Homework 1 Solution

ECE 269: Linear Algebra and Applications
Homework #1 Solution
Instructor: Behrouz Touri

1. *Review of prior Linear Algebra: Properties of Matrix multiplication.* Let $A, B \in \mathbb{R}^{n\times n}$ be regular $n \times n$ real-valued matrices ($n \geq 2$). Prove or disprove the following claims:
   (a) $AB = BA$.
   (b) If $AB = 0$, then $A = 0$ or $B = 0$.
   (c) If $A^k = 0$ for all $k > 1$, then $A = 0$.
   (d) If $A'A = 0$, then $A = 0$.

   Solution:

   (a) **False**: Let $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$. Then $AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $BA = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.
   (b) **False**: Let $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. Then $AB = 0$.
   (c) **False**: Let $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Then $A^2 = 0$ and thus $A^k = 0$ for all $k > 1$.
   (d) **True**. Let $A = [A_{ij}]$ and $B = A'A$. Note that $B_{ii} = \sum_{j=1}^n A_{ji}^2$. So, if B is the zero matrix, then $B_{ii} = 0$ which implies $A_{ji} = 0$ for all j. This means that the ith column would be zero, and since this holds for all columns, it implies A is the zero matrix.

2. *Some set theory.* Let A, B, C be three sets.
   (a) Show that if $A \subseteq B$, then $A - C \subseteq B - C$ where $A - C = A \cap C^c$.
   (b) Is this true or not: $A \cup (B \cap C) = (A \cup B) \cap C$.

   Solution:

   (a) For any $x \in A - C$, $x \in A$ and $x \in C^c$. Since $A \subseteq B$ and $x \in A$, we deduce that $x \in B$. So, $x \in B \cap C^c = B - C$.
   (b) **False**: Let $C = \emptyset$. Then $A \cup (B \cap C) = A \cup \emptyset = A$ and $(A \cup B) \cap C = (A \cup B) \cap \emptyset = \emptyset$. So if $A \neq \emptyset$, the two terms are not equal.

3. *Finite field $GF(4)$.* As mentioned in the class, a field is a set equipped with two tables (operations), an addition table, and a multiplication table that are related through the distributive law.

   (a) Construct those tables for the set $\mathbb{F} = \{0, 1, a, b\}$ where 0 is the unity of the additive table and 1 is the unity of the multiplication table.
   (b) Given your answer in part (a), solve $a \cdot x + 1 = b$ (i.e., find $x \in \mathbb{F}$ that satisfies this identity).

(a) We will construct the multiplicative table first. Let $x = a^2, y = ab, z = b^2$:

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	x	y
b	0	b	y	z

Each row/column for 1, a, or b needs to have 1. We will show $y = 1$ by proving that $y \neq 1$ and $x = z = 1$ lead to a contradiction. Suppose $y \neq 1$ and $x = z = 1$, i.e. $a^{-1} = a$ and $b^{-1} = b$. If $y = a$, $ab = a$. By multiplying both sides by a^{-1}, we get $b = 1$, which is a contradiction. Similarly, $y = b$ leads to a contradiction. Therefore, we have $y = 1$, i.e. $a^{-1} = b$ and $b^{-1} = a$. We will show $x = b$ by showing contradictions. If $x = 1$, $a^2 = 1$. By multiplying both sides by $a^{-1} = b$, we have $a = b$, which is a contradiction. If $x = a$, $a^2 = a$. By multiplying both sides by a^{-1}, we have $a = 1$, which is also a contradiction. Therefore, $x = b$. Similarly, $z = a$.

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Next, we will construct the additive table. We define p, q, r, s, t, u as the following table:

$+$	0	1	a	b
0	0	1	a	b
1	1	p	q	r
a	a	q	s	t
b	b	r	t	u

Suppose $q = a+1 = 0$. Then $1 = -a$. By multiplying both sides of $a+1 = 0$ by a, we get $b + a = 0$. Since $b = -a = 1$, this is a contradiction. Therefore, $q \neq 0$. Similarly, $r \neq 0$ and $t \neq 0$. Since each row/column has 0, $p = s = u = 0$. If $q = 1$, $a = 0$ (contradiction). If $q = a$, $1 = 0$ (contradiction). Therefore, $q = b$. Similarly, $r = a$ and $t = 1$.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

(b) $ax + 1 = b$ is equivalent to $ax = b + (-1) = b + 1 = a$. So, $x = 1$.

4. *Field Properties.* Let $(\mathbb{F}, +, \cdot)$ be a field with the additive identity element z and multiplicative identity element o. Prove the following.

   (a) For all $a \in \mathbb{F}$, $z \cdot a = z$.

   (b) Show that if $\mathbb{F}$ is finite, and $a \neq z$, then $a^q = o$ for some $q \geq 1$.

