Problem 1

(a) Two users

Users 1 and 2 have the following system of linear equation with the following solution space:

\[
\begin{align*}
P(\alpha_1) &= P(1) = a_2 + a_1 + s = 0, \\
P(\alpha_2) &= P(\beta) = a_2 \beta^2 + a_1 \beta + s = 0,
\end{align*}
\]

\[
\Rightarrow \begin{cases} 
  a_1 = s \beta, \\
  a_2 = s \beta^2.
\end{cases}
\]

Considering all possible values for \(s\), we have the following four solutions:

<table>
<thead>
<tr>
<th>(s)</th>
<th>(a_1)</th>
<th>(a_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>(\beta)</td>
<td>(\beta^2)</td>
</tr>
<tr>
<td>(\beta)</td>
<td>(\beta^2)</td>
<td>1</td>
</tr>
<tr>
<td>(\beta^2)</td>
<td>1</td>
<td>(\beta)</td>
</tr>
</tbody>
</table>

Since \(s\), \(a_1\) and \(a_2\) are all chosen uniformly randomly and independently, all of the four possible solutions have the same probability of occurring. Therefore all values of \(s\) are still equally probable.

(b) Three users

User 3 adds the following equation to the system from subproblem (a):

\[
P(\alpha_3) = P(\beta^2) = a_2 \beta^2 + a_1 \beta^2 + s = \beta^2.
\]

Routine checking of the solutions from subproblem (a) reveals that only the last one also satisfies this equation in addition to the first two. Therefore all three users can uniquely determine that \(s = \beta^2\).

Problem 2

(a) Code parameters

Obviously, from the size of \(H\), we have \(n = 4\). Since \(H\) is full rank (e.g. by first two columns), we have \(k = n - \text{rank}(H) = 4 - 2 = 2\).

No one column of \(H\) multiplied by a non-zero scalar gives a zero vector, so there’s no codeword of weight 1. Moreover, no non-trivial linear combination of two columns of \(H\) gives a zero vector, because any pair are clearly linearly independent, so there’s no codeword of weight 2. However, \((1, 3, 1, 0)\) is a codeword and has weight 3. Therefore \(d = 3\).
(b) Number of solutions

According to the coset coding protocol from the lecture, Alice chooses uniformly randomly \((x_1, x_2) \in \mathbb{F}_5^2\) and \((x_3, x_4)\) will be uniquely determined by \((s_1, s_2)\) through a system of linear equations. Therefore there are \(|\mathbb{F}_5|^2 = 5^2 = 25\) solutions to choose from.

(c) Two intercepted values

Knowing that \(x_2 = 3\) and \(x_4 = 2\), the original system of linear equations defined by \(Hx^T = (s_1, s_2)^T\) simplifies as follows:

\[
\begin{align*}
x_1 + x_2 + x_3 + x_4 &= s_1, \\
x_1 + 2x_2 + 3x_3 + 4x_4 &= s_2,
\end{align*}
\]

\[
\begin{align*}
x_1 + x_3 &= s_1, \\
x_1 + 3x_3 &= s_2 + 1.
\end{align*}
\]

Since the simplified system of linear equations is full rank, for every choice of \((s_1, s_2)\) it has a unique solution \((x_1, x_3)\). Since it was shown in the lecture that every \((x_1, x_2, x_3, x_4)\) is equally probable without knowing the secret, so is every \((x_1, x_3)\) equally probable and therefore by bijection every \((s_1, s_2)\) is still equally probable.

(d) Three intercepted values

Additionally knowing that \(x_1 = 1\), the system from subproblem (c) simplifies even further:

\[
\begin{align*}
x_1 + x_3 &= s_1, \\
x_1 + 3x_3 &= s_2 + 1,
\end{align*}
\]

\[
\begin{align*}
1 + x_3 &= s_1, \\
3x_3 &= s_2.
\end{align*}
\]

Considering all possible values for \(x_3\), we have the following four solutions:

<table>
<thead>
<tr>
<th>(x_3)</th>
<th>(s_1)</th>
<th>(s_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Now Eve has some information about \((s_1, s_2)\) because only these five combinations are possible out of all 25, but not enough to determine the secret uniquely.

(e) Three intercepted values and one secret value

Additionally knowing that \(s_2 = 3\), simply checking of the solutions from subproblem (d) reveals that only the second one also satisfies this equation. Therefore Eve can now also determine that \(s_1 = 2\).

