means that if $1 \leq j < i \leq m$, then $a_{i\,j} = 0$. Prove that if $(u_1, \ldots, u_m)$ are linearly independent and if all the diagonal entries of A are nonzero, then $(v_1, \ldots, v_m)$ are also linearly independent.

Hint. Use induction on m.

(2) Let $A = (a_{i\,j})$ be an upper-triangular matrix. Prove that if all the diagonal entries of A are nonzero, then A is invertible and the inverse A^{-1} of A is also upper-triangular.

Hint. Use induction on m and multiplication by blocks.

Prove that if A is invertible, then all the diagonal entries of A are nonzero (do not use determinants or eigenvalues!).

Hint. Use induction on m and multiplication by blocks.

(3) Prove that if the families $(u_1, \ldots, u_m)$ and $(v_1, \ldots, v_m)$ are related as in (1), then $(u_1, \ldots, u_m)$ are linearly independent iff $(v_1, \ldots, v_m)$ are.

Problem B3 (40 pts). (In solving this problem, **do not use determinants**). Consider the $n \times n$ matrix

$$A = \begin{pmatrix} 1 & 2 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 2 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & 2 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 1 & 2 & 0 \\ 0 & 0 & \ldots & 0 & 0 & 1 & 2 \\ 0 & 0 & \ldots & 0 & 0 & 0 & 1 \end{pmatrix}.$$

(1) Find the solution $x = (x_1, \ldots, x_n)$ of the linear system

$$Ax = b,$$

for

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

(2) Prove that the matrix A is invertible and find its inverse A^{-1}. Given that the number of atoms in the universe is estimated to be $\leq 10^{82}$, compare the size of the coefficients the inverse of A to 10^{82}, if $n \geq 300$.

(3) Prove that $(A - I)^n = 0$.

Problem B4 (80 pts). Consider the polynomials

$$\begin{array}{llll} B_0^2(t) = (1-t)^2 & B_1^2(t) = 2(1-t)t & B_2^2(t) = t^2 & \\ B_0^3(t) = (1-t)^3 & B_1^3(t) = 3(1-t)^2 t & B_2^3(t) = 3(1-t)t^2 & B_3^3(t) = t^3, \end{array}$$

known as the *Bernstein polynomials* of degree 2 and 3.

(1) Show that the Bernstein polynomials $B_0^2(t), B_1^2(t), B_2^2(t)$ are expressed as linear combinations of the basis $(1, t, t^2)$ of the vector space of polynomials of degree at most 2 as follows:

$$\begin{pmatrix} B_0^2(t) \\ B_1^2(t) \\ B_2^2(t) \end{pmatrix} = \begin{pmatrix} 1 & -2 & 1 \\ 0 & 2 & -2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ t \\ t^2 \end{pmatrix}.$$

Prove that

$$B_0^2(t) + B_1^2(t) + B_2^2(t) = 1.$$

(2) Show that the Bernstein polynomials $B_0^3(t), B_1^3(t), B_2^3(t), B_3^3(t)$ are expressed as linear combinations of the basis $(1, t, t^2, t^3)$ of the vector space of polynomials of degree at most 3 as follows:

$$\begin{pmatrix} B_0^3(t) \\ B_1^3(t) \\ B_2^3(t) \\ B_3^3(t) \end{pmatrix} = \begin{pmatrix} 1 & -3 & 3 & -1 \\ 0 & 3 & -6 & 3 \\ 0 & 0 & 3 & -3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ t \\ t^2 \\ t^3 \end{pmatrix}.$$

Prove that

$$B_0^3(t) + B_1^3(t) + B_2^3(t) + B_3^3(t) = 1.$$

(3) Prove that the Bernstein polynomials of degree 2 are linearly independent, and that the Bernstein polynomials of degree 3 are linearly independent.

(4) Recall that the *binomial coefficient* $\binom{m}{k}$ is given by

$$\binom{m}{k} = \frac{m!}{k!(m-k)!},$$

with $0 \leq k \leq m$.

For any $m \geq 1$, we have the $m + 1$ *Bernstein polynomials* of degree m given by

$$B_k^m(t) = \binom{m}{k}(1-t)^{m-k}t^k, \quad 0 \leq k \leq m.$$

Prove that

$$B_k^m(t) = \sum_{j=k}^{m} (-1)^{j-k} \binom{m}{j} \binom{j}{k} t^j. \qquad (*)$$

Use the above to prove that $B_0^m(t), \ldots, B_m^m(t)$ are linearly independent.

