Fondements de l'informatique. Examen
Durée: 3h

Les 4 parties sont indépendantes, et peuvent être traitées dans un ordre quelconque. On pourra admettre le résultat d'une question pour passer aux questions suivantes. On pourra utiliser tous les résultats et les théorèmes démontrés ou énoncés en cours ou en petite classe ou dans le polycopié sans chercher à les redémontrer.

Il est possible d'avoir la note maximale sans répondre à toutes les questions. La difficulté des questions n'est pas une fonction linéaire ni croissante de leur numérotation.

La ***qualité et clarté de votre argumentation et de votre rédaction*** *sera une partie importante de votre évaluation.*

1 Machines de Turing

Question 1.1. *Parmi les questions suivantes, lesquelles sont décidables ? Récursivement énumérable ? dans P ? Justifier votre réponse.*

- *Déterminer si une machine de Turing M est telle qu'elle accepte un langage qui contient des mots d'au moins* 10 *longueurs différentes.*
- *Déterminer si un programme Python contient au moins* 10 *lignes de codes.*

On admettra dans la suite qu'il existe une machine de Turing universelle implémentable en moins de 10 000 lignes de Python.

Question 1.2. *Montrer que le langage suivant est indécidable mais récursivement énumérable : Déterminer si un programme Python exécute au moins* 100 000 *lignes de code différentes (c'est à dire à des positions différentes dans le programme) sur une entrée donnée (et peut s'arrêter ou non).*

Question 1.3. *Montrer que le langage suivant n'est ni décidable, ni récursivement énumérable : Déterminer si une machine de Turing M est telle qu'elle accepte un langage qui contient au moins un mot de chaque longueur.*

2 Problèmes de tuiles

On considère un ensemble fini $\mathcal{T}$, dont les élements sont appelés des *tuiles*. On fixe des relations de compatibilité entre tuiles : on fixe $H \subseteq \mathcal{T}^2$ qui indique les compatibilités horizontales, et $V \subseteq \mathcal{T}^2$ les compatibilités verticales.

On dit qu'une partie $\mathcal{E}$ du plan $\mathbb{Z}^2$ peut être *résolue* par $\mathcal{T}$ s'il existe une façon de placer les tuiles sur le plan qui respecte ces relations de compatibilité : Formellement, s'il existe une fonction $f : \mathcal{E} \to \mathcal{T}$ telle que, pour tout $(m, n) \in \mathcal{E}$,

1. si $(m+1, n) \in \mathcal{E}$ alors $(f(m, n), f(m+1, n)) \in H$ (compatibilité horizontale),
2. si $(m, n+1) \in \mathcal{E}$ alors $(f(m, n), f(m, n+1)) \in V$ (compatibilité verticale).

Question 2.1. *Montrer que $\mathbb{Z}^2$ peut être résolu par $\mathcal{T}$ si et seulement si tous les carrés $[\![-n, n]\!]^2$, pour $n \in \mathbb{N}$, peuvent être résolus par $\mathcal{T}$, où $[\![-n, n]\!]^2 = \{(x, y) \in \mathbb{Z}^2 : -n \leqslant x \leqslant n \wedge -n \leqslant y \leqslant n\}$.*

Remarques sur la complexité

Dans la suite de cet examen, R sera toujours un anneau (généralement $\mathbb{Z}$ ou $\mathbb{Q}$). On notera $R^{n\times m}$ l'ensemble des matrices à n lignes et m colonnes et à coefficients dans R. On notera $I_n \in R^{n\times n}$ la matrice identité de taille n et 0_n la matrice nulle. On posera $\log_k^+(x) = \log_k \max(1, x)$ qui sera utile pour exprimer des complexité sans traiter le cas du mot vide à part.

On pourra utiliser sans le mentionner qu'ajouter, soustraire, diviser et multiplier des nombres rationnels se fait en temps polynomial. De même, ajouter, soustraire et multiplier des matrices à coefficients dans R ne nécessite qu'un nombre polynomial d'opérations arithmétiques dans R. Lorsqu'une matrice est inversible, son inverse est aussi calculable en nombre polynomial d'opérations arithmétiques.

3 Programmation linéaire en nombre entiers

On s'intéresse au problème suivant, qui joue un rôle important en optimisation combinatoire.

`PROG–LIN–ENTIER` :
- **Donnée**: une matrice $C \in \mathbb{Z}^{n\times m}$ et un vecteur $b \in \mathbb{Z}^n$
- **Réponse**: existe-t-il $x \in \mathbb{Z}^m$ tel que[†] $Cx \leqslant b$?

On admettra que ce problème est dans NP, ce qui n'est pas complètement évident. On rappelle/admettra que le problème `3-SAT` suivant est NP-complet :
- **Donnée**: un ensemble de variables $x_1, \dots, x_m$ et une formule $F = C_1 \wedge C_2 \cdots \wedge C_n$ avec $C_i = y_{i,1} \vee y_{i,2} \vee y_{i,3}$ où pour tout i et j, $y_{i,j}$ est soit x_k , soit $\neg x_k$ pour l'un des x_k.
- **Réponse**: Décider si F est satisfiable : c'est-à-dire décider s'il existe $x_1, \dots, x_m \in \{0, 1\}$ tels que F s'évalue en vraie pour cette valeur de ses variables $x_1, \dots, x_m$.

