Solutions to Homework Set #2

1. Differentiation of polynomials. Let $P_n$ be the vector space consisting of all polynomials of degree $\leq n$ with real coefficient.

(a) Show that the monomials $x^i, i = 0, 1, \ldots, n,$ form a basis for $P_n.$

(b) Consider the transformation $T : P_n \to P_n$ defined by

$$T(p(x)) = \frac{dp(x)}{dx}.$$ 

For example, $T(1 + 3x + x^2) = 3 + 2x.$ Show that $T$ is linear.

(c) Using $\{1, x, \ldots, x^n\}$ as a basis, represent the transformation in part (b) by a matrix $A \in \mathbb{R}^{(n+1) \times (n+1)}.$ Find the rank of $A.$

(d) Characterize the nullspace of $A.$

Solution:

(a) Let $\alpha_0, \alpha_1, \ldots, \alpha_n \in \mathbb{R}$ be such that $\sum_{i=0}^{n} \alpha_i x^i$ is equal to the zero polynomial. Then, $\alpha_0 = \cdots = \alpha_n = 0,$ which shows that $\{x^i, i = 0, 1, 2, \ldots, n\}$ is independent. Moreover, any polynomial $P(x)$ of degree $\leq n$ can be expressed in terms of the coefficients of different powers of $x$ as

$$P(x) \equiv c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$$

and for every $c_0, \ldots, c_n \in \mathbb{R}, c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$ is a polynomial of degree $\leq n$ with real coefficients. Therefore, $P_n = \text{span}(1, x, \ldots, x^n).$ These two properties show that $\{x^i, i = 0, 1, \ldots, n\}$ is a basis for $P_n.$

(b) By elementary properties of the derivative, we have $T(\alpha p(x)) = \alpha T(p(x))$ for all $\alpha \in \mathbb{R},$ and $T(p(x) + q(x)) = T(p(x)) + T(q(x))$ for every $p(x), q(x) \in P_n.$ Therefore, $T$ is linear.

(c) Let $e_i := x^{i-1}, 1 \leq i \leq n.$ Then, we have $T(e_i) = (i - 1)e_{i-1}$ for $i = 2, 3, \ldots, n + 1,$ and $T(e_1) = 0.$ Therefore, using part (b) of Problem 1, we can represent $T$ by a matrix $A$ defined as

$$A = \begin{bmatrix} T(e_1) & T(e_2) & \cdots & T(e_{n+1}) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 2 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & n \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$
2. **Zero nullspace.** Let \( A \in F^{m \times n} \). Prove that the following statements are equivalent.

- (a) \( \mathcal{N}(A) = \{0\} \).
- (b) \( A' \) is onto (i.e., \( \mathcal{R}(A') = F^n \)).
- (c) Columns of \( A \) are independent.
- (d) \( A \) is tall (i.e., \( n \leq m \)) and full-rank (i.e., \( \text{rank}(A) = \min(m, n) = n \)).

**Solution:** We will show the chain of equivalences (a) \( \implies \) (b) \( \implies \) (c) \( \implies \) (d) \( \implies \) (a).

- (a) \( \implies \) (b): By the rank–nullity theorem, we have \( \dim(\mathcal{N}(A)) + \text{rank}(A) = n \), which implies \( \text{rank}(A) = n \) (since \( \dim(\mathcal{N}(A)) = 0 \)). Since \( \text{rank}(A) = \text{rank}(A') \), we then have \( \text{rank}(A') = n \).
- (b) \( \implies \) (c): Since \( A' \) is onto, \( \text{rank}(A') = \dim(\mathcal{R}(A')) = n \). Because \( \text{rank}(A) = \text{rank}(A') = n \), the \( \dim(\mathcal{R}(A)) = n \). Note now that \( A \) has \( n \) column vectors and for them to span a space of dimension \( n \), all of these column vectors have to be independent.
- (c) \( \implies \) (d): If the columns of \( A \) are independent, since each column vector is of length \( m \), there cannot be more than \( m \) of them (since more than \( m \) vectors of length \( m \) necessarily need to be dependent). Thus \( n \leq m \). Since \( n \) independent vectors span a space of dimension \( n \), we know that \( \dim(\mathcal{R}(A)) = n \implies \text{rank}(A) = n = \min(m, n) \).
- (d) \( \implies \) (a): By the rank–nullity theorem, \( \text{rank}(A) + \dim(\mathcal{N}(A)) = n \). Since \( \text{rank}(A) = n \), we have \( \dim(\mathcal{N}(A)) = 0 \), which implies that \( \mathcal{N}(A) = \{0\} \).

