



ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Advanced Information, Computation, Communication II

June 27, 2017

08h15 – 11h15

Important Notes

- No document or electronic device is allowed.
 - For each question, there is exactly one correct answer. We assign negative points to the wrong answers, in such a way that, in average, random choices give zero points. (Same as not answering.)
 - Mark your answer with a thick 'X' in the corresponding box. If you want to change your answer, color the box completely and mark the new answer with a 'X'.
 - 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 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:
Seat:

Student Name / Sciper no.:

Exam Solution

**Problem 1** [8 points]

Consider the 4 binary codes below:

Source Symbol	Codes			
	$C1$	$C2$	$C3$	$C4$
a	11	01	1100	01
b	10	001	00	111
c	101	000	0100	011
d	100	10	1	00
e	01	110	0101	010
f	001	111	1101	0110

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

Warning: the order of the questions is randomized, hence not necessarily according to the above table.

- 1/1 ☐ True ☒ False $C3$ is uniquely decodable
- 1/1 ☒ True ☐ False $C2$ is uniquely decodable
- 1/1 ☐ True ☒ False $C1$ is uniquely decodable
- 1/1 ☒ True ☐ False $C4$ is uniquely decodable
- 1/1 ☒ True ☐ False There exists an instantaneous code that has the same codeword lengths as $C2$
- 1/1 ☐ True ☒ False There exists an instantaneous code that has the same codeword lengths as $C1$
- 1/1 ☒ True ☐ False There exists an instantaneous code that has the same codeword lengths as $C4$
- 1/1 ☒ True ☐ False There exists an instantaneous code that has the same codeword lengths as $C3$

Problem 2 [7 points]Consider a code \mathcal{C} used for source coding. Answer the following True/False questions [1 point each]:

- 1/1 ☐ True ☒ False \mathcal{C} is with prefix $\Rightarrow \mathcal{C}$ is not uniquely decodable
- 1/1 ☐ True ☒ False \mathcal{C} satisfies Kraft's inequality $\Rightarrow \mathcal{C}$ is uniquely decodable
- 1/1 ☒ True ☐ False We can always replace a uniquely decodable code by a prefix-free code that has the same codeword lengths
- 1/1 ☒ True ☐ False \mathcal{C} does not satisfy Kraft's inequality $\Rightarrow \mathcal{C}$ is with prefix
- 1/1 ☐ True ☒ False \mathcal{C} is with prefix $\Rightarrow \mathcal{C}$ does not satisfy Kraft's inequality
- 1/1 ☐ True ☒ False \mathcal{C} satisfies Kraft's inequality $\Rightarrow \mathcal{C}$ is prefix-free
- 1/1 ☒ True ☐ False The codeword lengths do not satisfy Kraft's inequality $\Rightarrow \mathcal{C}$ is not uniquely decodable


Problem 3 [9 points]

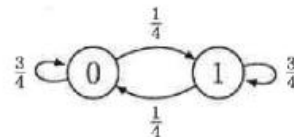
Consider a biased coin with $p(H) = \frac{1}{3}$ and $p(T) = 1 - p(H) = \frac{2}{3}$. We flip the coin indefinitely. The sequence of flips can be modeled as the output of the source $\mathcal{S} = S_1, S_2, \dots$

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

- | | | | |
|-----|--|---|---|
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $H(S_1, S_2, \dots, S_n) = n \cdot H(S_n S_1, S_2, \dots, S_{n-1})$ |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $H(S_1) = H(S_2)$ |
| 1/1 | <input type="checkbox"/> True | <input checked="" type="checkbox"/> False | $H(S_1, S_2, S_3) = (2 \log_2 3 - 3) \text{ bits}$ |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $H(S_2, S_3) = 2 \cdot H(S_2 S_3)$ |
| 1/1 | <input type="checkbox"/> True | <input checked="" type="checkbox"/> False | $H(S_2, S_3 S_1) = H(S_1, S_2, S_3) - H(S_2, S_3)$ |
| 1/1 | <input type="checkbox"/> True | <input checked="" type="checkbox"/> False | $H(S_1 S_2) = H(S_1, S_2)$ |
| 1/1 | <input type="checkbox"/> True | <input checked="" type="checkbox"/> False | $H(S_1, S_2) < H(S_1) + H(S_2)$ |
| 1/1 | <input type="checkbox"/> True | <input checked="" type="checkbox"/> False | $H(S_1 S_2) < H(S_1)$ |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $H(S_1, S_2, S_3) = (3 \log_2 3 - 2) \text{ bits}$ |

