Durham University

# EXAMINATION PAPER

| Examination Session: | Year: | Exam Code: |
|---|---|---|
| May | 2017 | MATH3401-WE01 |

**Title:** Codes and Crytography III

| | | |
|---|---|---|
| Time Allowed: | 3 hours | |
| Additional Material provided: | None | |
| Materials Permitted: | None | |
| Calculators Permitted: | Yes | Models Permitted: Casio fx-83 GTPLUS or Casio fx-85 GTPLUS. |
| Visiting Students may use dictionaries: No | | |

| | |
|---|---|
| Instructions to Candidates: | Credit will be given for: the best **FOUR** answers from Section A and the best **THREE** answers from Section B. Questions in Section B carry **TWICE** as many marks as those in Section A. |

| | |
|---|---|
| **Revision:** | |

ED01/2017

## SECTION A

1. Let $C = \langle (0,5,1,2,1), (0,\mathrm{T},2,1,7), (1,0,3,0,1), (2,1,4,4,5) \rangle \subseteq \mathbb{F}_{11}^5$.
   (We write 10 as T, for convenience.)

   (a) Find a basis for $C$.

   (b) Find a basis for $C^\perp$.

   (c) Find $d(C)$ and $d(C^\perp)$, giving your reasons.

2. Let $C$ be the $[n,k,d]$ code $\{\mathbf{x} \in \mathbb{F}_2^5 \mid \mathbf{x}H^t = \mathbf{0}\}$, where $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ is a check-matrix for $C$. This code is transmitted over a symmetric binary channel with symbol-error probability $p = 0.1$.

   (a) Find parameters $n$, $k$, and $d$ for $C$. (No need to explain.)

   (b) Make a syndrome look-up table for $C$, and use it to decode these received words: $(1,1,1,1,0)$, $(1,0,1,0,1)$.

   (c) We now decide to decode a received word $\mathbf{y}$ only if $S(\mathbf{y}) = S(\mathbf{x})$ with $w(\mathbf{x}) \leq 1$. Explain why we might choose to do this, given this value of $d(C)$.

   (d) By this rule;

      (i) How many of the $2^5$ possible words will we decode?

      (ii) What is the probability that a received word will be correctly decoded?

3. Let $C_1 = \{\mathbf{x} \in \mathbb{F}_5^6 \mid \mathbf{x}H_1^t = \mathbf{0}\}$, where $H_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 & 4 \end{pmatrix}$, so that $C_1$ is a $\mathrm{Ham}_5(2)$ code .

   (a) A word in $C_1$ is sent, and received as $\mathbf{y} = (4,3,2,0,1,2)$. Decode this word to find $\mathbf{c}_1 \in C_1$.

   (b) Write down a generator-matrix $G_1$ for $C_1$, and then perform channel decoding on $\mathbf{c}_1$. (That is, find the original message vector in $\mathbb{F}_5^4$ which is encoded as $\mathbf{c}_1$.)

   (c) Find $\mu \in \mathbb{F}_5$ such that $C_2 = \{\mathbf{x} \in \mathbb{F}_5^6 \mid \mathbf{x}H_2^t = \mathbf{0}\}$, where $H_2 = \begin{pmatrix} 0 & 2 & 1 & 3 & 1 & 2 \\ 4 & 2 & 0 & 1 & 4 & \mu \end{pmatrix}$, is also a $\mathrm{Ham}_5(2)$ code. Explain how you find it; you may wish to consider sets $L_{\mathbf{v}} = \{\lambda\mathbf{v} \mid \lambda \in \mathbb{F}_5, \lambda \neq 0\}$.

   (d) We know that any two $\mathrm{Ham}_5(2)$ codes are equivalent; confirm this by showing that we can transform $H_1$ into $H_2$ by applying a suitable sequence of changes to the columns.

   (e) Let $\mathbf{x} = (x_1, \ldots, x_6)$ be any codeword of $C_1$. Use your answer to (d) to write down, in terms of the $x_i$, a codeword of $C_2$. Check this works, by finding the word in $C_2$ which corresponds to $\mathbf{c}_1 \in C_1$.

4. Use the following convention to convert alphabetic messages into numbers.

$$\sqcup \to 0, \quad A \to 1, \quad \ldots, Z \to 26. \tag{1}$$

   (a) Convert the plaintext "HOW MANY" into an array of numbers using the above convention.

   (b) Use part (a) to convert the plaintext "HOW MANY" into the ciphertext using the affine cipher

$$x \to 7x + 5 \bmod 27.$$

   (c) What is the decryption function?

5. (a) Using the convention (1), convert the message "HI BOB" into a number.

   (b) Suppose your RSA modulus is $n = 5 \times 13 = 65$ and your encryption exponent is $e = 35$.

      (i) Find the decryption modulus $d$.

      (ii) Alice uses the RSA encryption algorithm with the pair $(n, e) = (65, 35)$ to code a message and sends you the number $c = 13$. Use this information to first decrypt the message as a number, and then using the convention (1), convert this number into a plaintext message.

6. Let $E : y^2 = x^3 - 5x + 8$ be an algebraic curve defined over $\mathbb{Q}$.

   (a) Compute the discriminant of $E$ and show that this curve is elliptic.

   (b) Let $P = (1, 2)$ and $Q = \left(-\frac{7}{4}, -\frac{27}{8}\right)$ be two rational points on $E$. Compute the points $-P$, $Q \oplus (-P)$ and $[2]P$ using the addition law on $E$.

## SECTION B

7. Let $A$ be an alphabet, with $|A| = q$.

   (a) For a word $x \in A^n$, and $t \in \mathbb{Z}, 0 \leq t \leq n$, define the sphere $S(x,t) \subseteq A^n$, and show that $|S(x,t)| = 1 + n(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t$.

