Solutions to Homework Set #1

1. Linear functions over $\mathbb{F}^n$.

(a) Show that the function $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ defined by $f(x) = Ax$, where $A \in \mathbb{F}^{m \times n}$, is linear.

(b) Show that any linear function $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ has a representation $f(x) = Ax$ for some $A \in \mathbb{F}^{m \times n}$.

(c) Show that the representation in part (b) is unique by proving that $Ax = Bx$ for every $x$ implies that $A = B$.

Solution:

(a) For any $x_1, x_2 \in \mathbb{F}^n$ and $\alpha_1, \alpha_2 \in \mathbb{F}$, we have

\[
f(\alpha_1 x_1 + \alpha_2 x_2) = A(\alpha_1 x_1 + \alpha_2 x_2) \\
= \alpha_1 Ax_1 + \alpha_2 Ax_2 \\
= \alpha_1 f(x_1) + \alpha_2 f(x_2),
\]

which shows that $f$ is linear. Here, (1) follows from the properties of matrix multiplication.

(b) Every $x = [x_1 \ x_2 \ \cdots \ x_n]' \in \mathbb{F}^n$ can be written as

\[
x = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n,
\]

where $e_k \in \mathbb{F}^n$ is the (column) vector $[0 \ 0 \ \cdots \ 1 \ \cdots \ 0]'$ that consists of 1 in the $k$-th position and 0’s everywhere else. Let $f(e_k) = v_k \in \mathbb{F}^m$, $k = 1, 2, \ldots, n$. We then have, by the linearity of $f$,

\[
f(x) = f(x_1 e_1 + x_2 e_2 + \cdots + x_n e_n) \\
= x_1 f(e_1) + x_1 f(e_1) + \cdots + x_n f(e_n) \\
= x_1 v_1 + x_2 v_2 + \cdots + x_n v_n \\
= Ax,
\]

where

\[
A := [v_1 \ v_2 \ \cdots \ v_n] = [f(e_1) \ f(e_2) \ \cdots \ f(e_n)] \in \mathbb{F}^{m \times n}.
\]

This construction can be applied for any linear function $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$.

(c) Suppose $Ax = Bx$ for every $x \in \mathbb{F}^n$. Then, choosing $x = e_k$, we see that $Ae_k = Be_k$, or in other words, the $k$-th columns of $A$ and $B$ are identical. This holds for $k = 1, 2, \ldots, n$, whence $A = B$. 

1
2. A linear function from convolution. Suppose that real-valued sequences \( \{u(n)\}_{n=-\infty}^{\infty} \) and \( \{v(n)\}_{n=-\infty}^{\infty} \) represent the input and output signals of a discrete-time linear time-invariant system with impulse response \( h(n) \in \mathbb{R}, \ n \in \mathbb{Z} \). Then, \( \{u(n)\} \) and \( \{v(n)\} \) are related via convolution as

\[
v(n) = \sum_{k=-\infty}^{\infty} h(k)u(n-k), \quad n \in \mathbb{Z}.
\]

Suppose that \( u(n) = 0 \) for \( n < 0 \) or \( n > N \), and define

\[
x = \begin{bmatrix} u(0) \\ u(1) \\ \vdots \\ u(N) \end{bmatrix} \quad \text{and} \quad y = \begin{bmatrix} v(0) \\ v(1) \\ \vdots \\ v(N) \end{bmatrix}.
\]

Thus \( x \) and \( y \) are vectors that capture \( N+1 \) values of the input and output signals, respectively.

(a) Find the matrix \( T \) such that

\[
y = Tx
\]

in terms of \( h(n) \).

(b) Describe the structure of \( T \). Matrices of this structure is said to be Toeplitz.