Problem 4 [6 points]

Let S_1, S_2, S_3, \dots be an infinite sequence produced by source \mathcal{S} . All S_i take values in $\{0, 1\}$ and the probability $p_{S_{n+1}|S_n}(\cdot|\cdot)$ is schematically represented in the following graph:



For instance, the directed edge from 0 to 1 means that $p_{S_{n+1}|S_n}(1|0) = \frac{1}{4}$.

We assume that $p_{S_1}(0) = \frac{1}{4}$ and $p_{S_1}(1) = \frac{3}{4}$.

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 [1 point each]:

- | | | | |
|-----|--|---|---|
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $p_{S_n}(0) = \frac{2^n - 1}{2^{n+1}}$ is correct and $p_{S_n}(0) = \frac{2^n - 1}{2^{n+2}}$ is incorrect |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $H(\mathcal{S}) = 1 \text{ bit}$ |
| 1/1 | <input type="checkbox"/> True | <input checked="" type="checkbox"/> False | $H^*(\mathcal{S}) = (2 - \log_2 3) \text{ bits}$ |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $H(S_n S_1, S_2, \dots, S_{n-1}) = H(S_{n-1} S_1, S_2, \dots, S_{n-2})$ |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | The source \mathcal{S} is regular |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $H(S_1, \dots, S_n) = (n - 1)H(S_n S_{n-1}) + H(S_1)$ |

**Problem 5** [7 points]

Consider a biased dice with $p(1) = p(2) = \frac{1}{4}$ and $p(3) = p(4) = p(5) = p(6) = \frac{1}{8}$. We throw this dice n times, for some fixed integer $n \geq 2$. We denote by $S = (S_1, S_2, \dots, S_n)$ the source formed by the outcomes of the n throws. 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]:

- | | | | |
|-----|--|---|---|
| 1/1 | <input type="checkbox"/> True | <input checked="" type="checkbox"/> False | $H(S_n S_1, S_2, \dots, S_{n-1}) = n \cdot L(S, \Gamma_{SF})$ |
| 1/1 | <input type="checkbox"/> True | <input checked="" type="checkbox"/> False | $L(S, \Gamma_{SF}) < L(S, \Gamma_H)$ |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $H(S_1, S_2, \dots, S_n) = n \cdot H(S_1)$ |
| 1/1 | <input type="checkbox"/> True | <input checked="" type="checkbox"/> False | $H(S) = 2n \log_2 3$ bits |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $H(S_1) = \frac{L(S, \Gamma_{SF})}{n}$ |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $H(S) = \frac{5n}{2}$ bits |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $L(S, \Gamma_H) = H(S)$ |

Problem 6 [2 points]

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

- | | | | |
|-----|--|--------------------------------|--|
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $(\mathbb{Z}/31\mathbb{Z} \setminus \{[0]_{31}\}, \cdot)$ is a commutative group |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $(\mathbb{Z}/4\mathbb{Z} \setminus \{[1]_4, [3]_4\}, +)$ is a commutative group |

Problem 7 [4 points]

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

- | | | | |
|-----|--|---|--|
| 1/1 | <input type="checkbox"/> True | <input checked="" type="checkbox"/> False | $(\mathbb{Z}/8\mathbb{Z}^*, \cdot)$ and $(\mathbb{Z}/4\mathbb{Z}, +)$ are isomorphic |
| 1/1 | <input type="checkbox"/> True | <input checked="" type="checkbox"/> False | $(\mathbb{Z}/5\mathbb{Z}^*, \cdot)$ and $(\mathbb{Z}/8\mathbb{Z}^*, \cdot)$ are isomorphic |
| 1/1 | <input checked="" type="checkbox"/> True | <input type="checkbox"/> False | $((\mathbb{Z}/2\mathbb{Z})^2, +)$ and $(\mathbb{Z}/8\mathbb{Z}^*, \cdot)$ are isomorphic |
| 1/1 | <input type="checkbox"/> True | <input checked="" type="checkbox"/> False | $(\mathbb{Z}/4\mathbb{Z}, +)$ and $((\mathbb{Z}/2\mathbb{Z})^2, +)$ are isomorphic |

