Exam Solution
Total score: 76/76

+1/1/60+

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Final Exam

Advanced Information, Computation, Communication II

June 25, 2019

16h15 19h15

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 a person that chooses at random according to a uniform distribution over the possible choices gains 0 points in average. (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 an '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.
- All entropies are in bits.

Room:
Seat:

Student Name / Sciper no.:
Exam Solution

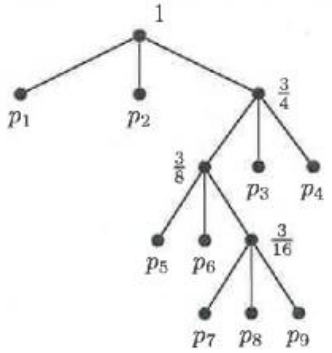
Problem 1 [5 points]
Let $\mathcal{S} = \{0, \frac{1}{2}\pi, \pi, \frac{3}{2}\pi, 2\pi, \frac{5}{2}\pi, 3\pi, \frac{7}{2}\pi\}$, and let X be a random variable which is uniformly distributed over $\mathcal{S}$. We further define random variables $Y = 2^X$ and $Z = \sin(X)$. Answer the following True/False questions [1 point each]:

1/1	☐ True	☒ False	$H(Z) = H(X)$
1/1	☐ True	☒ False	$H(X\|Z) = H(Z\|X)$
1/1	☒ True	☐ False	$H(X\|Y) = H(Y\|X)$
1/1	☐ True	☒ False	$H(X,Y) > H(Y)$
1/1	☒ True	☐ False	$H(X) = H(Y)$

Problem 2 [8 points]
Alice has 2 coins in her pocket: a fair coin which produces heads and tails with equal probability and a fake coin which produces only tails. She picks at random one of the coins and flips it indefinitely. The sequence of flips can be modeled as the output of the source $\mathcal{S} = S_1, S_2, \ldots$
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	☐ True	☒ False	$H(\mathcal{S}) = 1$
1/1	☒ True	☐ False	$H(S_3, S_4) < H(S_1) + H(S_2)$
1/1	☐ True	☒ False	$H(S_1, S_2) = H(S_1)$
1/1	☒ True	☐ False	$H(S_1) = H(S_2)$
1/1	☐ True	☒ False	$\mathcal{S}$ is not stationary
1/1	☒ True	☐ False	$H(S_1) = 2 - \frac{3}{4}\log_2 3$
1/1	☒ True	☐ False	$H^*(\mathcal{S}) < H(\mathcal{S})$
1/1	☒ True	☐ False	$H(S_1, S_2, \ldots, S_n) < n$

Problem 3 [3 points]
Consider the following decoding tree, where $\sum_{i=1}^{9} p_i = 1$ and where the probability assigned to an intermediate node equals the sum of the probabilities of the leaves (terminal nodes) below it.



What is the average codeword-length? Check one:

3/3
- ☐ $\frac{21}{16}$
- ☒ $\frac{37}{16}$
- ☐ 2
- ☐ 1

Problem 4 [2 points]
Let a, m, c be integers strictly larger than zero.
Answer the following True/False questions [1 point each]:

1/1 ☒ True ☐ False If $\gcd(a, m) = c$, then there exist integers u, v such that $c = au + mv$

1/1 ☐ True ☒ False If there exist integers u, v such that $c = au + mv$, then $\gcd(a, m) = c$

Problem 5 [3 points]
Answer the following True/False questions [1 point each].
For any $x, n \in \mathbb{Z}$, with $n \geq 0$:

1/1 ☒ True ☐ False $x^{10n+1} \equiv x \pmod{11}$

1/1 ☒ True ☐ False $x^{4n+1} \equiv x \pmod{10}$

1/1 ☐ True ☒ False $x^{10n+1} \equiv x \pmod{10}$

Problem 6 [3 points]
Let p be an odd prime number, and $q = 2p + 1$ another prime number.