Solution:

(a) We have

\[
v(n) = \sum_{k=-\infty}^{\infty} h(k)u(n-k) = \sum_{l=-\infty}^{\infty} h(n-l)u(l) = \sum_{l=0}^{N} h(n-l)u(l),
\]

where the last equality follows since \( \{u(l)\} \) is supported only on \( \{0,1,\ldots,N\} \). We therefore have, for \( n = 0, 1, \ldots, N \),

\[
v(n) = a^T_n x,
\]

where \( a_n := [h(n) \ h(n-1) \ \cdots \ h(n-N)]' \). Thus,

\[
y = \begin{bmatrix} v(0) \\ v(1) \\ \vdots \\ v(N) \end{bmatrix}
\]

\[
= \begin{bmatrix} a^T_0 \\ a^T_1 \\ \vdots \\ a^T_N \end{bmatrix} x
\]

\[
= \begin{bmatrix} h(0) & h(-1) & \cdots & h(-N) \\ h(1) & h(0) & \cdots & h(-N+1) \\ \vdots & \vdots & \ddots & \vdots \\ h(N) & h(N-1) & \cdots & h(0) \end{bmatrix} x =: Tx
\]
where $T$ is the matrix whose $(i,j)^{th}$ entry is given by $h(i - j)$, for $1 \leq i \leq N + 1$ and $1 \leq j \leq N + 1$.

(b) Each descending diagonal in $T$ from left to right is constant, or in other words, the $(i,j)$ element of $T$ depends only on $(i - j)$. Square matrices with this structure are called Toeplitz.

3. **Matrix multiplication.** Let $A, B \in \mathbb{R}^{n \times n}$. Prove or provide a counterexample to each of the following statements.

(a) If $AB = 0$, then $A = 0$ or $B = 0$.
(b) If $A^2 = 0$, then $A = 0$.
(c) If $A'A = 0$, then $A = 0$.

**Solution:**

(a) Let

$$A = \begin{bmatrix}
1 & 0 & 0 & \cdots & 0 \\
1 & 0 & 0 & \cdots & 0 \\
1 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 0 & 0 & \cdots & 0 
\end{bmatrix} = \begin{bmatrix}
e'_1 \\
e'_2 \\
e'_3 \\
\vdots \\
e'_{n-1} \\
\vdots \\
1 & 0 & 0 & \cdots & 0
\end{bmatrix}$$

and $B = \begin{bmatrix}
0 & 0 & 0 & \cdots & 0 \\
1 & 1 & 1 & \cdots & 1 \\
0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0
\end{bmatrix} = \begin{bmatrix}e_2 & e_2 & e_2 & \cdots & e_2\end{bmatrix}$.

Then, $AB = 0$, but neither $A$ nor $B$ is itself 0. Thus the statement is false.

(b) Consider

$$A = \begin{bmatrix}1 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0
\end{bmatrix},$$

i.e., $A_{ij} = 1$ if $i = 1$ and $j = n$, and $A_{ij} = 0$ otherwise. Then, $A^2 = 0$ but $A \neq 0$. Thus the statement is false.

(c) Let $B = A'A$. Then, we have, for $1 \leq i \leq n$,

$$B_{ii} = \sum_{j=1}^{n} A_{ij}A_{ij}$$

$$= \sum_{j=1}^{n} A_{ij}^2.$$ 

Thus, $B_{ii} = 0$ implies $A_{ij} = 0$ for every $j \in \{1, 2, \ldots, n\}$. This shows that that $A'A = 0$ implies $A = 0$. 

3
Note that this does not hold for $A \in \mathbb{F}_2^{n \times n}$. Consider, for example,

$$A = \begin{bmatrix}
1 & 1 & 1 & 1 & \cdots & 1 \\
1 & 1 & 1 & 1 & \cdots & 1 \\
0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 0
\end{bmatrix} \in \mathbb{F}_2^{n \times n}.
$$

Then, $A' A = 0$ but $A \neq 0$.

4. **Affine functions.** A function $f : \mathbb{R}^n \to \mathbb{R}^m$ is said to be **affine** if for any $x, y \in \mathbb{R}^n$ and any $\alpha, \beta \in \mathbb{R}$ with $\alpha + \beta = 1$, we have

$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y).$$

Note that without the restriction $\alpha + \beta = 1$, this would be the definition of linearity.

(a) Suppose that $A \in \mathbb{R}^{m \times n}$ and $b \in \mathbb{R}^m$. Show that the function $f(x) = Ax + b$ is affine.

(b) Prove the converse, namely, show that any affine function $f$ can be represented uniquely as $f(x) = Ax + b$ for some $A \in \mathbb{R}^{m \times n}$ and $b \in \mathbb{R}^m$.

(Hint: Consider the linearity of the function $g(x) = f(x) - f(0)$.)