(5) Prove that

$$B_0^m(t) + \cdots + B_m^m(t) = 1.$$

Extra credit (20 pts). What can you say about the symmetries of the $(m+1) \times (m+1)$ matrix expressing $B_0^m, \ldots, B_m^m$ in terms of the basis $1, t, \ldots, t^m$?

Prove your claim (beware that in equation $(*)$ the coefficient of t^j in B_k^m is the entry on the $(k+1)$th row of the $(j+1)$th column, since $0 \leq k, j \leq m$. Make appropriate modifications to the indices).

What can you say about the sum of the entries on each row of the above matrix? What about the sum of the entries on each column?

(6) (This is **no longer for extra credit!**) The purpose of this question is to express the t^i in terms of the Bernstein polynomials $B_0^m(t), \ldots, B_m^m(t)$, with $0 \leq i \leq m$.

First, prove that

$$t^i = \sum_{j=0}^{m-i} t^i B_j^{m-i}(t), \quad 0 \leq i \leq m.$$

Then prove that

$$\binom{m}{i} \binom{m-i}{j} = \binom{m}{i+j} \binom{i+j}{i}.$$

Use the above facts to prove that

$$t^i = \sum_{j=0}^{m-i} \frac{\binom{i+j}{i}}{\binom{m}{i}} B_{i+j}^m(t).$$

Conclude that the Bernstein polynomials $B_0^m(t), \ldots, B_m^m(t)$ form a basis of the vector space of polynomials of degree $\leq m$.

Compute the matrix expressing $1, t, t^2$ in terms of $B_0^2(t), B_1^2(t), B_2^2(t)$, and the matrix expressing $1, t, t^2, t^3$ in terms of $B_0^3(t), B_1^3(t), B_2^3(t), B_3^3(t)$.

You should find

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1/2 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1/3 & 2/3 & 1 \\ 0 & 0 & 1/3 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

(7) A *polynomial curve* $C(t)$ *of degree* m in the plane is the set of points $C(t) = \begin{pmatrix} x(t) \\ y(t) \end{pmatrix}$ given by two polynomials of degree $\leq m$,

$$\begin{aligned} x(t) &= \alpha_0 t^{m_1} + \alpha_1 t^{m_1-1} + \cdots + \alpha_{m_1} \\ y(t) &= \beta_0 t^{m_2} + \beta_1 t^{m_2-1} + \cdots + \beta_{m_2}, \end{aligned}$$

with $1 \leq m_1, m_2 \leq m$ and $\alpha_0, \beta_0 \neq 0$.

Prove that there exist $m+1$ points $b_0, \ldots, b_m \in \mathbb{R}^2$ so that

$$C(t) = \begin{pmatrix} x(t) \\ y(t) \end{pmatrix} = B_0^m(t) b_0 + B_1^m(t) b_1 + \cdots + B_m^m(t) b_m$$

for all $t \in \mathbb{R}$, with $C(0) = b_0$ and $C(1) = b_m$. Are the points $b_1, \ldots, b_{m-1}$ generally on the curve?

We say that the curve C is a *Bézier curve* and $(b_0, \ldots, b_m)$ is the list of *control points* of the curve (control points need not be distinct).

Remark: Because $B_0^m(t) + \cdots + B_m^m(t) = 1$ and $B_i^m(t) \geq 0$ when $t \in [0,1]$, the curve segment $C[0,1]$ corresponding to $t \in [0,1]$ belongs to the convex hull of the control points. This is an important property of Bézier curves which is used in geometric modeling to find the intersection of curve segments. Bézier curves play an important role in computer graphics and geometric modeling, but also in robotics because they can be used to model the trajectories of moving objects.

Problem B5 (40 pts). (a) Let A be an $n \times n$ matrix. If A is invertible, prove that for any $x \in \mathbb{R}^n$, if $Ax = 0$, then $x = 0$.

The converse is true: If for all $x \in \mathbb{R}^n$, $Ax = 0$ implies that $x = 0$, then A is invertible. We will prove this fact later, and you may use it without proof in part (b) of this problem.

(b) Let A be an $m \times n$ matrix and let B be an $n \times m$ matrix. Prove that $I_m - AB$ is invertible iff $I_n - BA$ is invertible.

Hint. Look at $A(I - BA)$ and $(I - AB)A$.

