Ens. : TEACHER NAME
EXAM NAME - MAN
DATE
Durée : XXX minutes

1

Student One

SCIPER : **111111**

Do not turn the page before the start of the exam. This document is double-sided, has 12 pages, the last ones possibly blank. Do not unstaple.

- Place your student card on your table.
- **No other paper materials** are allowed to be used during the exam.
- Using a **calculator** or **any electronic device** is not permitted during the exam.
- 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 uniformly at random over the possible options gains 0 points on average.
- Use a **black or dark blue ballpen** and clearly erase with **correction fluid** if necessary.
- Unless specified otherwise, all the entropies are in bits.

Respectez les consignes suivantes | Observe this guidelines | Beachten Sie bitte die unten stehenden Richtlinien

choisir une réponse | select an answer Antwort auswählen	ne PAS choisir une réponse | NOT select an answer NICHT Antwort auswählen	Corriger une réponse | Correct an answer Antwort korrigieren
☒ ☑ ■	□	□ ▢

ce qu'il ne faut **PAS** faire | what should **NOT** be done | was man **NICHT** tun sollte

▨ ☒ ○ ⊡ ▨ □

Pour votre examen, imprimez de préférence les documents compilés à l'aide de auto-multiple-choice.

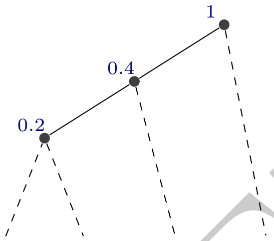
First part: Source Coding

For each question, mark the box corresponding to the correct answer. Each multiple choice question has **exactly one** correct answer.

Question 1

[2 points] Suppose we have a source S. Consider a Huffman encoding Γ for S constructed like we have seen in class. Suppose that $L(S, \Gamma) = 1.5$.

Can the following sub-tree be part of the Huffman tree corresponding to the Huffman code Γ? Remember: the numbers depicted represent the sum of the probabilities of the symbols corresponding to the leaves of the tree. For instance, 0.2 denotes the fact that the probabilities of the symbols in the leaves of the corresponding sub-tree sum to 0.2.



□ VRAI ■ FAUX

Question 2

[5 points] Let X be a random variable distributed over the alphabet $\mathcal{X} = \{0, 1, \ldots, n\}$. Assume also that there exist $x_1, x_2 \in \mathcal{X}$ such that $p_X(x_1) \neq p_X(x_2)$ (*i.e.*, X is not uniformly distributed over $\mathcal{X}$). Let $Y = 2^X$ and $Z = \lfloor X/2 \rfloor$.

$H(X, Z) > H(X)$

□ VRAI ■ FAUX

$H(Y) = H(X)$

■ VRAI □ FAUX

$H(Y|X) = H(Z|X)$

■ VRAI □ FAUX

$H(Y) \geq \log_2(n+1)$

□ VRAI ■ FAUX

$H(Z) = H(Y)$

□ VRAI ■ FAUX

Question 3

[3 points] Consider the following mysterious binary encoding:

symbol	encoding
a	??0
b	??0
c	??0
d	??0

where with '?' we mean that we do not know which bit is assigned as the first two symbols of the encoding of any of the source symbols a, b, c, d. What can you infer on this encoding assuming that the code-words are all different?

□ The encoding is uniquely-decodable but not prefix-free.

■ The encoding is uniquely-decodable.

□ We do not possess enough information to say something about the code.

□ It does not satisfy Kraft's Inequality.

Question 4

[4 points] Suppose that you possess a D-ary encoding Γ for the source S that does not satisfy Kraft's Inequality. Specifically, in this problem, we assume that our encoding satisfies $\sum_{i=1}^{n} D^{-l_i} = k+1$ with $k > 0$. What can you infer on the average code-word length $L(S,\Gamma)$?

■ $L(S,\Gamma) \geq H_D(S) - \log_D(e^k)$.

□ The code would not be uniquely-decodable and thus we can't infer anything on its expected length.

