1

Prof. M. C. Gastpar
Advanced information, computation, communication II - MAN
22 June 2023
Duration: 180 minutes

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

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

[4 points] Let S_1 be a random variable taking values in $\{a, b\}$ with probability $p_{S_1}(a) = \frac{1}{4}$ and $p_{S_1}(b) = \frac{3}{4}$. Let S_2 be a random variable, independent of S_1, taking values in $\{c, d\}$ with probability $p_{S_2}(c) = q$ and $p_{S_2}(d) = 1 - q$, for some $q \in [0, 1]$. Let Γ_H be the binary Huffman code for the sequence $S = S_1 S_2$, and let $L(S, \Gamma_H)$ be the average codeword-length of Γ_H. Answer the following true/false questions.

$1 \leq L(S, \Gamma_H) \leq 2$ for all $q \in [0, 1]$.

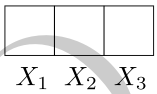
☐ VRAI ☐ FAUX

$\text{length}(\Gamma_H(bc)) = 3$ for all $q < \frac{1}{4}$.

☐ VRAI ☐ FAUX

Question 2

[4 points] Consider the following three boxes.



We fill the three boxes with bits with the following procedure:

(a) We select one box uniformly at random and we fill it with 1;

(b) For each of the remaining two boxes, we fill it with either 0 or 1 independently and uniformly at random.

We denote the value in the i-th box with the random variable X_i, as in the figure. What is $H(X_1, X_2, X_3)$?

☐ $\log 7$
☐ $\frac{3}{2} + \frac{3}{4} \log 3$
☐ $2 + \log 3$
☐ $\log 7 - \frac{6}{7} \log 3$

Question 3

[4 points] Let S be a random variable taking values in $\{a, b, c, d, e\}$ with the following probabilities.

	a	b	c	d	e
$p_S(\cdot)$	1/3	1/3	1/9	1/9	1/9

Let Γ_D be the D-ary Huffman code for S. Let $L(S, \Gamma_D)$ be the average codeword-length of Γ_D, and let $H_D(S)$ be the D-ary entropy of S. Answer the following true/false questions.

$L(S, \Gamma_D) > H_D(S)$ for every $D > 3$.

☐ VRAI ☐ FAUX

If $D = 3$, then $L(S, \Gamma_D) = H_D(S)$.

☐ VRAI ☐ FAUX

Question 4

[4 points] Let $X_1, X_2, \ldots$ be i.i.d. binary random variables with $p_{X_i}(1) = \frac{1}{4}$ for every $i \geq 1$. Let Y_1 be a uniform binary random variable, and let

$$Y_i = Y_{i-1} \oplus X_{i-1}$$

for every $i \geq 2$, where $\oplus$ denotes the modulo-2 sum. For any given $n \geq 1$, what is the value of $H(Y_1, Y_2, \ldots, Y_n)$? [Hint: what is the value of $H(Y_i|Y_1, \ldots, Y_{i-1})$?]

☐ n
☐ $\left(2 - \frac{3}{4}\log 3\right) n + \frac{3}{4}\log 3 - 1$
☐ $\left(2 - \frac{3}{4}\log 3\right) n + 1$
☐ $\left(3 - \frac{3}{4}\log 3\right) n + \frac{3}{4}\log 3 - 2$

Question 5

[2 points] Let E and F be two events. Suppose that they satisfy $p(E|F) = p(E) > 0$.

Claim: Then we must have $p(F|E) = p(F)$.

☐ VRAI ☐ FAUX

Question 6

[4 points] Consider the source $S_1, S_2, \ldots$ such that S_1 is uniformly distributed on $\mathbb{Z}/10\mathbb{Z}^*$, and for every $n \geq 1$, S_{n+1} is distributed uniformly on $\mathbb{Z}/(S_n+1)\mathbb{Z}^*$. Let $H(\mathcal{S}) = \lim_{n\to\infty} H(S_n)$. Answer the following true/false questions.

$H(\mathcal{S}) = 0$

☐ VRAI ☐ FAUX

The source is stationary.

☐ VRAI ☐ FAUX

Question 7

[2 points] A binary prefix-free code Γ is made of four codewords. The first three codewords have codeword lengths $\ell_1 = 2$, $\ell_2 = 3$ and $\ell_3 = 3$. What is the minimum possible length for the fourth codeword?

☐ 2
☐ 3
☐ 1
☐ 4

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 8:

[3 points] Consider an RSA encryption where the (p, q) are determined as $(53, 61)$. Check if the following encoding and decoding exponent pairs are valid.

$(e, d) = (319, 23)$ are valid exponents.

☐ VRAI ☐ FAUX

$(e, d) = (123, 79)$ are valid exponents.

☐ VRAI ☐ FAUX

$(e, d) = (7, 223)$ are valid exponents.

☐ VRAI ☐ FAUX

Question 9

[4 points] Find all solutions of $24x + [9]_{45} = [13]_{45}$ in the range $[0, 44]$. How many different solutions are there?