**Solution:**

(a) Let $\alpha, \beta \in \mathbb{R}$ be such that $\alpha + \beta = 1$, and let $x, y \in \mathbb{R}^n$. Then, we have

$$f(\alpha x + \beta y) = A(\alpha x + \beta y) + b$$

$$= \alpha Ax + \beta Ay + (\alpha + \beta)b$$

$$= \alpha(Ax + b) + \beta(Ay + b)$$

$$= \alpha f(x) + \beta f(y),$$

which shows that $f$ is affine.

(b) Let $f$ be an affine function from $\mathbb{R}^n$ to $\mathbb{R}^m$, and let $g(x) := f(x) - f(0)$. We know that

$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y) \quad (2)$$

for all $x, y \in \mathbb{R}^n$ and $\alpha + \beta = 1$. Using 0 in place of $y$ in (2), we have, for all $x \in \mathbb{R}^n$ and $\alpha \in \mathbb{R}$, $f(\alpha x) = \alpha f(x) + (1 - \alpha)f(0)$. We then have, for $x, y \in \mathbb{R}^n$ and $\alpha \in \mathbb{R}$,

$$g(\alpha x) = f(\alpha x) - f(0)$$

$$= \alpha f(x) + (1 - \alpha)f(0) - f(0)$$

$$= \alpha(f(x) - f(0))$$

$$= \alpha g(x)$$
and
\[
g(x + y) = f(x + y) - f(0) \\
= f \left( 2 \left( \frac{1}{2} x + \frac{1}{2} y \right) \right) - f(0) \\
= 2f \left( \frac{1}{2} x + \frac{1}{2} y \right) - (f(0) - f(0)) \\
= 2 \left( \frac{1}{2} f(x) + \frac{1}{2} f(y) \right) - f(0) - f(0) \\
= f(x) - f(0) + f(y) - f(0) \\
= g(x) + g(y),
\]
which shows that \( g \) is linear, whence, from Problem 1, parts (b) and (c), \( g(x) \) can be represented uniquely as \( g(x) = Ax \) for some \( A \in \mathbb{R}^{m \times n} \). Letting \( f(0) =: b \in \mathbb{R}^m \), we thus see that any affine function \( f \) can be uniquely represented as \( f(x) = Ax + b \) for some \( A \in \mathbb{R}^{m \times n} \) and \( b \in \mathbb{R}^m \).

5. **Symmetric and Hermitian matrices.** A square matrix \( A \) is said to be symmetric if its transpose \( A' \) satisfies \( A' = A \), and a complex-valued square matrix \( A \) is said to be Hermitian if its conjugate transpose \( A^* = (\overline{A})' = \overline{A'} \) satisfies \( A^* = A \). Thus, a real-valued square matrix \( A \) is symmetric if and only if it is Hermitian. Which of the following is a vector space?

(a) The set of all \( n \times n \) real-valued symmetric matrices over \( \mathbb{R} \).
(b) The set of all \( n \times n \) complex-valued symmetric matrices over \( \mathbb{C} \).
(c) The set of all \( n \times n \) complex-valued Hermitian matrices over \( \mathbb{R} \).
(d) The set of all \( n \times n \) complex-valued Hermitian matrices over \( \mathbb{C} \).

For each case, either verify that it is a vector space or prove otherwise.

**Solution:**

(a) It is easy to check that the sum of two real symmetric matrices is also real and symmetric, as is the product of a real scalar and a real symmetric matrix. These prove the closure under vector addition and scalar multiplication, respectively. The rest of the axioms follow directly as a consequence of elementary properties of matrix addition and scalar multiplication. Thus, it is a vector space.

(b) It is easy to check that the sum of two complex symmetric matrices is also complex and symmetric, as is the product of a complex scalar and a complex symmetric matrix. These prove the closure under vector addition and scalar multiplication, respectively. The rest of the axioms follow directly as a consequence of elementary properties of matrix addition and scalar multiplication. Thus, it is a vector space.

(c) It is easy to check that the sum of two complex Hermitian matrices is a complex Hermitian matrix, as is the product of a real scalar and a complex Hermitian matrix. These prove the closure under vector addition and scalar multiplication, respectively. The rest of the axioms follow directly as a consequence of elementary properties of matrix addition and scalar multiplication. Thus, it is a vector space.
(d) A necessary (but not sufficient) condition for a matrix to be Hermitian is that the diagonal entries are real. Now, consider a Hermitian matrix $A$ and the complex scalar $i$. Then, $i \cdot A$ has diagonal entries that are not real and, therefore, is not Hermitian. Thus, closure under scalar multiplication fails to hold, and it is not a vector space.

