ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Information Sciences

June 24, 2016

12h15 – 15h15

Important Notes

- No document or electronic device is allowed.
- For multiple choice questions, there is exactly one correct choice. We assign a small amount of negative points to the wrong answers, in such a way that, in average, random choices give zero points. (Same as not answering.)
- For the True/False questions, the wrong answer gives exactly the negative of the number of points assigned to the correct answer. Again, a random choice gives zero points in average. (Same as not answering.)
- For multiple choice and True/False questions, mark your answer with a thick 'X' in the corresponding box. If you want to change your answer, color the complete box (of the wrong answer) and mark the new answer with a 'X'.
- A few questions are neither multiple choice nor of the True/False kind. You will receive full points if your answer is correct and properly justified. (We want to see that you did not guess, and want to give partial credit if applicable). The gray bar below those questions is used for grading purposes. Please do not write on it.
- Each page has a code on top of it (see the top of this page). Do not write on it.
- For technical reasons, pencils are not allowed.

The table below provides numerical values which might be useful for solving certain problems.

x	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
$\log_2(x)$	−3.3219	−2.3219	−1.7370	−1.3219	−1.0000	−0.7370	−0.5146	−0.3219	−0.1520

x	2	3	4	5	6	7	8	9	10
$\log_2(x)$	1.0000	1.5850	2.0000	2.3219	2.5850	2.8074	3.0000	3.1699	3.3219

The prime numbers smaller than 100 are:
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89$ et 97.

Except otherwise specified, all the numbers are in base 10.

Room:
Row: / Seat:

Student Name / Sciper no.:
Exam Solution

Consider the 4 binary codes below:

	Codes			
Source Symbol	$C1$	$C2$	$C3$	$C4$
a	000	10	11	0010
b	01	000	011	11
c	111	11	1010	0
d	1100	01	00	1010
e	10	100	100	1011
f	011	001	010	0110

Problem 1 [4 points]
Answer the following True/False questions [1 point each]:

☒ True ☐ False $C3$ is instantaneous

☐ True ☒ False $C2$ is instantaneous

☐ True ☒ False $C1$ is instantaneous

☐ True ☒ False $C4$ is instantaneous

Problem 2 [4 points]
Answer the following True/False questions [1 point each]:

☐ True ☒ False $C2$ is uniquely decodable

☒ True ☐ False $C1$ is uniquely decodable

☐ True ☒ False $C4$ is uniquely decodable

☒ True ☐ False $C3$ is uniquely decodable

Problem 3 [4 points]
Answer the following True/False questions [1 point each]:

☒ True ☐ False There exists an instantaneous code that has the same codeword lengths as $C3$

☒ True ☐ False There exists an instantaneous code that has the same codeword lengths as $C1$

☒ True ☐ False There exists an instantaneous code that has the same codeword lengths as $C4$

☐ True ☒ False There exists an instantaneous code that has the same codeword lengths as $C2$

A box contains 4 dice:

- 2 fair 4-sided dice A and B: $p(i) = \frac{1}{4}, \quad i = \{1, 2, 3, 4\}$
- 1 loaded 4-sided dice C: $p(2) = 1$
- 1 loaded 4-sided dice D: $p(3) = 1$

You pick one of the dice at random and throw it indefinitely. The sequence of throws can be modeled as the output of the source $\mathcal{S} = S_1, S_2, \ldots$

Problem 4 [4.5 points]
Answer the following True/False questions [3/4 points each]:

☐ True ☒ False $H(S_1, S_2|S_3) = H(S_2, S_3)$

☒ True ☐ False $H(S_3, S_4) < H(S_1) + H(S_2)$

☒ True ☐ False $H(S_1) = H(S_2)$

☒ True ☐ False $H(S_1, S_2) = H(S_3, S_4)$

☐ True ☒ False S_1 and S_2 are independent

☐ True ☒ False $H(S_2, S_3) = H(S_2) + H(S_3)$

Problem 5 [5.5 points]
Determine $p_{S_1,\ldots,S_n}(s_1, \ldots, s_n)$ for the source $\mathcal{S}$ defined above.