Problem 3

(a)

Proof by induction on \(i\):
Base Let $i = 0$, then, by initial values from extended Euclid’s algorithm:

$$s_i(x)t_{i-1}(x) - s_{i-1}(x)t_i(x) = s_0(x)t_{-1}(x) - s_{-1}(x)t_0(x) = 0 \cdot 0 - 1 \cdot 1 = -1 = (-1)^{i+1}.$$ 

Step Let $i = 1, \ldots, \tau$. The induction hypothesis for $i - 1$ is $s_{i-1}(x)t_{i-2}(x) - s_{i-2}(x)t_{i-1}(x) = (-1)^{i-1}$. Then, by loop equalities from extended Euclid’s algorithm:

$$s_i(x)t_{i-1}(x) - s_{i-1}(x)t_i(x) = (s_{i-2}(x) - q_i(x)s_{i-1}(x))t_{i-1}(x) - s_{i-1}(x)(t_{i-2}(x) - q_i(x)t_{i-1}(x)) =$$

$$= s_{i-2}(x)t_{i-1}(x) - q_i(x)s_{i-1}(x)t_{i-1}(x) - s_{i-1}(x)t_{i-2}(x) + q_i(x)s_{i-1}(x)t_{i-1}(x) =$$

$$= s_{i-2}(x)t_{i-1}(x) - s_{i-1}(x)t_{i-2}(x) = -(s_{i-1}(x)t_{i-2}(x) - s_{i-2}(x)t_{i-1}(x)) =$$

$$= -(-1)^i = (-1)^{i+1}.$$

(b) Proof by strong induction on $i$:

Bases Let $i = -1$, then, by initial values from extended Euclid’s algorithm:

$$s_i(x)a(x) + t_i(x)b(x) = s_{-1}(x)a(x) + t_{-1}(x)b(x) = 1 \cdot a(x) + 0 \cdot b(x) = a(x) = r_{-1}(x) = r_i(x).$$

Let $i = 0$, then, by initial values from extended Euclid’s algorithm:

$$s_i(x)a(x) + t_i(x)b(x) = s_0(x)a(x) + t_0(x)b(x) = 0 \cdot a(x) + 1 \cdot b(x) = b(x) = r_0(x) = r_i(x).$$

Step Let $i = 1, \ldots, \tau+1$. The induction hypothesis for $i-2$ is $s_{i-2}(x)a(x) + t_{i-2}(x)b(x) = r_{i-2}(x)$ and the induction hypothesis for $i - 1$ is $s_{i-1}(x)a(x) + t_{i-1}(x)b(x) = r_{i-1}(x)$. Then, by loop equalities from extended Euclid’s algorithm:

$$s_i(x)a(x) + t_i(x)b(x) =$$

$$= (s_{i-2}(x) - q_i(x)s_{i-1}(x))a(x) + (t_{i-2}(x) - q_i(x)t_{i-1}(x))b(x) =$$

$$= s_{i-2}(x)a(x) - q_i(x)s_{i-1}(x)a(x) + t_{i-2}(x)b(x) - q_i(x)t_{i-1}(x)b(x) =$$

$$= s_{i-2}(x)a(x) + t_{i-2}(x)b(x) - q_i(x)(s_{i-1}(x)a(x) + t_{i-1}(x)b(x)) =$$

$$= r_{i-2}(x) - q_i(x)r_{i-1}(x) = r_i(x).$$

(c) Proof by induction on $i$:

Base Let $i = 0$, then, by initial values from extended Euclid’s algorithm:

$$\deg(t_i(x)) + \deg(r_{i-1}(x)) = \deg(t_0(x)) + \deg(r_{-1}(x)) = \deg(1) + \deg(a(x)) = 0 + \deg(a(x)) = \deg(a(x)).$$
Step

Let \( i = 1, \ldots, \tau + 1 \). The induction hypothesis for \( i - 1 \) is \( \deg(t_{i-1}(x)) + \deg(r_{i-2}(x)) = \deg(a(x)) \).

From subproblem (b) for \( i - 1 \) and \( i \), we have:

\[
\begin{aligned}
  &\begin{cases}
    s_{i-1}(x)a(x) + t_{i-1}(x)b(x) = r_{i-1}(x), \\
    s_i(x)a(x) + t_i(x)b(x) = r_i(x).
  \end{cases}
\end{aligned}
\]

Multiplying the first equation by \( t_i(x) \) and the second equation by \( t_{i-1}(x) \) gives:

\[
\begin{aligned}
  &\begin{cases}
    s_{i-1}(x)t_i(x)a(x) + t_{i-1}(x)t_i(x)b(x) = t_i(x)r_{i-1}(x), \\
    s_i(x)t_{i-1}(x)a(x) + t_i(x)t_{i-1}(x)b(x) = t_{i-1}(x)r_i(x).
  \end{cases}
\end{aligned}
\]

Subtracting the first equation from the second yields the following, using subproblem (a):

\[
\begin{aligned}
  &\begin{cases}
    (s_i(x)t_{i-1}(x) - s_{i-1}(x)t_i(x))a(x) = t_{i-1}(x)r_i(x) - t_i(x)r_{i-1}(x) \\
    (-1)^{i+1}a(x) = t_{i-1}(x)r_i(x) - t_i(x)r_{i-1}(x) \\
    t_i(x)r_{i-1}(x) = t_{i-1}(x)r_i(x) + (-1)^ia(x).
  \end{cases}
\end{aligned}
\]

The remainders of the polynomial division satisfy \( \deg(r_i(x)) < \deg(r_{i-1}(x)) < \deg(r_{i-2}(x)) \), thus:

\[ \deg(t_{i-1}(x)r_i(x)) = \deg(t_{i-1}(x)) + \deg(r_i(x)) < \deg(t_{i-1}(x)) + \deg(r_{i-2}(x)) = \deg(a(x)), \]

where the last equality is the induction hypothesis.

