1. Use the Berlekamp-Massey Algorithm to find the shortest (unique) LFSR that generates the sequence:

\[ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ . \]

2. Suppose that \( X_1 \) and \( X_2 \) are independent random variables defined on the set \{0, 1\}. Let \( \epsilon_i \) denote the bias of \( X_i \), \( \epsilon_i = \Pr[X_i = 0] - \frac{1}{2} \), for \( i = 1, 2 \). Prove that if the random variables \( X_1 \) and \( X_1 \oplus X_2 \) are independent, then \( \epsilon_2 = 0 \) or \( \epsilon_1 = \pm \frac{1}{2} \).

3. Consider the 4-bit to 4-bit S-box defined by the fourth row of the DES S-box \( S_4 \):

\[
\begin{array}{cccccccccccccccc}
7 & 13 & 14 & 3 & 0 & 6 & 9 & 10 & 1 & 2 & 8 & 5 & 11 & 12 & 4 & 15 \\
13 & 8 & 11 & 5 & 6 & 15 & 0 & 3 & 4 & 7 & 2 & 12 & 1 & 10 & 14 & 9 \\
10 & 6 & 9 & 0 & 12 & 11 & 7 & 13 & 15 & 1 & 3 & 14 & 5 & 2 & 8 & 4 \\
3 & 15 & 0 & 6 & 10 & 1 & 13 & 8 & 9 & 4 & 5 & 11 & 12 & 7 & 2 & 14 \\
\end{array}
\]

Denote by \( (x_1, x_2, x_3, x_4) \) and by \( (y_1, y_2, y_3, y_4) \) the input bits and output bits respectively. Find the output bit \( y_j \) for which the bias of \( x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus y_j \) is the largest.

4. Given three input bits \( (x_1, x_2, x_3) \) the output bits \( (y_1, y_2) \) an 3-to-2 S-box \( \pi_S \) are defined as follows:

\[
\begin{align*}
y_1 &= x_1 x_2 \oplus x_3 \\
y_2 &= x_1 x_3 \oplus x_2
\end{align*}
\]

Compute the linear approximation table of \( \pi_S \).

5. (Stinson 3.9 a),b)) Let \( \pi_S \) be an \( m \)-bit to \( n \)-bit S-box. Show that

a) \( N_L(0, 0) = 2^m \).

b) \( N_L(a, 0) = 2^{m-1} \), for all \( a \neq 0 \).

6. First, a mathematical expression of \( N_L(a, b) \) is derived. Consider the sum

\[
\sum_{x \in \{0, 1\}^m} (-1)^{a \cdot x \oplus b \cdot \pi_S(x)},
\]

computed over integers. It is easy to see that

\[
\sum_{x \in \{0, 1\}^m} (-1)^{a \cdot x \oplus b \cdot \pi_S(x)} = \# \{ x \in \{0, 1\}^m | a \cdot x \oplus b \cdot \pi_S(x) = 0 \} - \# \{ x \in \{0, 1\}^m | a \cdot x \oplus b \cdot \pi_S(x) = 1 \} = N_L(a, b) - (2^m - N_L(a, b)) = 2N_L(a, b) - 2^m.
\]
It follows that

\[ N_L(a, b) = 2^{m-1} + \frac{1}{2} \sum_{x \in \{0,1\}^m} (-1)^{a \cdot x \oplus b \cdot \pi_S(x)}. \]  

(1)

The results given in Problem 5 a) and b) can also be expressed as follows:

\[ \sum_{x \in \{0,1\}^m} (-1)^{a \cdot x} = \begin{cases} 2^m, & \text{if } a = 0 \\ 0, & \text{if } a \neq 0 \end{cases} \]  

(2)

(a) Problem (Stinson 3.9 c)): Let \( \pi_S \) be an \( m \)-bit to \( n \)-bit S-box. Show that

\[ \sum_{a=0}^{2^{m-1}} N_L(a, b) = 2^{2m-1} \pm 2^{m-1}, \]

for all \( n \)-bit mask values \( b \), where the sum is taken over all \( m \)-bit mask values \( a \) (enumerated from 0 to \( 2^m - 1 \)).

(b) Check the result in (a) for the linear approximation table computed in Problem 4.