How many elements of order p does $(\mathbb{Z}/q\mathbb{Z}, +)$ contain? Check one (1.5 points):

1.5/1.5
- ☐ $2p$
- ☒ 0
- ☐ p
- ☐ $p - 1$

How many elements of order p does $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, +)$ contain? Check one (1.5 points):

1.5/1.5
- ☐ 0
- ☐ p
- ☐ $p(p - 1)$
- ☒ $p - 1$

Problem 7 [4 points]

What is the multiplicative inverse of 5 in $(\mathbb{Z}/462\mathbb{Z}^*, \cdot)$? Check one:

- ☐ There is more than one
- ☐ 92
- ☒ 185
- ☐ 230
- ☐ 15
- ☐ 93
- ☐ 73
- ☐ It does not exist
- ☐ 5

4/4

Problem 8 [4 points]

Consider RSA with the following parameters: $p = 13$, $q = 7$, $m = pq$, $k = \text{lcm}(p-1, q-1)$. Which of the following could be chosen as encoding exponent e and decoding exponent d? Check one:

- ☐ $e = 6, d = 11$
- ☒ $e = 5, d = 5$
- ☐ $e = 17, d = 4$
- ☐ $e = 7, d = 8$
- ☐ $e = 12, d = 5$

4/4

Problem 9 [2 points]

In the one-time pad, if the key happens to be the all-zero sequence, then the ciphertext is identical to the plaintext, i.e. the message is sent in clear. To eliminate this possibility, if the key turns out to be the all-zero sequence, you throw it away and redo the random experiment of generating the key. Answer the following True/False question.

2/2

☐ True ☒ False The resulting cryptosystem achieves perfect secrecy.

Problem 10 [3 points]
Consider a finite field $\mathbb{F}$ of characteristic p. Answer the following True/False questions [1 point each]:

1/1 ☐ True ☒ False $x^{p-1} = 1$ for all non-zero $x \in \mathbb{F}$

1/1 ☒ True ☐ False $px = 0$ for all $x \in \mathbb{F}$

1/1 ☒ True ☐ False p is prime

Problem 11 [4 points]
Alice wants to add a signature to a message for Bob. Let t be the plaintext to be signed, h a hash function, and let f_A and f_B be Alice's and Bob's trapdoor one-way functions respectively, that one can find on the public directory. Alices's signature s is (check one):

☐ $s = h(f_A^{-1}(t))$

☐ $s = f_A(h(t))$

4/4 ☐ $s = f_B(h(t))$

☐ $s = f_B^{-1}(h(t))$

☒ $s = f_A^{-1}(h(t))$

Problem 12 [3 points]
What is the cardinality of $(\mathbb{Z}/291\mathbb{Z}^*, \cdot)$? Check one:

☐ 288

3/3 ☒ 192

☐ 194

☐ 290

Problem 13 [3 points]

Let $\mathcal{C}$ be an (n, k) Reed-Solomon code over $\mathbb{F}_q$. Suppose that we are given a codeword $\vec{x}$ with $n - k + e$ erasures, with $e \geq 0$. How many codewords of $\mathcal{C}$ are consistent with $\vec{x}$? Check one:

- [x] q^e
- [ ] q
- [ ] 1
- [ ] $n \quad k \quad e$
- [ ] q^{n-k+e}
- [ ] e
- [ ] 0

3/3

Problem 14 [4 points]

Consider a linear block code with parameters $n = 8$ and $k = 3$. Answer the following True/False questions [2 points each]. There necessarily exists a non-zero codeword $\vec{c}$ of Hamming weight $w(\vec{c})$ such that:

2/2 [x] True [ ] False $w(\vec{c}) \leq 6$

2/2 [ ] True [x] False $w(\vec{c}) \leq 5$

Problem 15 [2 points]

Let $\mathcal{C}$ be a linear block code. We transmit a codeword $\vec{x} \in \mathcal{C}$ over an error channel and we receive the word $\vec{y}$. Let $\vec{s}$ be its associated syndrome. Answer the following True/False questions [1 point each].