3. **Rank of \( AA' \).** Let \( A \in F^{m \times n} \).

- (a) Suppose that \( F = \mathbb{R} \). Prove that \( \text{rank}(AA') = \text{rank}(A) \) or provide a counterexample.
- (b) Suppose that \( F = \mathbb{F}_2 \). Repeat part (a).
- (c) Suppose that \( F = \mathbb{C} \). Repeat part (a).
- (d) Suppose that \( F = \mathbb{C} \). Prove that \( \text{rank}(AA^*) = \text{rank}(A) \) or provide a counterexample.

**Solution:**

- (a) If \( AA'x = 0 \), then \( x'AA'x = (A'x)'(A'x) = \|A'x\|^2 = 0 \), which implies that \( A'x = 0 \).
  Thus, for every \( x \in \mathcal{N}(AA') \), \( x \in \mathcal{N}(A') \), or equivalently, \( \mathcal{N}(AA') \subseteq \mathcal{N}(A') \). Conversely,
if \( A'x = 0 \), then \( AA'x = 0 \), which implies that \( \mathcal{N}(A') \subseteq \mathcal{N}(AA') \). Hence, \( \mathcal{N}(AA') = \mathcal{N}(A') \) and by the rank-nullity theorem,

\[
\text{rank}(A) = \text{rank}(A') = m - \dim(\mathcal{N}(A')) = m - \dim(\mathcal{N}(AA')) = \text{rank}(AA').
\]

(b) Consider

\[
A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}.
\]

In \( \mathbb{F}_2 \), \( AA' = 0 \). Thus, \( \text{rank}(A) = 1 \) but \( \text{rank}(AA') = 0 \).

(c) Consider

\[
A = \begin{bmatrix} 1 & i \\ 0 & 0 \end{bmatrix}.
\]

Again, \( AA' = 0 \). Thus, \( \text{rank}(A) = 1 \) but \( \text{rank}(AA') = 0 \).

(d) We can show that \( \text{rank}(A) = \text{rank}(AA^*) \) using the same proof as part (a), with \( A' \) replaced by \( A^* \). Indeed, \( (A^*)^*(A^*)x = 0 \implies A^*x = 0 \). Note, however, that this proof does not work for parts (b) and (c) – since in \( \mathbb{F}_2 \) or \( \mathbb{C} \), \( (A'x)'(A'x) = 0 \iff A'x = 0 \).

4. Rank of a sum. Let \( A, B \in \mathbb{F}^{m \times n} \). Show that

\[
\text{rank}(A + B) \leq \text{rank}(A) + \text{rank}(B).
\]

**Solution:** Let \( r_A \) and \( r_B \) denote the rank of \( A \) and \( B \) respectively. Consider a basis \( (u_1, u_2, \ldots, u_{r_A}) \) that spans \( \mathcal{R}(A) \) and another basis \( (v_1, v_2, \ldots, v_{r_B}) \) that spans \( \mathcal{R}(B) \). We will show that the set of vectors \( (u_1, u_2, \ldots, u_{r_A}, v_1, v_2, \ldots, v_{r_B}) \) spans \( \mathcal{R}(A + B) \).

Consider the column space of \( A + B \). If the columns of \( A \) are denoted by \( (a_1, a_2, \ldots, a_n) \), and those of \( B \) are denoted by \( (b_1, b_2, \ldots, b_n) \), the columns of \( A + B \) are denoted by \( (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \). Thus, any linear combination of \( (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \) can be written as a linear combination of the \( 2n \) vectors \( (a_1, b_1, a_2, b_2, \ldots, a_n, b_n) \). Since \( (u_1, u_2, \ldots, u_{r_A}) \) is a basis for \( \mathcal{R}(A) \) and \( (v_1, v_2, \ldots, v_{r_B}) \) a basis for \( \mathcal{R}(B) \), \( \text{span}(a_1, b_1, a_2, b_2, \ldots, a_n, b_n) = \text{span}(u_1, u_2, \ldots, u_{r_A}, v_1, v_2, \ldots, v_{r_B}) \).