Solution:

(a) By distributivity and additive identity, we have

$$z \cdot a = (z + z) \cdot a = z \cdot a + z \cdot a.$$

Moreover, by additive inverse,

$$z = z \cdot a + (-z \cdot a) = z \cdot a + z \cdot a + (-z \cdot a) = z \cdot a + z = z \cdot a.$$

(b) Since $\mathbb{F}$ is finite, there exist q_1 and $q_2 \geq 1$ with $q_1 < q_2$ such that $a^{q_1} = a^{q_2}$. Since any two nonzero elements' multiplication is not zero (in our case, z), we know both a^{q_1} and a^{q_2} are not zero. Therefore, there exists the multiplicative inverse $(a^{q_1})^{-1}$ and we have

$$o = (a^{q_1})^{-1} a^{q_1} = (a^{q_1})^{-1} a^{q_2}.$$

Also observe that by associativity of multiplication, $(a^{-1})^{q_1} a^{q_1} = o$. So, $(a^{-1})^{q_1} = (a^{q_1})^{-1}$ and $o = (a^{-1})^{q_1} a^{q_2} = a^{q_2 - q_1}$. Now we prove our assertion with $q = q_2 - q_1$.

5. *Subspaces.* Let $\mathcal{V}$ and $\mathcal{W}$ be subspaces of a vector space. Which of the following is also a subspace?

(a) *Minkowski sum* $\mathcal{V} + \mathcal{W} = \{v + w : v \in \mathcal{V}, \, w \in \mathcal{W}\}$.

(b) $\mathcal{V} \cap \mathcal{W}$.

(c) $\mathcal{V} \cup \mathcal{W}$.

For each case, either verify that it is a subspace or prove otherwise. **Solution:**

(a) This is a subspace.
Suppose that $u, v \in \mathcal{V} + \mathcal{W}$. Then, by the definition, $u = s + x$ and $v = t + y$ for some $s, t \in V, x, y \in W$. Therefore, for any $a \in F$ we have:

i. Since $s + t \in V$ and $x + y \in W$, $(s + x) + (t + y) = (s + t) + (x + y) = u + v \in V + W$.

ii. Since $as \in V$ and $ax \in W$, $a(s + x) = as + ax = av \in V + W$.

(b) This is a subspace.
Suppose $x, y \in V \cap W, a \in F$, i.e., $x, y \in V$ and $x, y \in W$.

i. Since V, W are subspaces, $x + y \in V$ and $x + y \in W$, $x + y \in V \cap W$.

ii. Similarly, $ax \in V$ and $ax \in W$, therefore $ax \in V \cap W$.

(c) This is not a subspace.
For example, suppose $V = \{[x, 0] \in \mathbb{R}^2\}$ and $W = \{[0, y] \in \mathbb{R}^2\}$. $[x, 0] + [0, y] = [x, y] \notin V \cup W$. Since the set is not closed with respect to addition, it is not a vector space.

6. *Bases.* Find a basis for each of the following subspaces of $\mathbb{R}^4$.

(a) All vectors whose components are equal.

(b) All vectors whose components sum to zero.

(c) All vectors orthogonal to both $\begin{bmatrix} 1 & 0 & 1 & 0 \end{bmatrix}'$ and $\begin{bmatrix} 0 & 1 & 0 & 1 \end{bmatrix}'$.

(d) All vectors spanned by $\begin{bmatrix} 1 & 1 & 0 & 0 \end{bmatrix}'$, $\begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix}'$, $\begin{bmatrix} 0 & 0 & 1 & 1 \end{bmatrix}'$, and $\begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}'$

Repeat parts (a)–(d) for $\mathbb{Z}_2^4$ instead of $\mathbb{R}^4$.

Solution:

(a) $\{\begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}'\}$ is a basis for the subspace.

(b) $\{\begin{bmatrix}1 & 0 & 0 & -1\end{bmatrix}', \begin{bmatrix}0 & 1 & 0 & -1\end{bmatrix}', \begin{bmatrix}0 & 0 & 1 & -1\end{bmatrix}'\}$ is a basis for the subspace.

Let $x = \begin{bmatrix}a & b & c & d\end{bmatrix}' \in \mathbb{R}^4$. Since the components sum to zero, $a + b + c + d = 0$. i.e., $d = -a - b - c$. Therefore, the subspace is $\{x = a\begin{bmatrix}1 & 0 & 0 & -1\end{bmatrix}' + b\begin{bmatrix}0 & 1 & 0 & -1\end{bmatrix}' + c\begin{bmatrix}0 & 0 & 1 & -1\end{bmatrix}' | a, b, c \in \mathbb{R}\}$. Since $\begin{bmatrix}1 & 0 & 0 & -1\end{bmatrix}', \begin{bmatrix}0 & 1 & 0 & -1\end{bmatrix}', \begin{bmatrix}0 & 0 & 1 & -1\end{bmatrix}'$ span the subspace and they are linearly independent, they form a basis.

(c) $\{\begin{bmatrix}1 & 0 & -1 & 0\end{bmatrix}', \begin{bmatrix}0 & 1 & 0 & -1\end{bmatrix}'\}$ is a basis for the subspace.