6. **Subspaces.** Let $V$ and $W$ be subspaces of a vector space. Which of the following is also a subspace?

   (a) Minkowski sum $V + W = \{ v + w : v \in V, w \in W \}$.
   (b) $V \cap W$.
   (c) $V \cup W$.

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

**Solution:**

(a) Let $S := V + W$. Let $s_1, s_2 \in S$, $s_1 = v_1 + w_1$, and $s_2 = v_2 + w_2$, where $v_1, v_2 \in V$ and $w_1, w_2 \in W$. Also, let $a, b \in F$. Then, we have the following:

   i. Closure under vector addition and scalar multiplication:

   $$\alpha s_1 + \beta s_2 = \alpha (v_1 + w_1) + \beta (v_2 + w_2)$$

   $$= (\alpha v_1 + \beta v_2) + (\alpha w_1 + \beta w_2) \in S,$$

   since $\alpha v_1 + \beta v_2 \in V$ and $\alpha w_1 + \beta w_2 \in W$.

   ii. Additive identity: Since $0 \in V$ and $0 \in W$, $0 = 0 + 0 \in S$.

   Thus, $S$ is a subspace.

(b) Let $U := V \cap W$. Then, $0 \in V$ and $0 \in W$, therefore $0 \in U$. Also, let $a, b \in F$ and $u_1, u_2 \in U$. Then, $u_1, u_2 \in V$ and $u_1, u_2 \in W$, therefore $\alpha u_1 + \beta u_2 \in V$ and $\alpha u_1 + \beta u_2 \in W$, whence $\alpha u_1 + \beta u_2 \in U$. Thus, $U$ is a subspace.

(c) Let us consider the vector space $\mathbb{R}^3$ over $\mathbb{F}$, and let $V = \{ [x \ 0 \ 0]' : x \in \mathbb{R} \}$, and $W = \{ [0 \ y \ z]' : y, z \in \mathbb{R} \}$. Then, both $V$ and $W$ are subspaces. Now, consider $U := V \cup W$. The vectors $u_1 := [1 \ 0 \ 0]'$ and $u_2 := [0 \ 1 \ 1]'$ are in $U$ by definition, but $u_1 + u_2 = [1 \ 1 \ 1]' \notin U$. Therefore, $U$ is not a subspace in this case.

7. **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 $[1 \ 1 \ 0 \ 0]'$ and $[0 \ 0 \ 1 \ 1]'$.
   (d) All vectors spanned by $[1 \ 1 \ 0 \ 0]'$, $[0 \ 1 \ 1 \ 0]'$, $[0 \ 0 \ 1 \ 1]'$, and $[1 \ 0 \ 0 \ 1]'$

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

**Solution:** $\mathbb{R}^4$. 

6
(a) The set of all vectors whose components are equal can be expressed as
\[ \{ [\alpha,\alpha,\alpha] : \alpha \in \mathbb{R} \} = \{ \alpha \cdot [1,1,1]^\prime : \alpha \in \mathbb{R} \} \]

Therefore, \([1 \enspace 1 \enspace 1 \enspace 1]^\prime\) is a basis for this subspace.

(b) The subspace can be expressed as
\[ \{ [\alpha \beta \gamma \delta] : \alpha,\beta,\gamma,\delta \in \mathbb{R}, \alpha + \beta + \gamma + \delta = 0 \} = \{ [\alpha,\beta,-\alpha - \beta - \delta] : \alpha,\beta,\gamma \in \mathbb{R} \} \]
\[ = \left\{ \alpha \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \\ 0 \\ -1 \end{bmatrix} + \gamma \begin{bmatrix} 0 \\ 0 \\ 1 \\ -1 \end{bmatrix}, \alpha,\beta,\gamma \in \mathbb{R} \right\} \]

Thus, the subspace is given by \(\text{span}([1 \enspace 0 \enspace 0 \enspace -1]^\prime, [0 \enspace 1 \enspace 0 \enspace -1]^\prime, [0 \enspace 0 \enspace 1 \enspace -1]^\prime)\).
One can verify that this collection of three vectors is also linearly independent, therefore it is a basis for the subspace.