- ☐ 0
- ☐ 3
- ☐ 2
- ☐ 1

Question 10:

[4 points] Let $n \geq 2$ be a positive integer, and M a uniformly distributed binary message of length $2n$. Let $P_K(M)$ denote the one-time pad encryption of M with key K. Let K_1 be a uniformly distributed binary key length n. Let K_2 be the complement of K_1. Let K_3 be the reverse of K_1. Let $K_i||K_j$ denote the concatenation of the two keys. Answer the following true/false questions.

Encryption with the key $K_5 = (K_1||K_2)$, $P_{K_5}(M)$ provides perfect secrecy.

☐ VRAI ☐ FAUX

Encryption with the key $K_4 = (K_1||K_1)$, $P_{K_4}(M)$ provides perfect secrecy.

☐ VRAI ☐ FAUX

Encryption with the key $K_6 = (K_1||K_3)$, $P_{K_6}(M)$ provides perfect secrecy.

☐ VRAI ☐ FAUX

Let K_7 be a key that is either equal to K_2 or K_3 with uniform probability. Encryption with the key $K_8 = (K_1||K_7)$, $P_{K_8}(M)$ provides perfect secrecy.

☐ VRAI ☐ FAUX

Question 11

[3 points] Find x such that $10x = [38]_{56}$.

- ☐ 49
- ☐ 28
- ☐ 41
- ☐ 15

Question 12:

[2 points] Let G be a set and $*$ a commutative operation on pairs of elements from G. Suppose there exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$. Also, suppose there exist elements $b, c, d \in G$ such that $b * c = d * c$.

If $b \neq d$, then $(G, *)$ cannot be a group.

☐ VRAI ☐ FAUX

$(G, *)$ is a group if and only if $b = d$.

☐ VRAI ☐ FAUX

Question 13

[4 points] Consider the group $(\mathbb{Z}/153\mathbb{Z}^*, \cdot)$. Find how many elements are in the group.

- [ ] 128
- [ ] 127
- [ ] 96
- [ ] 97

Question 14

[4 points] Passing on secrets: Alice has posted her RSA credentials as (m, e), with m the modulus and e the encoding exponent. As required by RSA, she keeps her decoding exponent d preciously secret. Bob has a message t_1, RSA-encrypts it using (m, e_1) and passes the resulting cryptogram c_1 on to Carlos. Carlos has a message t_2, RSA-encrypts it using (m, e_2) to obtain the cryptogram c_2. Then, Carlos multiplies the two cryptograms, $(c_1 \cdot c_2) \mod m$, and passes this to Alice. Alice applies her regular RSA decryption to $(c_1 \cdot c_2) \mod m$. Under what condition is the result of this decryption exactly equal to the product $(t_1 \cdot t_2) \mod m$?

- [ ] If d is prime and $(e_1 + e_2) \mod m = 1$.
- [ ] If for some integer ℓ, we have $e_1 e_2 d = \ell\phi(m) + 1$, where $\phi(\cdot)$ denotes Euler's totient function.
- [ ] If $e_1 = e_2 = e$.
- [ ] If $e_1 + e_2 = e$.

Question 15

[4 points] Find $[5263^{79359}]_{15}$.

- [ ] 13
- [ ] 7
- [ ] 8
- [ ] 12

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 16:

[4 points] Let $\mathbb{F}$ be a field of cardinality q and let $0 < k < n \leq q$ be unspecified integers. As seen in the lecture, we generate a (n, k, d_{min}) Reed-Solomon code with the following mapping:

$$\mathbb{F}^k \to \mathbb{F}^n \quad , \quad \vec{u} \mapsto \vec{c} = (P_{\vec{u}}(a_1), P_{\vec{u}}(a_2), \dots, P_{\vec{u}}(a_n))$$

for $a_i \in \mathbb{F}$ all distinct and P a polynomial of degree $k-1$ with coefficient vector $\vec{u} \in \mathbb{F}^k$.
Now, we construct a (n, k', d'_{min}) code $\mathcal{C}'$ similarly to the above one by assigning $a_1 \leftarrow a_2$ while leaving n, P and $a_2, \dots, a_n$ unchanged. As before, the code is generated by evaluating $P_{\vec{u}}(a_2, a_2, a_3, \dots, a_n)$ over all possible coefficients vectors $\vec{u} \in \mathbb{F}^k$. This is by definition not an RS code, however it is still a well-defined linear block code.
Answer the following true/false questions.

We know for certain that $d'_{min} = d_{min} - 1$.

☐ VRAI ☐ FAUX

We know for certain that $k' = k - 1$.

☐ VRAI ☐ FAUX

Question 17

[3 points] Let $\mathcal{C}_1$ be a (n_1, k) linear block code over $\mathbb{F}_p$ with p prime and $|\mathcal{C}_1| = 27$. Let $\mathcal{C}_2$ be a (n_2, k) linear block code over $\mathbb{F}_2$ of the same dimension k. Which of the following is true?