Let $x = \begin{bmatrix}a & b & c & d\end{bmatrix}' \in \mathbb{R}^4$. Since x is orthogonal to both $\begin{bmatrix}1 & 0 & 1 & 0\end{bmatrix}'$ and $\begin{bmatrix}0 & 1 & 0 & 1\end{bmatrix}'$, $\begin{bmatrix}1 & 0 & 1 & 0\end{bmatrix} x = a + c = 0$ and $\begin{bmatrix}0 & 1 & 0 & 1\end{bmatrix} x = b + d = 0$. Hence, $c = -a, d = -b$. Therefore, the subspace is $\{x = a\begin{bmatrix}1 & 0 & -1 & 0\end{bmatrix}' + c\begin{bmatrix}0 & 1 & 0 & -1\end{bmatrix}' | a, c \in \mathbb{R}\}$. Since $\begin{bmatrix}1 & 0 & -1 & 0\end{bmatrix}', \begin{bmatrix}0 & 1 & 0 & -1\end{bmatrix}'$ span the subspace and they are linearly independent, they form a basis.

(d) $\{\begin{bmatrix}1 & 1 & 0 & 0\end{bmatrix}', \begin{bmatrix}0 & 1 & 1 & 0\end{bmatrix}', \begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix}'\}$ is a basis for the subspace.

Since these vectors are independent and $\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}' = \begin{bmatrix}1 & 1 & 0 & 0\end{bmatrix}' - \begin{bmatrix}0 & 1 & 1 & 0\end{bmatrix}' + \begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix}'$, they form a basis for $\text{span}\{\begin{bmatrix}1 & 1 & 0 & 0\end{bmatrix}', \begin{bmatrix}0 & 1 & 1 & 0\end{bmatrix}', \begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix}', \begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}'\}$.

We will consider $\mathbb{Z}_2^4$ instead of $\mathbb{R}^4$.

(a) $\{\begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}'\}$ is a basis for the subspace.

Let $x = \begin{bmatrix}a & b & c & d\end{bmatrix}' \in \mathbb{Z}_2^4$. Since the components are equal, $a = b = c = d$. Therefore, the subspace is $\{x = a\begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}' | a \in \mathbb{Z}_2\}$. Since a vector $\begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}'$ spans the subspace, it is a basis.

(b) $\{\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}', \begin{bmatrix}0 & 1 & 0 & 1\end{bmatrix}', \begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix}'\}$ is a basis for the subspace.

Let $x = \begin{bmatrix}a & b & c & d\end{bmatrix}' \in \mathbb{Z}_2^4$. Since the components sum to zero, $a + b + c + d = 0$. i.e., $d = a + b + c$. Therefore, the subspace is $\{x = a\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}' + b\begin{bmatrix}0 & 1 & 0 & 1\end{bmatrix}' + c\begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix}' | a, b, c \in \mathbb{Z}_2\}$. Since $\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}', \begin{bmatrix}0 & 1 & 0 & 1\end{bmatrix}', \begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix}'$ span the subspace and they are linearly independent, they form a basis.

(c) $\{\begin{bmatrix}1 & 0 & 1 & 0\end{bmatrix}', \begin{bmatrix}0 & 1 & 0 & 1\end{bmatrix}'\}$ is a basis for the subspace.

Let $x = \begin{bmatrix}a & b & c & d\end{bmatrix}' \in \mathbb{Z}_2^4$. Since x is orthogonal to both $\begin{bmatrix}1 & 0 & 1 & 0\end{bmatrix}'$ and $\begin{bmatrix}0 & 1 & 0 & 1\end{bmatrix}'$, $\begin{bmatrix}1 & 0 & 1 & 0\end{bmatrix} x = a + c = 0$ and $\begin{bmatrix}0 & 1 & 0 & 1\end{bmatrix} x = b + d = 0$. Hence, $c = -a = (-1+2)a = a, d = -b = (-1+2)b = b$. Therefore, the subspace is $\{x = a\begin{bmatrix}1 & 0 & 1 & 0\end{bmatrix}' + c\begin{bmatrix}0 & 1 & 0 & 1\end{bmatrix}' | a, c \in \mathbb{Z}_2\}$. Since $\begin{bmatrix}1 & 0 & 1 & 0\end{bmatrix}', \begin{bmatrix}0 & 1 & 0 & 1\end{bmatrix}'$ span the subspace and they are linearly independent, they form a basis.

(d) $\{\begin{bmatrix}1 & 1 & 0 & 0\end{bmatrix}', \begin{bmatrix}0 & 1 & 1 & 0\end{bmatrix}', \begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix}'\}$ is a basis for the subspace.

Since these vectors are independent and $\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}' = \begin{bmatrix}1 & 1 & 0 & 0\end{bmatrix}' + \begin{bmatrix}0 & 1 & 1 & 0\end{bmatrix}' + \begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix}'$, they are a basis for $\text{span}\{\begin{bmatrix}1 & 1 & 0 & 0\end{bmatrix}', \begin{bmatrix}0 & 1 & 1 & 0\end{bmatrix}', \begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix}', \begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}'\}$.