1/1 [ ] True [x] False If $\vec{s} = \vec{0}$, no error occurred during transmission

1/1 [x] True [ ] False If $\vec{s} = \vec{0}$, $\vec{y}$ is a codeword

Problem 16 [8 points]
The output symbols of a source are used to fill a $k \times m$ matrix A, where $m \geq 2$. Each column of A is considered as the information vector of an (n, k) MDS block code over the same alphabet as the source, where $n > k$. Let B be the matrix obtained by substituting each column of A with the corresponding codeword. B is an $n \times m$ matrix. Answer the following True/False questions [2 points each].

2/2 ☒ True ☐ False If we transmit one row of B after the other, then the decoder can reconstruct the source output even if the channel erases $m(n-k)$ consecutive symbols.

2/2 ☒ True ☐ False If we transmit one column of B after the other, then the decoder can reconstruct the source output even if the channel erases $n-k$ symbols, regardless whether they are consecutive or not.

2/2 ☐ True ☒ False If we transmit one row of B after the other, then the decoder can reconstruct the source output even if the channel erases $n-k+1$ symbols (not necessarily consecutive).

2/2 ☐ True ☒ False If we transmit one column of B after the other, then the decoder can reconstruct the source output even if the channel erases $m(n-k)$ consecutive symbols.

Problem 17 [2 points]
Answer the following True/False question.

2/2 ☐ True ☒ False The Singleton bound applies only to linear codes.

Problem 18 [3 points]
Consider an (n, k) block code $\mathcal{C}$ over an alphabet $\mathcal{A}$, where $k = \log_{|\mathcal{A}|} |\mathcal{C}|$ is an integer. Is it true that for any choice of k positions within an n-tuple, if we fill those positions with k elements of $\mathcal{A}$, there is one and only one choice for the remaining $n-k$ positions so that the resulting n-tuple is a codeword in $\mathcal{C}$? Check one:

☐ True only if the code is linear and the generator matrix is in systematic form.
☐ True if the code is linear.
3/3 ☐ True but the code has to be MDS and linear.
☒ True whenever the code is MDS.

Problem 19 [3 points]

Let

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 & 1 \end{pmatrix}$$

be the generator matrix of a $(6,3)$ linear block code over $\mathbb{F}_3 = (\mathbb{Z}/3\mathbb{Z}, +, \cdot)$. Find the corresponding generator matrix G_s in systematic form, and check the correct answer. Check one:

- ☐ The last column of G_s is the transpose of $(0,1,2)$
- ☐ The last column of G_s is the transpose of $(2,1,2)$

3/3

- ☒ The last column of G_s is the transpose of $(2,2,2)$
- ☐ The last column of G_s is the transpose of $(2,1,1)$

Problem 20 [3 points]

Find the value of x, y, z so that $(x,1,y,1,z,1)$ is a codeword of a (6,3) Reed Solomon code over $\mathbb{F}_7 = (\mathbb{Z}/7\mathbb{Z}, +, \cdot)$. Check one:

- ☐ More than one choice of x, y, z exists since the Reed Solomon code is not fully specified.

3/3

- ☐ No such x, y, z exists
- ☒ $x = 1,\ y = 1,\ z = 1$

Problem 21 [4 points]

A linear block code $\mathcal{C}$ over $\mathbb{F}_3 = (\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ is described by the following parity-check matrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 2 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

What is the minimum distance for this code? Check one (2 points):

- ☐ 2

2/2

- ☐ 4
- ☒ 3

A codeword of $\mathcal{C}$ is sent over an erasure channel and the output is $(?,?,0,2,1)$. Find the value of the two erased positions and check the correct answer. Check one (2 points):

- ☒ The sum (over $\mathbb{F}_3$) of the two erased positions is 0

2/2

- ☐ The sum (over $\mathbb{F}_3$) of the two erased positions is 1
- ☐ The sum (over $\mathbb{F}_3$) of the two erased positions is 2