Since the vectors \( (u_1, u_2, \ldots, u_{r_A}, v_1, v_2, \ldots, v_{r_B}) \) span the column space of \( A + B \), it immediately follows that \( \text{rank}(A + B) = \dim(\mathcal{R}(A + B)) \leq r_A + r_B = \text{rank}(A) + \text{rank}(B) \).

5. Rank of a product. Let \( A \in \mathbb{R}^{6 \times 4} \) has rank 2 and \( B \in \mathbb{R}^{4 \times 5} \) has rank 3.

(a) Find the smallest possible value \( r_{\text{min}} \) of \( \text{rank}(AB) \). Find specific \( A \) and \( B \) such that \( \text{rank}(AB) = r_{\text{min}} \).

(b) Find the largest possible value \( r_{\text{max}} \) of \( \text{rank}(AB) \). Find specific \( A \) and \( B \) such that \( \text{rank}(AB) = r_{\text{max}} \).

**Solution:**
(a) We first prove that
\[
\text{nullity}(AB) \leq \text{nullity}(A) + \text{nullity}(B) \tag{1}
\]
for any pair of matrices \(A \in \mathbb{R}^{m \times n}\) and \(B \in \mathbb{R}^{n \times k}\). To show this, we decompose \(\mathcal{N}(AB)\) by \(\mathcal{N}(B)\) and its orthogonal complement \(\mathcal{N}(B)^ot = \mathcal{R}(B')\) as
\[
\mathcal{N}(AB) = \{ z \in \mathbb{R}^k : ABz = 0 \} \\
= \{ z \in \mathbb{R}^k : Bz = 0 \} + \{ z \in \mathcal{R}(B') : Bz \in \mathcal{N}(A) \} \\
= \mathcal{N}(B) + \mathcal{V}.
\]
Then,
\[
\text{nullity}(AB) = \dim(\mathcal{N}(AB)) \leq \dim(\mathcal{N}(B)) + \dim(\mathcal{V}) = \text{nullity}(B) + \dim(\mathcal{V}),
\]
and it suffices to show that \(\dim(\mathcal{V}) \leq \dim(\mathcal{N}(A)) = \text{nullity}(A)\). To upper bound \(\dim(\mathcal{V})\), suppose that \(z_1, \ldots, z_k\) form a basis for \(\mathcal{V}\). Then \(Bz_1, \ldots, Bz_k\) must be independent; otherwise,
\[
\alpha_1 Bz_1 + \cdots + \alpha_k Bz_k = B(\alpha_1 z_1 + \cdots + \alpha_k z_k) = 0
\]
implies that \(z = \alpha_1 z_1 + \cdots + \alpha_k z_k \neq 0\) and \(z \in \mathcal{N}(B)\), which is a contradiction to the assumption that \(z \in \mathcal{R}(B') = \mathcal{N}(B)^ot\). But at the same time, \(Bz_1, \ldots, Bz_k \in \mathcal{N}(A)\) and thus \(k \leq \dim(\mathcal{N}(A))\). Therefore, \(\dim(\mathcal{V}) \leq \dim(\mathcal{N}(A))\).

By the rank-nullity theorem, (1) implies
\[
n - \text{rank}(AB) \leq (k - \text{rank}(A)) + (n - \text{rank}(B)),
\]
or equivalently,
\[
\text{rank}(AB) \geq \text{rank}(A) + \text{rank}(B) - k,
\]
where \(k\) is the number of rows of \(B\). Thus, specializing to our problem, we have
\[
\text{rank}(AB) \geq 2 + 3 - 4 = 1.
\]
This lower bound is tight, as shown by
\[
A = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0
\end{bmatrix}
\]
of ranks 2 and 3, respectively, and
\[
AB = \begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix},
\]
which has rank 1.
(b) Recall that \( \text{rank}(AB) \leq \min(\text{rank}(A), \text{rank}(B)) = 2 \). This upper bound is tight, as shown by
\[
A = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\quad \text{and} \quad
B = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0
\end{bmatrix},
\]
and
\[
AB = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix},
\]
which has rank 2.