☐0 ☐0.5 ☐1 ☐1.5 ☐2 ☐2.5 ☐3 ☐3.5 ☐4 ☐4.5 ☐5 ☒5.5 *Reserved, do not write on this box*

$$p_{S_1,\ldots,S_n}(s_1, \ldots, s_n) = \frac{1}{4}\left[p(s_1, \ldots, s_n|A) + p(s_1, \ldots, s_n|B) + p(s_1, \ldots, s_n|C) + p(s_1, \ldots, s_n|D)\right]$$
$$= \begin{cases} \frac{1}{4} + \frac{1}{2}\frac{1}{4^n}, & s_1, \ldots, s_n = 2, \ldots, 2 \\ \frac{1}{4} + \frac{1}{2}\frac{1}{4^n}, & s_1, \ldots, s_n = 3, \ldots, 3 \\ \frac{1}{2}\frac{1}{4^n}, & \text{otherwise.} \end{cases}$$

Problem 6 [4.5 points]
For the source $\mathcal{S}$ defined above, let $H(\mathcal{S})$ be the entropy of a symbol and $H^*(\mathcal{S})$ be the entropy rate.
Answer the following True/False questions [3/4 point each]:

☒ True ☐ False $H^*(\mathcal{S}) < H(\mathcal{S})$

☒ True ☐ False $H^*(\mathcal{S}) < 2$ bits

☒ True ☐ False $H(\mathcal{S}) > \lim_{n\to\infty} \frac{H(S_1,\ldots,S_n)}{n}$

☐ True ☒ False The source $\mathcal{S}$ is not stationary

☐ True ☒ False $H^*(\mathcal{S}) = \infty$

☐ True ☒ False $H(\mathcal{S}) = 2$ bits

Problem 7 [4 points]
Consider a source (random variable) S that takes values in an alphabet of cardinality $8^n + 4$ for some integer $n \geq 1$, and probability distribution

$$P_S(k) = \begin{cases} \frac{1}{8}, & \text{for } k = 1, 2, 3, 4 \\ \frac{1}{2^{3n+1}}, & \text{otherwise.} \end{cases}$$

For S, we construct a binary Shannon-Fano code Γ_{SF} with an average codeword length $L(S, \Gamma_{SF})$ and a binary Huffman code Γ_H with an average codeword length $L(S, \Gamma_H)$. Let $H(S)$ be the entropy of S.
Answer the following True/False questions [1 point each]:

☒ True	□ False	$H(S) = \frac{3n}{2} + 2$ bits
□ True	☒ False	$L(S, \Gamma_H) > H(S)$
☒ True	□ False	$L(S, \Gamma_{SF}) = H(S)$
□ True	☒ False	$H(S) = 2n + 3$ bits

Problem 8 [4 points]

Alice wants to send an encrypted message to Bob, using trap-door one-way functions. The publicly available directory contains the functions f_A and f_B, which are the trap-door one-way functions of Alice and Bob, respectively. Suppose that t is the text and c the cryptogram. Check one:

☐ Alice sends $c = f_A^{-1}(t)$
☐ Alice sends $c = f_A(f_B(t))$
☐ Alice sends $c = f_A(t)$
☐ Alice sends $c = f_B^{-1}(t)$
☒ Alice sends $c = f_B(t)$

Problem 9 [4 points]

Answer the following True/False questions [1 point each]:

☒ True ☐ False If $(ab)^{-1}$ does not exist in $\mathbb{Z}/k\mathbb{Z}$, then it is not possible that both a^{-1} and b^{-1} exist.
☒ True ☐ False If a^{-1} and b^{-1} exist in $\mathbb{Z}/k\mathbb{Z}$, then $(ab)^{-1}$ exists and $(ab)^{-1} = a^{-1}b^{-1}$.
☒ True ☐ False If either a^{-1} or b^{-1} does not exist in $\mathbb{Z}/k\mathbb{Z}$, then $(ab)^{-1}$ does not exist.
☒ True ☐ False $(ab)^{-1} = a^{-1}b^{-1}$ is true in $\mathbb{Z}/k\mathbb{Z}$, provided that $(ab)^{-1}$ exists.

Problem 10 [4 points]

What is the multiplicative inverse of 27 in $\mathbb{Z}/97\mathbb{Z}$? Check one:

☐ 15
☐ 67
☐ 90
☐ 23
☐ 77
☒ 18
☐ 7
☐ 50
☐ There is more than one
☐ It does not exist
☐ 24

Problem 11 [5 points]

Using Fermat's theorem, find the multiplicative inverse of 9 in $\mathbb{Z}/23\mathbb{Z}$. Your answer should be an integer in $\{0, 1, \ldots, 22\}$. (A correct guess without development will receive half the points.)

☐0 ☐0.5 ☐1 ☐1.5 ☐2 ☐2.5 ☐3 ☐3.5 ☐4 ☐4.5 ☒5 *Reserved, do not write on this box*

Fermat's theorem implies that $9^{22} = 1$ (all results taken mod 23). By writing $9 \times 9^{21} = 1$, we see that 9^{21} is the multiplicative inverse of 9. Let us compute it by successively squaring:

$$\begin{aligned}
9^2 &= 12\\
9^4 &= 12^2 = 6\\
9^8 &= 6^2 = 13\\
9^{16} &= 13^2 = 8\\
9^{20} &= 9^{16} \times 9^4 = 2\\
9^{21} &= 9^{20} \times 9 = 18.
\end{aligned}$$

Problem 12 [4 points]

Consider an encryption scheme where the ciphertext C is computed from the plaintext T with the use of a key K as $C = T \cdot K \pmod{m}$, where m is an integer ≥ 2. Say which of the following is True/False.

