1. **Bottom of Page 3:** Explain why the number of multiples of \( P \) with weight \( w \) and degree \( d \) is around \( \frac{d^{w-1}}{(w-1)!2^p} \).

2. **Page 4, Section 2.1, Time-memory trade-off approach, 1st paragraph:**
   - Write a pseudo-code for Golic’s algorithm.
   - Detail the time and memory complexity of this algorithm.

3. **Bottom of Page 4:** Explain why computing discrete logarithms may help to find low-weight polynomials.

4. **Page 5, Section 2.2:** The code with generator matrix \( G \) given by (1) is a cyclic code. Is any minimum-weight codeword a relevant solution for the original problem?

5. **Page 6, proof of Theorem 1:** Prove the following statement: “the symbols in the other weight \( w \) codewords will be permuted, but the weight of these codewords stays the same”.

6. **Page 6, Theorem 1:** Give the expression of Matrix \( \Gamma \).

7. **Algorithm 1, Step 3:** Step 3 describes a procedure for computing all codewords \( x \) having weight \( p \) on Positions 0 to \( (k - 1) \), and weight 0 on Positions \( k \) to \( (k + z - 1) \). Explain why this procedure is more efficient than computing the weights of all elements \( uG' \) for \( wt(u) = p \).

8. **Algorithm 1, Step 5:** This step is erroneous. Checking whether the weight of \( x \) is \( (w - 2p) \) is not the right test. To which word must this test be applied? What is the weight of \( x \) in this case?

9. **Page 8, Theorem 2:**
   - What is the probability that a codeword with weight \( 2p \) on the first \( k \) positions and weight 0 on the next \( (z + l) \) positions can be written as the sum of two codewords from the list \( H_1 \) computed in Step 3.
   - Deduce the practical significance for Algorithm 1 of the following term in the expression of the complexity:

\[
\binom{n}{w-p} \binom{n-k-z-l}{w-2p} \left( 1 - \left( 1 - 2^{-z} \right)^{2^p} \right)
\]

10. **Page 10, middle of the page:** Since \( P(x) \) divides \( K(x) \), we have that \( pM^T = 0 \). Give a proof of this statement (note that \( P \) is the so-called characteristic polynomial of the LFSR, i.e. the reciprocal of its feedback polynomial).

11. **Page 11, Section 6:** Explain why “finding low-weight multiples of \( P \) can often be used in a correlation attack.”

12. **Page 12, Line 5:** Justify why the expected degree of the desired weight-4 multiple of \( P \) is around \( \frac{2^d}{3^3} \).