Problem B6 (40 pts). Consider the following $n \times n$ matrix, for $n \geq 3$:

$$B = \begin{pmatrix} 1 & -1 & -1 & -1 & \cdots & -1 & -1 \\ 1 & -1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & -1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & -1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & -1 & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 & -1 \end{pmatrix}$$

(1) If we denote the columns of B by $b_1, \ldots, b_n$, prove that

$$\begin{aligned} (n-3)b_1 - (b_2 + \cdots + b_n) &= 2(n-2)e_1 \\ b_1 - b_2 &= 2(e_1 + e_2) \\ b_1 - b_3 &= 2(e_1 + e_3) \\ \vdots \qquad & \qquad \vdots \\ b_1 - b_n &= 2(e_1 + e_n), \end{aligned}$$

where $e_1, \ldots, e_n$ are the canonical basis vectors of $\mathbb{R}^n$.

(2) Prove that B is invertible and that its inverse $A = (a_{ij})$ is given by

$$a_{11} = \frac{(n-3)}{2(n-2)}, \quad a_{i1} = -\frac{1}{2(n-2)} \quad 2 \leq i \leq n$$

and

$$\begin{aligned} a_{ii} &= -\frac{(n-3)}{2(n-2)}, \quad 2 \leq i \leq n \\ a_{ji} &= \frac{1}{2(n-2)}, \quad 2 \leq i \leq n, j \neq i. \end{aligned}$$

(3) Show that the n diagonal $n \times n$ matrices D_i defined such that the diagonal entries of D_i are equal the entries (from top down) of the ith column of B form a basis of the space of $n \times n$ diagonal matrices (matrices with zeros everywhere except possibly on the diagonal). For example, when $n = 4$, we have

$$D_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad D_2 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$D_3 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad D_4 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Problem B7 (20 pts). For any integer $n > 0$, recall that $\mathbb{Z}/n\mathbb{Z}$ denotes the set of equivalence classes of $\mathbb{Z}$ modulo n, which in bijection with the set $\{0, 1, \ldots, n-1\}$. We can define addition and multiplication modulo n but here we are more interested in multiplication, so for $a, b \in \{0, 1, \ldots, n\}$, we let

$$a \cdot b = ab \pmod{n},$$

which is the remainder of the division of ab by n.

From now on assume that $n \geq 2$. It is a bit tedious to verify that $\mathbb{Z}/n\mathbb{Z}$ with the above multiplication is an abelian monoid with identity element 1. We have the following multiplication tables for $n = 2, 3, 4$, given only for nonzero arguments:

$n = 2$

$\cdot$	1
1	1

$n = 3$

$\cdot$	1	2
1	1	2
2	2	1

$n = 4$

$\cdot$	**1**	2	**3**
1	**1**	2	**3**
2	2	0	2
3	**3**	2	**1**

Observe that for $n = 4$, the nonzero elements $\{1, 2, 3\}$ do not have a group structure under multiplication, since $2 \cdot 2 = 0$. What is the set of invertible elements under multiplication? Is it a group?

(1) Construct the multiplication table of $\mathbb{Z}/5\mathbb{Z}$. Is the set of nonzero elements $\{1, 2, 3, 4\}$ a group under multiplication?

(2) Construct the multiplication table of $\mathbb{Z}/6\mathbb{Z}$. Is $(\mathbb{Z}/6\mathbb{Z}) - \{0\}$ a group under multiplication? What is the set of invertible elements under multiplication? Is is a group?

(3) **Extra credit (20 pts)**. Again, assume $n \geq 2$. The set of invertible elements of $\mathbb{Z}/n\mathbb{Z}$ under multiplication is a group denoted $(\mathbb{Z}/n\mathbb{Z})^*$. The group $(\mathbb{Z}/n\mathbb{Z})^*$ has $\varphi(n)$ elements, where $\varphi(n)$ is the number of integers a, with $1 \leq a \leq n-1$, which are relatively prime with n ($gcd(a, n) = 1$).

A *generator* of $(\mathbb{Z}/n\mathbb{Z})^*$ is an element $g \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $\{g, g^2, \ldots, g^{\varphi(n)} = 1\} = (\mathbb{Z}/n\mathbb{Z})^*$ (the fact that $g^{\varphi(n)} \equiv 1 \pmod{n}$ is a theorem of Euler). Find a generator of $(\mathbb{Z}/n\mathbb{Z})^*$ for $n = 2, 3, 4, 5, 6$. Does $(\mathbb{Z}/8\mathbb{Z})^*$ have a generator?

What is the next n for which $(\mathbb{Z}/n\mathbb{Z})^*$ does not have a generator?

Remark: Gauss proved that $(\mathbb{Z}/n\mathbb{Z})^*$ always have a generator if n is prime. The proof is nontrivial!

TOTAL: 295 + 60 points.