Exam Solution
Total score: 80.5/80.5

+1/1/60+

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Advanced Information, Computation, Communication II

July 3, 2018

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 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.

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

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

Room:
Seat:

Student Name / Sciper no.:
Exam Solution

Problem 1 [4 points]

A 5-ary source S produces iid symbols following the distribution $p_S(0) = 1/2$, $p_S(1) = 1/4$, $p_S(2) = 1/8$, $p_S(3) = 1/16$, and $p_S(4) = 1/16$. For any integer $n > 0$, let C_n be the binary Huffman code for this source that encodes blocks of n symbols simultaneously. In the following questions, a code is optimal if it achieves the smallest average codeword-length per source symbol. Check one:

- ☐ There is no n for which C_n is optimal, since we can always decrease the average codeword-length by increasing n.
- 4/4 ☒ C_1 is optimal.
- ☐ C_1 is not optimal, but C_2 is.

Problem 2 [4 points]

Let X be a uniformly distributed random variable that takes values over the alphabet $\{0, \frac{1}{2}\pi, \pi, \frac{3}{2}\pi, 2\pi, \frac{5}{2}\pi, 3\pi, \frac{7}{2}\pi\}$. We further define $Y = 2^X$ and $Z = \sin(X)$. Answer the following True/False questions [1 point each]:

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

Problem 3 [4 points]

Let S be the source defined by the following table:

Alphabet	a	b	c	d	e
Probabilities	0.20	0.25	0.12	0.32	0.11

What is the smallest average codeword-length of a binary code that encodes one source symbol at a time? Check one:

- ☐ 2.43 bits
- ☐ 2.2 bits
- 4/4 ☐ 2.18 bits
- ☒ 2.23 bits
- ☐ 2.36 bits

Problem 4 [4 points]

Let $X \in \{0,1\}$ and $Y \in \{0,1\}$ be independent and uniformly distributed random bits, and let $\oplus$ be the addition modulo 2 operation. Answer the following True/False questions [1 point each]:

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

Problem 5 [4 points]

Consider the equation $[2]_8\, x + [3]_8 = [6]_8\, x + [7]_8$ with $x \in \mathbb{Z}/8\mathbb{Z}$. This equation has (check one):

- [ ] No solution
- [ ] A unique solution
- 4/4 [ ] An infinity of solutions
- [ ] 2 solutions
- [x] 4 solutions

Problem 6 [6 points]

Consider a symmetric-key cryptosystem which achieves perfect secrecy. Let T be the plaintext, C the cryptogram and K the key. Answer the following True/False questions [1 point each]:

1/1	[x] True	[ ] False	$H(T) \leq H(K)$
1/1	[x] True	[ ] False	$H(K\|C) \leq H(K)$
1/1	[x] True	[ ] False	$H(T\|C) \leq H(T, K\|C)$
1/1	[ ] True	[x] False	$H(T\|K, C) = H(T)$
1/1	[ ] True	[x] False	$H(T) < H(T\|C)$
1/1	[x] True	[ ] False	$H(T, K\|C) = H(K\|C) + H(T\|K, C)$

Problem 7 [4 points]

Is $10^{100} - 1$ invertible in $(\mathbb{Z}/77\mathbb{Z}, \cdot)$? Check one:

- [x] No
- 4/4 [ ] Yes

Problem 8 [4 points]

Let c_1 and c_2 be the encryption of the messages t_1 and t_2, respectively, using the same RSA public key (m, e). Answer the following True/False questions [1 point each]:

1/1	[x] True	[ ] False	$c_1 \cdot c_2$ is the encryption of $t_1 \cdot t_2$
1/1	[ ] True	[x] False	$c_1 + c_2$ is the encryption of $t_1 + t_2$
1/1	[x] True	[ ] False	$-c_1$ is the encryption of $-t_1$ because e is always an odd number
1/1	[x] True	[ ] False	c_1^{-1} is the encryption of t_1^{-1} (assuming that both inverses exist)

Problem 9 [2 points]
Answer the following True/False questions [1 point each]:

The RSA cryptosystem would be broken if you discovered a fast algorithm for:

1/1 ☒ True ☐ False Computing Euler's $\phi(m)$ for all positive integers m.

1/1 ☐ True ☒ False Given any two integers a and b, computing the Bézout coefficients u and v such that $ua + bv = \gcd(a, b)$.

Problem 10 [4.5 points]
Alice is sending to Bob the signed message (t, s), where t is the plaintext and s the signature done without hashing. The signature is obtained using RSA. The directory, which contains the public keys, has the following entries:

User	m	e
Alice	6	3
Bob	15	7

Which of the following signed messages is authentic (from Bob's viewpoint)? (check one):

4.5/4.5

- ☒ $(2, 2)$
- ☐ $(5, 2)$
- ☐ $(3, 2)$
- ☐ $(1, 2)$

Problem 11 [4.5 points]
Alice wants to send a private message t to Bob using ElGamal's encryption scheme. To do so, they agree on using the cyclic group $(\mathbb{Z}/5\mathbb{Z}^*, \cdot)$ and the generator $g = 3$. Bob chooses $x = 2$ and sends $g^x = 4$ to Alice. Alice sends back the cryptogram $(g^y, g^{xy}t) = (2, 3)$. What is the plaintext t? Check one:

4.5/4.5

- ☐ $t = 4$
- ☐ $t = 1$
- ☒ $t = 2$
- ☐ $t = 3$

Problem 12 [3 points]

Let p and q be two distinct prime numbers.