(c) The subspace can be expressed as
\[ \{ [\alpha,\beta,\gamma,\delta] : \alpha,\beta,\gamma,\delta \in \mathbb{R}, \alpha + \beta = \gamma + \delta = 0 \} = \{ [\alpha,-\alpha,\gamma,-\gamma] : \alpha,\gamma \in \mathbb{R} \} \]
\[ = \left\{ \alpha \begin{bmatrix} 1 \\ -1 \\ 0 \\ 0 \end{bmatrix} + \gamma \begin{bmatrix} 0 \\ 0 \\ 1 \\ -1 \end{bmatrix}, \alpha,\gamma \in \mathbb{R} \right\} \]

Thus, the subspace is given by \(\text{span}([1 \enspace -1 \enspace 0 \enspace 0]^\prime, [0 \enspace 0 \enspace 1 \enspace -1]^\prime)\). One can verify that these two vectors are also linearly independent, therefore they form a basis for the subspace.

(d) We have
\[ \alpha_1 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \alpha_3 \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \alpha_4 \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha_1 + \alpha_4 \\ \alpha_1 + \alpha_2 \\ \alpha_2 + \alpha_3 \\ \alpha_1 + \alpha_4 - (\alpha_1 + \alpha_2) + (\alpha_2 + \alpha_3) \end{bmatrix} \]

Therefore, the subspace can be expressed as
\[ \{ [\beta_1,\beta_2,\beta_3,\beta_1 - \beta_2 + \beta_3]^\prime : \beta_1,\beta_2,\beta_3 \in \mathbb{R} \} \]
\[ = \left\{ \beta_1 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \beta_2 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \beta_3 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \beta_1,\beta_2,\beta_3 \in \mathbb{R} \right\} \]
\[ = \text{span}([1 \enspace 0 \enspace 0 \enspace 1]^\prime, [0 \enspace 1 \enspace 0 \enspace -1]^\prime, [0 \enspace 0 \enspace 1 \enspace -1]^\prime) \]

As before, this latter set is independent and therefore, forms a basis for the subspace. \(\mathbb{F}_2^4\).
(a) The same as before.

(b) The same as before, except that now, $-1$ is the same as $1$, therefore the basis can be expressed more simply as $\{(1 \ 0 \ 0 \ 1)', (0 \ 1 \ 0 \ 1)', (0 \ 0 \ 1 \ 1)\}$.

(c) The subspace can be expressed as

$$\{[\alpha, \beta, \gamma, \delta]' : \alpha, \beta, \gamma, \delta \in \mathbb{F}_2, \alpha + \beta = \gamma + \delta = 0\} = \{[\alpha, \alpha, \gamma, \gamma]' : \alpha, \gamma \in \mathbb{F}_2\}$$

$$= \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \alpha, \gamma \in \mathbb{F}_2 \right\}.$$ 

Thus, the subspace is given by $\text{span}([1 \ 1 \ 0 \ 0]', [0 \ 0 \ 1 \ 1])$. One can verify that these two vectors are also linearly independent, therefore they form a basis for the subspace.

(d) We have

$$\alpha_1 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \alpha_3 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \alpha_4 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha_1 + \alpha_4 \\ \alpha_1 + \alpha_2 \\ \alpha_2 + \alpha_3 \\ (\alpha_1 + \alpha_4) + (\alpha_1 + \alpha_2) + (\alpha_2 + \alpha_3) \end{bmatrix}.$$ 

Therefore, the subspace can be expressed as

$$\{[\beta_1, \beta_2, \beta_3, \beta_1 + \beta_2 + \beta_3]' : \beta_1, \beta_2, \beta_3 \in \mathbb{F}_2\}$$

$$= \left\{ \beta_1 \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} + \beta_2 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} + \beta_3 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \beta_1, \beta_2, \beta_3 \in \mathbb{F}_2 \right\}$$

$$= \text{span}([1 \ 0 \ 0 \ 1]', [0 \ 1 \ 0 \ 1]', [0 \ 0 \ 1 \ 1]').$$

As before, this latter set is independent and therefore, forms a basis for the subspace.