□ $L(S,\Gamma) \geq kH_D(S)$.

□ $L(S,\Gamma) \geq \frac{H_D(S)}{k}$.

Question 5

[4 points] Consider a source S with some distribution P_S over the alphabet $\mathcal{A} = \{a, b, c, d, e, f\}$. Consider the following encoding Γ over a code alphabet $\mathcal{D}$ of size D with the following codeword lengths:

	a	b	c	d	e	f
$l(\Gamma(\cdot))$	1	1	1	2	2	4

Answer the following true/false questions.

If $D = 4$ then Γ is necessarily uniquely-decodable.

□ VRAI ■ FAUX

If $D = 3$ then Γ is **not** uniquely-decodable .

■ VRAI □ FAUX

If $D = 4$ then Γ is necessarily prefix-free.

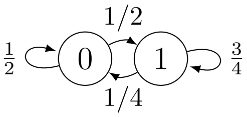
□ VRAI ■ FAUX

If $D = 2$ there exists a uniquely-decodable code with the same lengths of Γ.

□ VRAI ■ FAUX

Question 6

[6 points] Let $S_0, S_1, S_2, \dots$ be an infinite sequence produced by a source $\mathcal{S}$. All S_n take values in $\{0,1\}$, and S_{n+1} depends only on S_n, that is, $p_{S_{n+1}|S_0,\dots,S_n}(s_{n+1}|s_0,\dots,s_n) = p_{S_{n+1}|S_n}(s_{n+1}|s_n)$. The probability $p_{S_{n+1}|S_n}$ is schematically represented in the graph below:



For instance, the edge from 0 to 1 means that $p_{S_{n+1}|S_n}(1|0) = \frac{1}{2}$. We also have that $p_{S_0}(0) = 1$.

The source is regular.

■ VRAI □ FAUX

$H^\star(\mathcal{S})$ is finite.

■ VRAI □ FAUX

For every $n \geq 0$, $H(S_n|S_0,\dots,S_{n-1}) \neq H(S_n|S_{n-1})$.

□ VRAI ■ FAUX

For every $n \geq 0$, $\mathbb{P}(S_n = 0) = \frac{1}{3}4^{-n}(2 + 4^n)$.

■ VRAI □ FAUX

$H(\mathcal{S}) = h(1/3)$, where h is the binary entropy.

■ VRAI □ FAUX

Question 7

[2 points] Consider the following sources S_1, S_2, S_3, S_4 all defined on a 5-letter alphabet $\mathcal{S} = \{a, b, c, d, e\}$ and whose probability distributions are the followings

- $P_{S_1} = (0.172, 0.343, 0.175, 0.2, 0.11)$;
- $P_{S_2} = (0.025, 0.075, 0.15, 0.375, 0.375)$;
- $P_{S_3} = (0.125, 0.125, 0.5, 0.125, 0.125)$;
- $P_{S_4} = (0.1, 0.125, 0.225, 0.275, 0.275)$.

For which of these sources is the Shannon-Fano Encoding Γ_{SF} optimal?

□ All of the above.

■ The source S_3.

□ None of the above.

□ The source S_2.

□ The source S_1.

□ The source S_4.

Question 8

[4 points] Consider the following sequence of random variables $S_1, \ldots, S_n, \ldots$ Assume that the limit $H^\star(\mathcal{S}) = k$ exists and is finite. Suppose that there exists $\hat{n} > 0$ such that for all $i \geq \hat{n}$ one has that the marginal distributions of S_{i+1} and S_i satisfy $p_{S_{i+1}} = p_{S_i}$. Denote with $\mathcal{Y}_{\hat{n}}$ the alphabet of the source $S_{\hat{n}}$. Can one use this information to infer that the following holds:

$|\mathcal{Y}_{\hat{n}}| \geq 2^k$?

■ VRAI □ FAUX

Second part: Cryptography and Number Theory

For each question, mark the box corresponding to the correct answer. Each multiple choice question has **exactly one** correct answer.