6. **Oddtown.** Recall Oddtown with \( n \) people forming clubs according to the following rules:

- Each club has an odd number of members.
- Each pair of clubs share an even number of members.

In class, we discuss that \( n \) singleton clubs, namely, \( \{1\}, \{2\}, \ldots, \{n\} \) are compliant. We now form more interesting clubs.

(a) For \( n = 4 \), form 4 clubs, each with more than one member.

(b) For \( n = 6 \), form 6 clubs, not all of them of equal sizes.

**Solution:** We give an \( n \times n \) matrix \( A \), the rows of which represent clubs and the columns of which represent the people. \( A_{ij} \) is 1 if person \( j \) is a member of club \( i \), and 0 otherwise.

(a)
\[
A = \begin{bmatrix}
1 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1
\end{bmatrix}
\]
is a valid \( 4 \times 4 \) matrix.

(b)
\[
A = \begin{bmatrix}
1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]
is a valid \( 6 \times 6 \) matrix.
7. Parity check codes. Let

\[ G = \begin{bmatrix} I \\ A \end{bmatrix} \in \mathbb{F}_2^{n \times k}, \]

where \( A \in \mathbb{F}_2^{(n-k) \times k} \) and \( n \geq k \). Suppose that a \( k \)-bit message \( x \in \mathbb{F}_2^k \) is encoded into an \( n \)-bit codeword \( y = Gx \in \mathbb{F}_2^n \). This is an example of an \((n,k)\) binary linear parity check code. In this context, \( G \) is referred to as a generator matrix of the code and its range \( \mathcal{R}(G) \) is referred to as the set of codewords or the codebook. The additional \( n-k \) bits, or parity bits, provide redundant information that can be used for correction (or detection) of errors that occur to the codewords.

(a) Find \( |\mathcal{R}(G)| \) and interpret this value in terms of the codewords of the \((n,k)\) code.

(b) Let \( H = [A \mid I] \in \mathbb{F}_2^{(n-k) \times n} \). Show that \( HG = 0 \).

(c) Show that \( N(H) = \mathcal{R}(G) \), namely, \( y \) is a codeword if and only if \( Hy = 0 \). For this reason, \( H \) is referred to as a parity check matrix of the code.

(d) Consider the code with generator matrix \( H' \) that encodes \((n-k)\)-bit messages into \( n \)-bit codewords. This \((n,n-k)\) code is said to be dual to the original \((n,k)\) code with generator matrix \( G \). Find a parity check matrix \( P \) of the dual code, that is, a matrix \( P \) that satisfies \( Py = 0 \) if and only if \( y \) is a codeword of the dual code.

(e) Consider the \((7,4)\) Hamming code, specified by the generator matrix

\[
G = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1
\end{bmatrix}.
\]

How many codewords are there? List all of them.

(f) Consider the dual code of the \((7,4)\) Hamming code in part (f). How many codewords are in the dual code? List all of them.

Solution:

(a) For a useful code, no two different \( k \)-bit messages should be encoded into the same \( n \)-bit message. Therefore, \( G \) is one-one, implying that \( \text{nullity}(G) = 0 \). By the rank-nullity theorem, this implies \( \text{dim}(\mathcal{R}(G)) = \text{rank}(G) = k - \text{nullity}(G) = k \). Let \( \{c_1, \ldots, c_k\} \) be a basis for \( \mathcal{R}(G) \). We then have

\[
|\mathcal{R}(G)| = |\{(\alpha_1 c_1 + \cdots + \alpha_k c_k) : \alpha_1, \ldots, \alpha_k \in \mathbb{F}_2\}| = 2^k,
\]

since each \( \alpha_i \) can be chosen in \( 2 \) ways (0 or 1), and by the property of a basis, no two different choices of \( \alpha^k \) gives the same vector in \( \mathcal{R}(G) \). \( \mathcal{R}(G) \) is simply the set of possible codewords of the code, and therefore, this result implies that an \((n,k)\) binary linear parity check code has exactly \( 2^k \) codewords.
(b) We have

\[
HG = \begin{bmatrix} A & I \end{bmatrix} \begin{bmatrix} I \\ A \end{bmatrix}
= AI + IA \text{ (multiplying the matrices by blocks)}
= A + A
= 0,
\]

since for every \(a \in \mathbb{F}_2\), \(a + a = 0\).