Therefore:

\[ \deg(t_i(x)) + \deg(r_{i-1}(x)) = \deg(t_i(x)r_{i-1}(x)) \implies \deg(t_{i-1}(x)r_i(x) + (-1)^ia(x)) = \deg(a(x)), \]

where the last equality holds because obviously \( \deg((-1)^ia(x)) = \deg(a(x)) \) and \( \implies \) implies \( \deg(t_{i-1}(x)r_i(x)) < \deg(a(x)) \), so the sum has degree equal to its strictly greater term’s degree. ■

Problem 4

Let \( a(x) = \sum_{i=0}^m a_i x^i \) and \( b(x) = \sum_{i=0}^n b_i x^i \).

(a) Addition

Without loss of generality, assume \( m = n \), because zero coefficients can be added to make the sums have equal number of terms. Then, by definition, \( a(x) + b(x) = \sum_{i=0}^n (a_i + b_i) x^i \). Therefore:

\[
(a(x) + b(x))' = \sum_{i=1}^n i \cdot (a_i + b_i)x^{i-1} = \sum_{i=1}^n i \cdot a_i x^{i-1} + \sum_{i=1}^n i \cdot b_i x^{i-1} = a'(x) + b'(x).
\]

■

(b) Scalar multiplication

By definition, \( c \cdot a(x) = \sum_{i=0}^m c \cdot a_i x^i \). Therefore:

\[
(c \cdot a(x))' = \sum_{i=1}^m i \cdot (c \cdot a_i)x^{i-1} = c \cdot \sum_{i=1}^m i \cdot a_i x^{i-1} = c \cdot a'(x).
\]

■
(c) Multiplication

By definition:

\[ a(x) \cdot b(x) = \left( \sum_{i=0}^{m} a_i x^i \right) \cdot \left( \sum_{i=0}^{n} b_i x^i \right) = \sum_{i=0}^{m+n} \left( \sum_{j=0}^{i} a_j b_{i-j} \right) x^i, \]

Hence, its derivative is:

\[ (a(x) \cdot b(x))' = \sum_{i=1}^{m+n} i \cdot \left( \sum_{j=0}^{i} a_j b_{i-j} \right) x^{i-1}. \] (3)

Analogously, by carefully matching indices and exponents, we get:

\[ a(x) \cdot b'(x) = \left( \sum_{i=1}^{m} i \cdot a_i x^{i-1} \right) \cdot \left( \sum_{i=0}^{n} b_i x^i \right) = \sum_{i=1}^{m+n} \left( \sum_{j=0}^{i} j \cdot a_j b_{i-j} \right) x^{i-1}, \] (4)

\[ a'(x) \cdot b(x) = \left( \sum_{i=1}^{m} i \cdot a_i x^{i-1} \right) \cdot \left( \sum_{i=0}^{n} b_i x^i \right) = \sum_{i=1}^{m+n} \left( \sum_{j=0}^{i} j \cdot a_j b_{i-j} \right) x^{i-1}. \] (5)

Therefore:

\[ a(x) \cdot b'(x) + a'(x) \cdot b(x) = \left[ \sum_{i=1}^{m+n} \left( \sum_{j=0}^{i} (i-j) \cdot a_j b_{i-j} \right) x^{i-1} \right] + \left[ \sum_{i=1}^{m+n} \left( \sum_{j=0}^{i} j \cdot a_j b_{i-j} \right) x^{i-1} \right] = \]

\[ = \sum_{i=1}^{m+n} \left[ \left( \sum_{j=0}^{i} (i-j) \cdot a_j b_{i-j} \right) + \left( \sum_{j=0}^{i} j \cdot a_j b_{i-j} \right) \right] x^{i-1} = \]

\[ = \sum_{i=1}^{m+n} \left( \sum_{j=0}^{i} (i-j) \cdot a_j b_{i-j} + j \cdot a_j b_{i-j} \right) x^{i-1} = \]

\[ = \sum_{i=1}^{m+n} \left( \sum_{j=0}^{i} i \cdot a_j b_{i-j} \right) x^{i-1} = \sum_{i=1}^{m+n} i \cdot \left( \sum_{j=0}^{i} a_j b_{i-j} \right) x^{i-1}. \]

\[ \square \]