Question 9

[3 points] Can a commutative group have two different identity elements, e_1, e_2?

□ Yes, product groups always have two different identity elements.

□ Yes, but only if $e_1^2 = e_2^2$.

■ No.

□ Yes, but only if they are inverses of each other.

Question 10:

[3 points] Let $K = (K_1, K_2, ..., K_n)$, where each K_i is independently chosen from $\{0, 1\}$ with uniform probability. Let $K' = (K'_1, K'_2, ..., K'_n)$ such that, for each i, $K'_i \in \{0, 1\}$ and

$$K'_i = \sum_{j=1}^{i} K_j \bmod 2.$$

Answer the following true/false questions.

Using K as the key one can achieve perfect secrecy if the message is n bits.

■ VRAI □ FAUX

Using K' as the key one can achieve perfect secrecy if the message is n bits.

■ VRAI □ FAUX

Question 11

[RSA Encryption, Part 1 - 3 points] Consider an RSA encryption where the public key is published as $(m, e) = (35, 11)$. Which one of the following numbers is a valid decoding exponent?

■ 11

□ 5

□ 7

□ 17

Question 12

[RSA Encryption, Part 2 - 5 points] Consider an RSA encryption where the public key is published as $(m, e) = (55, 17)$. Which one of the following numbers is a valid decoding exponent?

□ 83

■ 53

□ 23

□ 43

Question 13:

[2 points] Consider a message T and a key K chosen independently from T. Answer the following true/false questions.

If $H(T) \leq H(K)$, then there exists a perfectly secret encryption scheme using K.

□ VRAI ■ FAUX

If there exists a perfectly secret encryption scheme using K, then $H(T) \leq H(K)$.

■ VRAI □ FAUX

Question 14:

[4.5 points] Answer the following true/false questions.

$(\mathbb{Z}/20\mathbb{Z}, +)$ has exactly 3 elements with order 4.

□ VRAI ■ FAUX

$[5^{100}]_{21}$ has a multiplicative inverse.

■ VRAI □ FAUX

$(\mathbb{Z}/14\mathbb{Z}^*, \cdot)$ is isomorphic to $(\mathbb{Z}/6\mathbb{Z}, +)$.

■ VRAI □ FAUX

Question 15

[4 points] Consider the group $(\mathbb{Z}/23\mathbb{Z}^*, \cdot)$. Find how many elements of the group are generators of the group. (Hint: 5 is a generator of the group.)

□ 11
■ 10
□ 2
□ 22

Question 16

[4 points] Find $[3^{288294}]_{35}$.

□ 33
□ 9
■ 29
□ 11

Question 17

[5 points] In RSA, we set $p = 7, q = 11, e = 13$. The public key is $(m, e) = (77, 13)$. The ciphertext we receive is $c = 14$. What is the message that was sent?
(Hint: You may solve faster using Chinese remainder theorem.)

- □ $t = 7$
- □ $t = 63$
- ■ $t = 42$
- □ $t = 14$

Third part: Coding Theory

For each question, mark the box corresponding to the correct answer. Each multiple choice question has **exactly one** correct answer.

Question 18:

[4 points] Let $\mathcal{C}$ be a binary $(6, 3)$ linear code containing the codewords $\mathbf{x}_1 = 011011$, $\mathbf{x}_2 = 101101$ and $\mathbf{x}_3 = 111000$. Answer the following true/false questions.

The rate of the code is $R = \frac{1}{2}$.

☒ VRAI □ FAUX

A generator matrix for the code is

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

□ VRAI ☒ FAUX

The minimum distance of the code is $d_{\min} = 3$.

☒ VRAI □ FAUX

The codewords $\mathbf{x}_1, \mathbf{x}_2$ and $\mathbf{x}_3$ uniquely determine $\mathcal{C}$.