(c) Let \(y = [y_1 \ldots y_n]' \in \mathcal{N}(H)\). Then, we have

\[
Hy = 0
\]

\[
\implies A \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_k \\ y_1 \\ \vdots \\ y_n \end{bmatrix} + \begin{bmatrix} y_{k+1} \\ \vdots \\ y_n \end{bmatrix} = 0
\]

\[
\implies A \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_k \\ y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} y_{k+1} \\ \vdots \\ y_n \end{bmatrix}
\]

\[
\implies \begin{bmatrix} y_1 \\ \vdots \\ y_k \\ y_{k+1} \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} I \\ A \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_k \end{bmatrix}
\]

which shows that \(y \in \mathcal{R}(G)\). Conversely, let \(x \in \mathcal{R}(G)\). Then, \(x = Gu\) for some \(u \in \mathbb{F}_2^k\).
Therefore, we have \(Hx = HGu = 0\). Thus, \(\mathcal{N}(H) = \mathcal{R}(G)\).

(d) \(c\) is a codeword of the dual code if and only if \(c = H'y\) for some \(y \in \mathbb{F}_2^{n-k}\). We therefore conclude that \(c := [c_1 \ldots c_n]'\) is a codeword of the dual code if and only if
\[
\begin{bmatrix}
  c_1 \\
  \vdots \\
  c_n 
\end{bmatrix}
= \begin{bmatrix} A' \\ I \end{bmatrix} y \\
\iff \\
\begin{bmatrix}
  c_1 \\
  \vdots \\
  c_{n-k} \\
  c_{n-k+1} \\
  \vdots \\
  c_n 
\end{bmatrix}
= \begin{bmatrix} A' y \\ y \end{bmatrix} \\
\iff A'
\begin{bmatrix}
  c_{n-k+1} \\
  \vdots \\
  c_n 
\end{bmatrix}
= \begin{bmatrix} c_1 \\
  \vdots \\
  c_{n-k} 
\end{bmatrix} \\
\iff A'
\begin{bmatrix}
  c_{n-k+1} \\
  \vdots \\
  c_n 
\end{bmatrix} + \begin{bmatrix} c_1 \\
  \vdots \\
  c_{n-k} 
\end{bmatrix} = 0 \\
\iff \begin{bmatrix} I_{k \times n} & A' \end{bmatrix}
\begin{bmatrix}
  c_1 \\
  \vdots \\
  c_n 
\end{bmatrix} = 0 \\
\iff G' c = 0.
\]

Therefore, \( P := G' \) is a parity check matrix of the dual code.

(e) Number of codewords = \( 2^4 = 16 \). By taking all possible linear combinations of the columns of \( G \), the codewords can be enumerated as

\[
\begin{align*}
  [0000000]', & [0001011]', \\
  [0010110]', & [0011101]', \\
  [0100101]', & [0101110]', \\
  [0110011]', & [0111000]', \\
  [1000111]', & [1001100]', \\
  [1010011]', & [1011010]', \\
  [1100101]', & [1101001]', \\
  [1110100]', & [1111111]'.
\end{align*}
\]

(f) The dual code has \( 2^3 = 8 \) codewords. Writing the matrix \( G \) in part (f) as

\[
G = \begin{bmatrix} I \\ A \end{bmatrix}
\]
a generator matrix for the dual code is given by

\[
\begin{bmatrix}
A' \\
I
\end{bmatrix} = \begin{bmatrix}
1 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 0 \\
0 & 1 & 1 \\
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix}.
\]

The codewords are

\[
[0000000]' , [1101001]', [1011010]' , [0110011]', [1110100]' , [0011101]', [0101110]' , [1000111]' .
\]