Coding and cryptography

Below are mostly the final answers to the questions. Of course, far more complete solutions are necessary during the exam, but this may help you check your calculations and/or arguments.

31-3-2022

1. (a) It violates the Hamming bound.
   (b) It cannot exist as 7×3 check matrix for it must have distinct non-zero rows, and that leads to a codeword of weight 3.
2. (a) Argue on the seven rows of H that also appear in a 7×7 identity matrix.
   (b) $\frac{57}{64}$
   (c) 4
   (d) $2^{57} \cdot 65$
3. (a) the rows of H are 100, 010, 001, 110, 011, 111, and 101 in that order
   (b) 1110010
4. (a) $g(x) = x^6 + x^4 + 1$
   (b) 8
5. (a) $(x^2 + x + 1)(x^6 + x^4 + x^3 + x + 1)$
   (b) 64 and 729
6. (a) 4
   (b) $m_\alpha(x) = 1 + x + x^2 + x^3 + x^4$.
7. (a) no (too many errors if $s_1 = 0$ but $s_3 \neq 0$)
   (b) no (too many errors; the auxiliary polynomial has no roots)
8. (a) $n - 1 = 120 = 2^3 \cdot 15$. $3^{15} = (243)^3 \equiv 1^3 \equiv 1$ modulo 121 so we can stop here.
   (b) No conclusions can be drawn: 121 might be prime but it does not follow.

9-6-2022

1. (a) It violates the Hamming bound.
   (b) A 14×4 matrix with as rows 14 (out of 15) distinct non-zero elements in K^4, including 1000, 0100, 0010, 0001 and 1100, is a check matrix of such a code.
2. (a) Argue on the seven rows of H that also appear in a 7×7 identity matrix.
   (b) $\frac{70}{77}$
   (c) 3
   (d) $2^{70} \cdot 78$
3. (a) the rows of H are 100, 010, 001, 101, 111, 110, and 011 in that order
   (b) 1010011
4. (a) $g(x) = x^2 + 1$
   (b) 6
   (c) 2
5. (a) $(x + 1)(x^3 + x + 1)(x^4 + x^3 + 1)$
   (b) 8; 125

6. (a) 4
   (b) $m_\alpha(x) = 1 + x^3 + x^4$.
7. (a) yes (only one error, $w(x)$ decodes to $w(x) + x^{11}$)
   (b) yes (two errors, $w(x)$ decodes to $w(x) + x + x^7$)
8. (a) $n - 1 = 96 = 2^5 \cdot 3$. $2^3 = 8 \not\equiv 1$; $2^3 = 8 \not\equiv -1$; $2^6 = 8^2 = 64 \not\equiv -1$; $2^{12} = 64^2 = (-33)^2 = 1089 \equiv 22 \not\equiv -1$; $2^{24} = 22^2 = 484 \equiv 96 \equiv -1$; $2^{48} = (-1)^2 = 1 \not\equiv -1$; all modulo 96.
   (b) No conclusions can be drawn: 97 might be prime but it does not follow.

21-3-2023

1. (a) It violates the Hamming bound.
   (b) A 6×4 matrix with rows 1000, 0100, 0010, 0001, 1110 and 0111 is a check matrix of such a code.
2. (a) Argue on the nine rows of H that also appear in a 9×9 identity matrix.
   (b) $\frac{36}{45} = \frac{4}{5}$
   (c) 4
   (d) $2^{36} \cdot 46$
3. (a) the rows of H are 100, 010, 001, 101, 111, 110, and 011 in that order
   (b) 1010011
4. (a) $g(x) = x^5 + x^{10} + x^{20}$
   (b) $\frac{20}{35} = \frac{4}{7}$
5. (a) $(x + 1)^2(x^5 + x^3 + x^2 + x + 1)$
   (b) 2
6. (a) 4
   (b) $m_\alpha(x) = 1 + x + x^4$.
7. (a) yes (two errors, $w(x)$ decodes to $w(x) + x + x^7$)
   (b) yes (only one error, $w(x)$ decodes to $w(x) + x^{12}$)
8. (a) $n - 1 = 120 = 2^3 \cdot 15$. $5^{15} = 56 \not\equiv 1$; $5^{15} = 56 \not\equiv -1$; $5^{30} = 56^2 = 3136 \equiv 111 \not\equiv -1$; $5^{60} = 111^2 \equiv (-10)^2 = 100 \not\equiv -1$, all modulo 121.
   (b) 121 cannot be prime.