☒ VRAI □ FAUX

Question 19:

[4 points] Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two linear codes in $\mathbb{F}_q^n$. Let $\mathcal{C}_a = \mathcal{C}_1 \cap \mathcal{C}_2$ be the code formed by the codewords that $\mathcal{C}_1$ and $\mathcal{C}_2$ have in common. Let $\mathcal{C}_b = \mathcal{C}_1 \cup \mathcal{C}_2$ be the code formed by all the codewords of $\mathcal{C}_1$ and all the codewords of $\mathcal{C}_2$. Answer the following true/false questions.

$\mathcal{C}_a$ is necessarily a linear code.

☒ VRAI □ FAUX

$\mathcal{C}_b$ is necessarily a linear code.

□ VRAI ☒ FAUX

Question 20

[3 points] Let $\mathcal{C}$ be a (n, k) Reed-Solomon code on $\mathbb{F}_q$. Let $\mathcal{C}'$ be the $(2n, k)$ code such that each codeword of $\mathcal{C}'$ is a codeword of $\mathcal{C}$ repeated twice, i.e., if $(x_1, \ldots, x_n) \in \mathcal{C}$, then $(x_1, \ldots, x_n, x_1, \ldots, x_n) \in \mathcal{C}'$. What is the minimum distance of $\mathcal{C}'$?

□ $2n - k + 2$

□ $2n - 2k + 1$

■ $2n - 2k + 2$

□ $2n - k + 1$

Question 21:

[4 points] Let $\mathcal{C}$ be a binary $(5, 2)$ linear code with generator matrix

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

and consider a minimum-distance decoder obtained by choosing the coset leaders of the standard array of $\mathcal{C}$ so that the error probability is minimized under a binary symmetric channel with bit-flip probability $\epsilon < \frac{1}{2}$. Answer the following true/false questions.

The word 00101 is certainly not one of the coset leaders.

■ VRAI □ FAUX

The decoder can correct some errors of weight 2.

■ VRAI □ FAUX

The word 00100 must be one of the coset leaders.

■ VRAI □ FAUX

The decoder can correct all errors of weight 1.

■ VRAI □ FAUX

Question 22:

[4 points] Let $\mathcal{S} \subset \mathbb{F}_4^4$ be the subset of vectors $\mathbf{v} = (v_1, v_2, v_3, v_4)$ satisfying the equation

$$v_1^2 + v_2^2 + v_3^2 + v_4^2 = 0.$$

Hint: Recall from class that the addition and multiplication tables of $\mathbb{F}_4 = \{0, 1, a, b\}$ *are the following.*

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Answer the following true/false questions.

$\mathcal{S}$ has 64 elements.

■ VRAI □ FAUX

$\mathcal{S}$ is a vector space.

■ VRAI □ FAUX

Question 23

[4 points] Let $\mathcal{C}$ be a binary (n, k) linear code with minimum distance $d_{\text{min}} = 4$. Let $\mathcal{C}'$ be the code obtained by adding a parity-check bit $x_{n+1} = x_1 \oplus x_2 \oplus \cdots \oplus x_n$ at the end of each codeword of $\mathcal{C}$. Let d'_{min} be the minimum distance of $\mathcal{C}'$. Which of the following is true?

■ $d'_{\text{min}} = 4$

□ d'_{min} can take different values depending on the code $\mathcal{C}$.

□ $d'_{\text{min}} = 5$

□ $d'_{\text{min}} = 6$

Question 24:

[4.5 points] Let $\mathcal{C}$ be the $(6,3)$ linear code on $\mathbb{F}_3$ whose parity-check matrix is

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

Answer the following true/false questions.

The minimum distance of $\mathcal{C}$ is $d_{\text{min}} = 2$.

□ VRAI ■ FAUX

The matrix

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

is also a valid parity-check matrix for $\mathcal{C}$.

■ VRAI □ FAUX

The sequence $\mathbf{y} = 111000$ is a codeword of $\mathcal{C}$.

■ VRAI □ FAUX

Question 25

[2 points] Let b be the maximum number of linearly independent columns of a parity check matrix H of a linear code. Then, the minimum distance of the code is $b + 1$.

□ VRAI ■ FAUX