The encryption scheme is perfectly secure if [1 point each]:

☒ True ☐ False T, K are randomly chosen in $\mathbb{Z}/m\mathbb{Z}^*$ and m is prime

☐ True ☒ False T, K are randomly chosen in $\mathbb{Z}/m\mathbb{Z}$ and m is prime

☒ True ☐ False T, K are randomly chosen in $\mathbb{Z}/m\mathbb{Z}^*$

☐ True ☒ False T, K are randomly chosen in $\mathbb{Z}/m\mathbb{Z}$

Problem 13 [5 points]

Let p be a prime number and m a positive integer. The number of integers in $\{1, 2, \ldots, p^m\}$ that are relatively prime with p^m is (check one):

□ $2p$
□ mp
□ p
□ p^m
□ $p^m - p$
☒ $p^{m-1}(p-1)$

Problem 14 [4 points]

Consider RSA with the following parameters: $p = 7$, $q = 5$, $m = pq$, $k = \text{lcm}(p-1, q-1)$. Which of the following could be chosen as encoding exponent e and decoding exponent d? (Check one):

□ $e = 12$, $d = 15$
☒ $e = 17$, $d = 5$
□ $e = 15$, $d = 11$
□ $e = 7$, $d = 23$
□ $e = 6$, $d = 19$

Problem 15 [4 points]

A history teacher gives an exam in a room with desks arranged in m rows and n columns. In placing the exam sheets, he starts on the main diagonal and, when he reaches an edge, he continues from the opposite edge, according to the "torus rule". Check one:

☒ Every desk ends up with an exam sheet if $m = 42$ and $n = 19$.
□ Every desk ends up with an exam sheet if $m = 42$ and $n = 21$.
□ Every desk ends up with an exam sheet if and only if m and n are not both even or both odd.
□ Every desk ends up with an exam sheet if and only if m and n are distinct prime numbers.
□ Every desk ends up with an exam sheet.

Problem 16 [4 points]

What is the dimension of the vector space defined by the solutions $v = (x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in \mathbb{F}_{11}^7$ of the following set of equations?

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 &= 0 \\ 2x_2 + 3x_3 + x_5 &= 0 \\ 2x_2 + 7x_3 + x_4 + 2x_5 + 2x_6 + 3x_7 &= 0 \\ 4x_3 + x_4 + x_5 + 2x_6 + 3x_7 &= 0 \end{aligned}$$

Check one:

☒ 4
□ 3
□ 11
□ 6
□ 7
□ 2

Problem 17 [3 points]

Let $\mathcal{C}$ be a code and $c, c' \in \mathcal{C}$. What is the contrapositive of the statement $c \neq c' \Rightarrow d(c, c') \geq d_{\min}(\mathcal{C})$? Check one:

□ $c = c' \Rightarrow d(c, c') < d_{\min}(\mathcal{C})$
□ $d(c, c') > d_{\min}(\mathcal{C}) \Rightarrow c = c'$
□ $c \neq c' \Rightarrow d(c, c') < d_{\min}(\mathcal{C})$
☒ $d(c, c') < d_{\min}(\mathcal{C}) \Rightarrow c = c'$

Problem 18 [3 points]

Consider the Reed-Solomon (n,k) code with $n-k=2t$. What is the maximum value l such that all errors of weight l can be corrected by the code? Check one:

□ $2t$

☒ t

□ $\lfloor (n-1)/2 \rfloor$

□ k

□ $n-k+1$

□ n

Problem 19 [3 points]

Let

$(a_1,a_2,a_3)=(1,2,4)$

$(y_1,y_2,y_3)=(1,1,1)$.