Problem 8 [3 points]

Alice and Bob have public trapdoor one-way functions, respectively f_A and f_B . Alice wants to send a signed message to Bob. The original message is m . She sends (check one):

- | | |
|-----|---|
| 3/3 | <input checked="" type="checkbox"/> $f_A^{-1}(m)$ |
| | <input type="checkbox"/> $f_B(m)$ |
| | <input type="checkbox"/> $f_B^{-1}(m)$ |
| | <input type="checkbox"/> $f_A(m)$ |

**Problem 9** [4 points]

Consider the RSA public key $(m, e) = (55, 3)$. What is the decryption of the RSA ciphertext $c = 2$? Check one:

- ☐ 2
☒ 18
☐ 7
☐ 3
☐ 8

4/4

Problem 10 [4 points]

Let m and n be coprime positive integers. How many elements are there in $\mathbb{Z}/mn\mathbb{Z}^*$? ($\phi(\cdot)$ represents Euler's totient function.) Check one:

- ☐ $mn - \phi(m)\phi(n)$
☐ $mn - \phi(m) - \phi(n) + \phi(mn)$
☐ $\phi(m) + \phi(n)$
☒ $\phi(m)\phi(n)$
☐ $\phi(m + n)$

4/4

Problem 11 [4 points]

Let E be an encryption scheme, with message T and key K . $E_K(T)$ represents the encryption of T with the key K .

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

- 1/1 ☐ True ☒ False If K and T are uniformly distributed over their respective alphabets, then E provides perfect secrecy
- 1/1 ☐ True ☒ False If K , T and $E_K(T)$ all have same length, then E provides perfect secrecy
- 1/1 ☐ True ☒ False If E provides perfect secrecy, then $H(T) = H(K)$
- 1/1 ☐ True ☒ False If $H(E_K(T)) = H(K)$, then E provides perfect secrecy

**Problem 12** [4 points]

Let H be the parity-check matrix of a linear code of parameters (n, k, d_{\min}) .

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

- 1/1 ☒ True ☐ False All collections of $n - k + 1$ columns of H are linearly dependent
- 1/1 ☒ True ☐ False If the code is not MDS, there exists a collection of $n - k$ columns of H that are linearly dependent
- 1/1 ☒ True ☐ False The rank of H is $n - k$
- 1/1 ☒ True ☐ False d_{\min} is the smallest number of linearly dependent columns of H

Problem 13 [5 points]

Suppose that the input to a binary channel is a codeword of the binary code described by the following parity-check matrix

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

Suppose that the channel output is $y = (1, 0, 0, 1, 0)$. You know that the channel introduces at most one error (at most one flipped position). Which is the correct answer? Check one:

- ☐ The error is in position 3
- 5/5 ☒ The error is in position 2
- ☐ The error is in position 5
- ☐ There is no error
- ☐ The error is in position 4
- ☐ The error is in position 1

Problem 14 [4 points]

Suppose that the input to a binary channel is a codeword of the binary code described by the following parity-check matrix

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

Suppose that the channel output is $y = (1, ?, ?, 1, 0)$. Which is the correct answer? Check one:

- 4/4 ☒ The transmitted codeword is $(1, 1, 0, 1, 0)$
- ☐ The transmitted codeword is $(1, 0, 1, 1, 0)$
- ☐ The transmitted codeword is $(1, 0, 0, 1, 0)$
- ☐ The transmitted codeword is $(1, 1, 1, 1, 0)$
- ☐ There is more than one way to fill in