   (b) Let $C$ be a $q$-ary $(n, M, d)$ code, with $d > 2t$.
   Show that the spheres $S(c,t)$ for $c \in C$ are disjoint.

   (c) Define carefully what it means to say that a code is *perfect*.

   (d) The Golay code $\mathcal{G}_{11}$ is a ternary $[11, 6, 5]$-code. Show that $\mathcal{G}_{11}$ is perfect.

   (e) In a homework problem, we constructed a check matrix for such a $\mathcal{G}_{11}$ code:

$$H = [I_5 \mid A] = \begin{pmatrix} 1 & & & & & 1 & 1 & 1 & 2 & 2 & 0 \\ & 1 & & 0 & & 1 & 1 & 2 & 1 & 0 & 2 \\ & & 1 & & & 1 & 2 & 1 & 0 & 1 & 2 \\ & 0 & & 1 & & 1 & 2 & 0 & 1 & 2 & 1 \\ & & & & 1 & 1 & 0 & 2 & 2 & 1 & 1 \end{pmatrix}.$$

   Let $A$ have columns $\mathbf{a}_1, \ldots, \mathbf{a}_6$, and notice that for $2 \leq i \leq 6$, $\mathbf{a}_i$ contains just one zero. Given this, and that $d(\mathcal{G}_{11}) = 5$, explain why each of these columns must also contain two 1's and two 2's.

   (f) Write down a check-matrix $\hat{H}$ for the extended code $\hat{\mathcal{G}_{11}}$.
   What can we say about the parameters $[n', k', d']$ of $\hat{\mathcal{G}_{11}}$?

   (g) By the usual method, find a generator-matrix for $\hat{\mathcal{G}_{11}}$. What is $d(\hat{\mathcal{G}_{11}})$? (*Hint:* When row-reducing, the fact you explained in (e) may save you some work.)

8. To construct the 5-ary cyclic codes of block-length 4, we consider the ring of polynomials $R_4 = \mathbb{F}_5[x]/(x^4 - 1)$.

   (a) Show that $x^4 - 1$ factors as $(x-1)(x-2)(x-3)(x-4)$ in $\mathbb{F}_5$ .

   (b) For each dimension $1 \leq k \leq 4$, determine how many cyclic 5-ary $[4, k]$-codes there are.

   (c) Consider the six codes of dimension 2. For each one, write down:
   a generator-polynomial $g_i(x) \in R_4$,
   and a generator-matrix $G_i \in M_{k,4}(\mathbb{F}_5)$.

   (d) In general, a code can have several distinct generator-matrices. How do we know that these are in fact six distinct codes? Show that two of them are equivalent.

   (e) One of these codes has generator matrix $G = \begin{pmatrix} 2 & 3 & 1 & 0 \\ 0 & 2 & 3 & 1 \end{pmatrix}$.
   Let $G$'s rows be $\mathbf{c}_1$, $\mathbf{c}_2$, and use them to confirm that the other cyclic shifts $(1, 0, 2, 3)$ and $(3, 1, 0, 2)$ are also in the code, but that $(0, 1, 2, 3)$ is not.

   (f) Write down the corresponding check-polynomial $h_i(x)$, and a check-matrix $H_i$, for each code.

   (g) Show that three of these codes are duals of the other three; in other words, they form three pairs $C, C^{\perp}$.

9. (i) Suppose Alice and Bob share the same RSA modulus $n$ and suppose their encryption exponents $e_A$ and $e_B$ are relatively prime. i.e. Alice and Bob use the RSA encryption system using the pairs $(n, e_A)$ and $(n, e_B)$ respectively. Charles wants to send the message $x$ to both Alice and Bob simultaneously. Therefore, he encrypts $x$ to get the corresponding values $c_A$ and $c_B$, and sends them to Alice and Bob respectively. Show that if Eve manages to intercept both $c_A$ and $c_B$ and knows the pairs $(n, e_A)$ and $(n, e_B)$, then she can easily decrypt $x$.

   (ii) Explain the Diffie-Hellman key exchange algorithm between Alice and Bob, where they use a prime $p$ and a primitive root $g$ modulo $p$.

   (iii) (a) A shift cipher key is exchanged between Alice and Bob using the Diffie-Hellman key exchange protocol with $g = 5, p = 47$. The actual numbers exchanged in this process between Alice and Bob were $X = 38$ and $Y = 11$. Find the key $k$ using this information.

   (b) Using the key $k$ in the previous part, decipher the message

   ″J XNGSFZUJGD″.

10. (i) Let $E$ be an elliptic curve defined over $\mathbb{F}_p$ for some prime $p \geq 3$. State Hasse's theorem for $E$.

(ii) (a) Consider the elliptic curve defined over $\mathbb{F}_5$ by the equation

$$y^2 = x^3 + x + 1.$$

Determine the cardinality of the group $E(\mathbb{F}_5)$.

(b) Let $N$ be an integer with $N \equiv 1 \bmod 5$. Let $E$ be the elliptic curve defined over $\mathbb{Q}$ by the equation

$$y^2 = x^3 + N^2x + N^3.$$

Show that there is no $P \in E(\mathbb{Q})$ of order 13.

(iii) Let $E$ be an elliptic curve defined by the equation

$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Z}$. Let $p$ be an odd prime co-prime to $4a^3 + 27b^2$. Set $f(x) := x^3 + ax + b$.

(a) Show that the cardinality of the set $E(\mathbb{F}_p)$ is equal to

$$p + 1 + \sum_{n=0}^{p-1} \left( \frac{f(n)}{p} \right),$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol in the above sum.

(b) Using part (a) or otherwise, prove that

$$\left| \sum_{n=0}^{p-1} \left( \frac{f(n)}{p} \right) \right| \leq 2\sqrt{p}.$$