Which of the following polynomials $P(x)$ over $\mathbb{R}$ fulfills $P(a_i)=y_i$, $i=1,2,3$? Check one:

□ $\frac{(x-2)(x-4)}{3}$

□ $\frac{(x-1)(4-x)}{2}$

□ $\frac{(x-2)(x-4)}{4}$

☒ $\frac{(x-2)(x-4)}{3} - \frac{(x-1)(x-4)}{2} + \frac{(x-1)(x-2)}{6}$

□ $\frac{(x-2)(x-1)}{6}$

□ $\frac{(x-2)(x-4)}{2} - \frac{(x-1)(x-4)}{3} + \frac{(x-1)(x-2)}{4}$

Problem 20 [4.5 points]

Consider a finite field $\mathbb{F}_q$ of characteristic p. Answer the following True/False questions [3/4 point each]:

☒ True □ False If $q=4$, $x^p+y^p=x^p-y^p$ for all $x,y \in \mathbb{F}_q$

☒ True □ False $x^q=x$ for all $x \in \mathbb{F}_q$

☒ True □ False $(x+y)^p=x^p+y^p$ for all $x,y \in \mathbb{F}_q$

□ True ☒ False $px=1$ for all $x \in \mathbb{F}_q$

☒ True □ False $q=p^m$ where m is an integer.

□ True ☒ False $x^p=1$ for all $x \in \mathbb{F}_q$

Consider a binary code $\mathcal{C}$ which has the codewords of the form $c \in \mathcal{C} = (D_1, D_2, D_3, D_4, P_1, P_2, P_3)$ where D_1 through D_4 are data bits and P_1, P_2, P_3 are parity bits. The parity bits are defined as below:

$$\begin{aligned} P_1 &= D_1 + D_2 + D_4 \pmod 2 \\ P_2 &= D_1 + D_3 + D_4 \pmod 2 \\ P_3 &= D_2 + D_3 + D_4 \pmod 2 \end{aligned}$$

Problem 21 [4 points]
Answer the following True/False questions about the code $\mathcal{C}$ [1 point each]:

☒ True □ False $\mathcal{C}$ is a linear code

☒ True □ False $d_{min} = 3$

□ True ☒ False The dimensionality of the code is 3

□ True ☒ False $d_{min} = 2$

Problem 22 [3 points]
Consider the following matrices:

$$G_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}, G_2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}, G_3 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Each row of the above matrices is a valid codeword of $\mathcal{C}$. Answer the following True/False questions [1 point each]:

□ True ☒ False G_2 is a generator matrix for $\mathcal{C}$.

☒ True □ False G_1 is a generator matrix for $\mathcal{C}$.

□ True ☒ False G_3 is a generator matrix for $\mathcal{C}$.

Problem 23 [3 points]
Define a linear code by the following parity-check matrix H.

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Assuming a 1-bit error, find the error position if the received word $y = (1, 0, 0, 1, 0, 0, 1, 0)$. The error is at position (check one):

□ 4
□ 1
☒ 8
□ 2
□ 5
□ 7

Consider an RS code $\mathcal{C}$ over $\mathbb{F}_5$ with the following parameters: $k = 3$, $n = 5$, $a_i = i$, $i = 1, 2, 3, 4, 5$. For $i = 1, \ldots, k$ let $Q_i(x)$ be the degree $k-1$ polynomial which is 1 at $x = a_i$ and is 0 at $x = a_j$, $j \neq i$, $1 \leq j \leq k$.

Problem 24 [3 points]
Is $\vec{x} = (Q_1(a_1), Q_1(a_2), \ldots, Q_1(a_n))$ an element of $\mathcal{C}$? Justify your answer.

□0 □0.5 □1 □1.5 □2 □2.5 ☒3 *Reserved, do not write on this box*

According to the definition given in class, if $p(x)$ is a polynomial of degree $k-1$ or less over $\mathbb{F}_5$, then $(p(a_1), \ldots, p(a_n))$ is a codeword of $\mathcal{C}$. The degree of the polynomial is important. All the $Q_i(x)$ have degree $k-1$ or less. So, the answer is YES.

Problem 25 [2 points]
Now, consider the $k \times n$ matrix

$$A = \begin{bmatrix} Q_1(a_1) & Q_1(a_2) & \ldots & Q_1(a_n) \\ Q_2(a_1) & Q_2(a_2) & \ldots & Q_2(a_n) \\ \vdots & & & \\ Q_k(a_1) & Q_k(a_2) & \ldots & Q_k(a_n) \end{bmatrix}$$

Evaluate the submatrix that consists of the first k columns of A.

□0 □0.5 □1 □1.5 ☒2 *Reserved, do not write on this box*

It is the $(k \times k)$ identity matrix.

Problem 26 [3 points]
Is A a generator matrix for the code $\mathcal{C}$? Justify your answer.

□0 □0.5 □1 □1.5 □2 □2.5 ☒3 *Reserved, do not write on this box*

Yes. As a justification, we need to argue that the k rows of A form a basis of the code. Indeed:

(i) each row is a codeword (see Problem 24);

(ii) the rows are linearly independent (see Problem 25);

(iii) the number of rows equals the dimensionality k of the code.

Use this page if you need more space for the handwritten questions.