- ☐ $|\mathcal{C}_2| = 21$
- ☐ $|\mathcal{C}_2| = 27$
- ☐ $|\mathcal{C}_2| = 8$
- ☐ $|\mathcal{C}_2| = 16$

Question 18:

[4 points] Let $G_i, i \in \{1, \ldots, 8\}$, be valid generator matrices of dimensions $\mathbb{F}^{k_i \times n_i}$, all over the same field $\mathbb{F}$. Which of the following are always valid generator matrices?
Hint: recall that "valid" means that for all i, $k_i \le n_i$ and rank$(G_i) = k_i$.

$\left(G_3 \;\middle|\; \begin{array}{c|c} G_4 & 0 \\ \hline 0 & G_5 \end{array} \right)$ where $k_3 = k_4 + k_5$.

☐ VRAI ☐ FAUX

$\begin{pmatrix} G_1 \\ \hline G_2 \end{pmatrix}$ where $n_1 = n_2$ and $k_1 + k_2 \le n_1$.

☐ VRAI ☐ FAUX

$D_1 \cdot G_6 \cdot D_2$, where $D_1 \in \mathbb{F}^{k_6 \times k_6}$ and $D_2 \in \mathbb{F}^{n_6 \times n_6}$ are diagonal matrices with non-zero diagonal elements.

☐ VRAI ☐ FAUX

$G_7 + G_8$ with $k_7 = k_8$ and $n_7 = n_8$.

☐ VRAI ☐ FAUX

Question 19:

[4 points] Let $\mathcal{C}_1$ be a linear code over $\mathbb{F}_3^n$, and let $\mathcal{C}_2$ be a linear code over $\mathbb{F}_2^n$. Answer the following true/false questions.

$\mathcal{C}_1 \cap \mathcal{C}_2$ is necessarily a linear code over $\mathbb{F}_2^n$.

☐ VRAI ☐ FAUX

$\mathcal{C}_1 \cup \mathcal{C}_2$ is necessarily a linear code over $\mathbb{F}_3^n$.

☐ VRAI ☐ FAUX

Question 20

[3 points] A colleague challenges you to create a $(n-1, k, d_{min})$ code $\mathcal{C}'$ from a (n, k, d_{min}) code $\mathcal{C}$ as follows: given a generator matrix G that generates $\mathcal{C}$, drop one column from G. Then, generate the new code with this truncated $k \times (n-1)$ generator matrix.
The catch is that your colleague only gives you a set $\mathcal{S} = \{\vec{s}_1, \vec{s}_2, \vec{s}_3\}$ of 3 columns of G that you are allowed to drop, where $\vec{s}_1$ is the all-zeros vector, $\vec{s}_2$ is the all-ones vector, and $\vec{s}_3$ is a canonical basis vector. From the length of the columns s_i you can infer k. You do not know n, neither do you know anything about the $n-3$ columns of G that are not in $\mathcal{S}$. However, your colleague tells you that G is in systematic form, i.e., $G = [I \;\; P]$ for some unknown P, and that all of the elements in $\mathcal{S}$ are columns of P.
Which of the following options in $\mathcal{S}$ would you choose as the column of G to drop?

- ☐ $\vec{s}_3$ (one of the canonical basis vectors).
- ☐ $\vec{s}_1$ (the all-zeros vector).
- ☐ $\vec{s}_2$ (the all-ones vector).
- ☐ It is impossible to guarantee that dropping a column from $\mathcal{S}$ will not decrease the minimum distance.

Question 21

[4 points] Let $\mathcal{C}$ be a (n, k) linear block code over $\mathbb{F}_2$ of block length n such that n is even and minimum distance $d_{min} = 3$. We construct a new code $\mathcal{C}'$ by appending onto each codeword $\vec{x} \in \mathcal{C}$ three parity bits as follows:
$x_{n+1} = x_1 \oplus x_3 \oplus x_5 \oplus \ldots \oplus x_{n-1}$,
$x_{n+2} = x_2 \oplus x_4 \oplus x_6 \oplus \ldots \oplus x_n$,
$x_{n+3} = x_1 \oplus x_2 \oplus x_3 \oplus \ldots \oplus x_n$.
Denote the minimum distance of this new linear block code by d'_{min}. Which of the following is true?

- ☐ $d'_{min} = 3$
- ☐ $d'_{min} = 4$
- ☐ We cannot tell with certainty what d'_{min} is; it depends on $\mathcal{C}$.
- ☐ $d'_{min} = 5$

Question 22:

[6 points] Let

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

be the generator matrix of a $(6, 4)$ linear code $\mathcal{C}$ over $\mathbb{F}_2$.
Answer the following true/false questions.

$d_{min} = 2$.

☐ VRAI ☐ FAUX

Performing an arbitrary column permutation on G yields a generator matrix of a linear code with the same parameters n, k, d_{min}.

☐ VRAI ☐ FAUX

If one substitutes the last row of G by $(1, 0, 0, 1, 1, 1)$, the thereby obtained matrix generates the same code $\mathcal{C}$.

☐ VRAI ☐ FAUX

G admits a systematic form (i.e., it can be put into systematic form via elementary row operations).

☐ VRAI ☐ FAUX