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

- [ ] $2p$
- [x] 0
- [ ] $p-1$
- [ ] p

1.5/1.5

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

- [ ] p
- [ ] 1
- [ ] $p-1$
- [x] 0

1.5/1.5

Problem 13 [4 points]
Consider a linear block code with parameters $n = 8$ and $k = 3$. Answer the following True/False questions [1 point each].

The code must contain a non-zero codeword of Hamming weight

1/1 ☒ True ☐ False 7 or less
1/1 ☐ True ☒ False 5 or less
1/1 ☒ True ☐ False 6 or less
1/1 ☐ True ☒ False 4 or less

Problem 14 [3 points]
Let $\mathbb{F}_q$ be the finite field of size q, and consider the vector space $V = \mathbb{F}_q^n$. Let $W \subseteq V$ be the linear subspace defined by a set of m linear homogeneous equations. Select the correct statement (check one):

☐ $\text{card}(W) \geq q^m$
☒ $\text{card}(W) \geq q^{n-m}$
3/3 ☐ $\text{card}(W) \leq q^{n-m}$
☐ $\text{card}(W) \leq q^m$

Problem 15 [4 points]
Let $\mathcal{C}$ be an (n, k) Reed-Solomon code over $\mathbb{F}_q$, where $k < n$, and consider the map

$$f : \mathcal{C} \longrightarrow \mathbb{F}_q^{n-1}$$
$$(s_1, \ldots, s_n) \longmapsto (s_1, \ldots, s_{n-1}).$$

Check one:

☐ The image of f is an $(n-1, k-1)$ block code, but not a Reed-Solomon code since it cannot fulfill the Singleton bound with equality.

4/4 ☐ The image of f is an $(n-1, k)$ block code, but not a Reed-Solomon code since it cannot fulfill the Singleton bound with equality.

☒ The image of f is a Reed-Solomon code.

Problem 16 [7 points]

Consider a source S defined in terms of an (n,k) linear block code $\mathcal{C}$ over $\mathbb{F}_q$ as follows, where $k < n$. The code $\mathcal{C}$ is generated by a matrix G in systematic form. The source outputs a codeword from $\mathcal{C}$, selected at random from the uniform distribution on $\mathcal{C}$. So, S takes values in $\mathcal{C}$. Check one (3 points):

- [ ] None of the other options
- [x] $H_q(S) = k$
- [ ] $H_q(S) = n$
- [ ] $H_q(S) = n - k$

3/3

Now consider the map

$$\Gamma : \mathcal{C} \longrightarrow \mathbb{F}_q^k$$
$$(s_1, \ldots, s_n) \longmapsto (s_1, \ldots, s_k).$$

Check one (4 points):

- [ ] The map Γ does not meet the definition of a source encoder since it is not invertible.
- [ ] The map Γ is a valid source encoder but not necessarily optimal in the sense that a uniquely-decodable q-ary code that achieves a smaller average codeword-length might exist.
- [x] The map Γ meets the definition of a source encoder and no uniquely-decodable q-ary code can achieve a smaller average codeword-length.

4/4

Problem 17 [4.5 points]

Consider an (n,k) binary block code, where n and k are even, used to transmit over a binary symmetric channel that flips the input with probability ϵ. The following expression

$$\sum_{i=0}^{\frac{n-k}{2}} \binom{n}{i} \epsilon^i (1-\epsilon)^{n-i}$$

is (check one):

- [ ] The probability that a minimum-distance decoder finds the correct codeword.
- [x] A lower bound to the probability that a minimum-distance decoder finds the correct codeword when the code is MDS.
- [ ] The probability that a minimum-distance decoder finds the correct codeword when the code is MDS.
- [ ] A lower bound to the probability that a minimum-distance decoder finds the correct codeword.

4.5/4.5

Problem 18 [5 points]

Let $\mathcal{C}$ be a $(7,3)$ linear code over $\mathbb{F}_7 = (\mathbb{Z}/7\mathbb{Z}, +, \cdot)$ given by a generator matrix which, once put in reduced echelon form, becomes

$$G = \begin{pmatrix} 1 & 0 & 2 & 0 & 3 & 3 & 3 \\ 0 & 1 & 1 & 0 & 2 & 3 & 4 \\ 0 & 0 & 0 & 1 & 1 & 2 & 1 \end{pmatrix}.$$

Check one (2 points):

2/2

- [ ] The code $\mathcal{C}$ is MDS
- [x] The code $\mathcal{C}$ is not MDS

Which one of the following words is contained in $\mathcal{C}$? Check one (3 points):

3/3

- [ ] $(1,2,4,1,3,1,1)$
- [ ] $(1,2,3,0,3,1,0)$
- [ ] $(1,2,4,2,2,6,0)$
- [x] $(1,2,4,3,3,1,0)$

Problem 19 [5 points]

Let $\mathcal{C}$ be an (n,k) Reed-Solomon code over $\mathbb{F}_q$. Suppose that we are given a channel output $y \in \mathbb{F}_q^n$ with $n-k+e$ erasures, where e is a positive integer. How many codewords are consistent with y? Check one:

5/5

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