**Problem 15** [3 points]

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

- 1/1 ☐ True ☒ False Every (n, k) block code, whether linear or not, has a generator matrix
- 1/1 ☒ True ☐ False A linear code that has minimum distance 5 can have at most one codeword of the form $(1, 0, 0, 0, c_5, c_6, c_7, c_8)$
- 1/1 ☐ True ☒ False Every $(8, 4)$ linear code has at least one codeword of the form $(1, 0, 0, 0, c_5, c_6, c_7, c_8)$

Problem 16 [4 points]Fix a finite field \mathbb{F} , let $p(x) = a + bx + cx^2 + dx^3$ be a polynomial over \mathbb{F} of degree 3, and suppose that a_1, a_2, a_3, a_4, a_5 are distinct field elements. Suppose you are given k points of the form $(a_i, y_i) \in \mathbb{F}^2$.

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

- 1/1 ☒ True ☐ False For $k = 5$ a polynomial of the form $p(x)$ such that $y_i = p(a_i)$, $i = 1, \dots, k$, may or may not exist. If it exists, it is unique.
- 1/1 ☒ True ☐ False For $k = 3$ a polynomial of the form $p(x)$ such that $y_i = p(a_i)$, $i = 1, \dots, k$, always exists but it is not necessarily unique.
- 1/1 ☐ True ☒ False For $k = 5$ a polynomial of the form $p(x)$ such that $y_i = p(a_i)$, $i = 1, \dots, k$, may or may not exist and may or may not be unique.
- 1/1 ☐ True ☒ False For $k = 3$ a polynomial of the form $p(x)$ such that $y_i = p(a_i)$, $i = 1, \dots, k$, always exists and is unique.

Problem 17 [2 points]

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

There exists a linear code over a finite field \mathbb{F} that has the following parameters:

- 1/1 ☐ True ☒ False $n = 100$, the code has 63 codewords, $d_{\min} = 6$
- 1/1 ☒ True ☐ False $n = 10^3$, $|\mathbb{F}| = 1024$, the code has 2^{50} codewords, $d_{\min} = 996$

Problem 18 [4 points]Consider a Reed-Solomon code over $\mathbb{F}_5 = (\mathbb{Z}/5\mathbb{Z}, +, \cdot)$ with parameters $k = 1$, $n = 4$, defined by $a_1 = 3$, $a_2 = 0$, $a_3 = 4$, $a_4 = 2$. Answer the following True/False questions [2 points each].

- 2/2 ☐ True ☒ False $(3, 0, 4, 2)$ is a valid codeword
- 2/2 ☒ True ☐ False $(1, 1, 1, 1)$ is a valid codeword

**Problem 19** [4 points]

Answer the following True/False questions [2 points each].

The following generator matrices G and \tilde{G} generate the same code over $\mathbb{F}_5 = (\mathbb{Z}/5\mathbb{Z}, +, \cdot)$:

2/2

☒ True ☐ False

$$G = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad \tilde{G} = \begin{bmatrix} 1 & 0 & 4 & 3 \\ 0 & 1 & 2 & 3 \end{bmatrix}$$

2/2

☐ True ☒ False

$$G = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad \tilde{G} = \begin{bmatrix} 1 & 0 & 4 & 3 \\ 0 & 1 & 3 & 2 \end{bmatrix}$$

Problem 20 [2 points]Which of the following is a parity-check matrix for the generator matrix $G = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 \end{bmatrix}$ of a code over $\mathbb{F}_5 = (\mathbb{Z}/5\mathbb{Z}, +, \cdot)$? Check one:

2/2

☒ $\begin{bmatrix} 1 & 3 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{bmatrix}$

☐ $\begin{bmatrix} 1 & 3 & 1 & 0 \\ 2 & 3 & 0 & 1 \end{bmatrix}$

Problem 21 [5 points]Consider a linear code \mathcal{C} of parameters (n, k) , constructed on \mathbb{F}_{11} . How many distinct generator matrices are there for this code? Check one:

5/5

☐ 11^{n-k}

☒ $\prod_{i=0}^{k-1} (11^k - 11^i)$

☐ 11^k

☐ $11^n - 11^k$

☐ $\sum_{i=0}^k \frac{n!}{i!(n-i)!}$

☐ $\frac{n!}{k!(n-k)!}$