Question 3.1. *Montrer que le problème `3-SAT` se réduit en temps polynomial au même problème avec la contrainte en plus que chaque clause ne contient pas à la fois une variable et sa négation.*

Pour une formule F de `3-SAT` comme ci-dessus, on considère la matrice $C^F \in \mathbb{Z}^{n\times m}$ définie par

$$C^F_{i,j} = \begin{cases} -1 & \text{si la variable } x_j \text{ apparaît sans négation dans } C_i, \\ 1 & \text{si la variable } x_j \text{ apparaît avec négation dans } C_i, \\ 0 & \text{si la variable } x_j \text{ n'apparaît pas } C_i. \end{cases}$$

Notons que cela est bien défini grâce à la question 3.1. On pose le vecteur $b^F \in \mathbb{Z}^n$ défini par

$$b^F_i = -1 + \sum_{j=1}^{m} \max(0, C^F_{i,j}).$$

Exemple. Prenons $m = 4$ variables et $F = (x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee \neg x_3 \vee x_4)$ avec $n = 2$ clauses. La matrice C^F et le vecteur b^F sont alors

$$C^F = \begin{pmatrix} -1 & 1 & -1 & 0 \\ -1 & 0 & 1 & -1 \end{pmatrix}, \qquad b^F = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

En effet, la variable x_1 apparaît sans négation dans les deux clauses (d'où les -1 de la première colonne), x_2 apparait négativement dans C_1 et pas du tout dans C_2, x_3 apparaît positivement dans C_1 et négativement dans C_2, et enfin x_4 n'apparaît pas dans C_1 et positivement dans C_2.

Question 3.2. *Montrer que F est satisfiable si et seulement s'il existe $x \in \{0, 1\}^m$ tel que $C^F x \leqslant b^F$.*

†. Ici, $Cx \leqslant b$ veut dire que $(Cx)_i \leqslant b_i$ pour tout $i = 1, \dots, n$.

On considère la variante suivante du problème PROG–LIN–ENTIER qui sera utile pour la suite.

PROG–LIN–ENTIER–CONJONCTION :
- **Donnée**: deux matrices $C \in \mathbb{Z}^{n\times m}$ et $C' \in \mathbb{Z}^{n'\times m}$, et deux vecteurs $b \in \mathbb{Z}^n$ et $b' \in \mathbb{Z}^{n'}$
- **Réponse**: existe-t-il $x \in \mathbb{Z}^m$ tel que $Cx \leqslant b$ et $C'x \leqslant b'$?

Question 3.3. *Montrer que PROG–LIN–ENTIER–CONJONCTION se réduit en temps polynomial au problème PROG–LIN–ENTIER.*

Question 3.4. *Montrer qu'il existe une matrice $D \in \mathbb{Z}^{2m\times m}$ et un vecteur $d \in \mathbb{Z}^{2m}$, tels que pour tout $x \in \mathbb{Z}^m$, $Dx \leqslant d$ si et seulement si $x \in \{0,1\}^m$.*

Question 3.5. *Montrer que PROG–LIN–ENTIER est* NP*-complet.*

Une variante importante du problème PROG–LIN–ENTIER est celui de l'existence d'une solution à un système linéaire en nombre entier. Pour $E = \mathbb{N}$ ou $\mathbb{Z}$, définit le problème suivant, dont on admettra qu'il est dans NP :

E–SYS-LINEAIRE :
- **Donnée**: une matrice $B \in \mathbb{Z}^{n\times m}$ et un vecteur $z \in \mathbb{Z}^n$
- **Réponse**: existe-t-il $x \in E^m$ tel que $Bx = z$?

Question 3.6. *Montrer que* $\mathbb{N}$*–SYS-LINEAIRE est* NP*-complet.*

4 Problèmes de (semi-)groupes de matrices

Dans la suite, on se donne un ensemble fini $A \subseteq R^{n\times n}$ de matrices, à coefficients dans un anneau R qui sera soit $\mathbb{Z}$ soit $\mathbb{Q}$. On définit le *semi-groupe* généré par A, noté $[\![A]\!]$, comme l'ensemble des produits finis de matrices de A. Formellement,

$$[\![A]\!] = \{X_1 \cdots X_m : m \in \mathbb{N}, X_1, \ldots, X_m \in A\}.$$

Si toutes les matrices de A sont inversibles, on définit aussi le *groupe* généré par A, noté $(\!|A|\!)$, qui est l'ensemble des produits finis de matrices de A ainsi que leurs inverses. Formellement,

$$(\!|A|\!) = [\![A \cup \overline{A}]\!], \qquad \overline{A} = \{M^{-1} : M \in A\}.$$

On **prendra garde** que $[\![A]\!] \neq (\!|A|\!)$ en général. On s'intéressera dans la suite aux problèmes suivants :

(R,n)–SEMIGROUPE–MORTALITÉ :
- **Donnée**: ensemble fini $A \subseteq R^{n\times n}$
- **Réponse**: $[\![A]\!]$ contient-il 0_n ?

(R,n)–SEMIGROUPE–APPARTENANCE :
- **Donnée**: ensemble fini $A \subseteq R^{n\times n}$ et $T \in R^{n\times n}$
- **Réponse**: $[\![A]\!]$ contient-il T ?

(R,n)–GROUPE–IDENTITÉ :
- **Donnée**: ensemble fini $A \subseteq R^{n\times n}$
- **Réponse**: $(\!|A|\!)$ contient-il I_n ?

(R,n)–GROUPE–APPARTENANCE :
- **Donnée**: ensemble fini $A \subseteq R^{n\times n}$ et $T \in R^{n\times n}$
- **Réponse**: $(\!|A|\!)$ contient-il T ?

Question 4.1. *Montrer que* $[\![A]\!] \neq (\!|A|\!)$ *pour* $A = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$.

Question 4.2. *Montrer que pour tout $R \in \{\mathbb{Z}, \mathbb{Q}\}$ et n, (R,n)–SEMIGROUPE–MORTALITÉ se réduit en temps polynomial au problème (R,n)–SEMIGROUPE–APPARTENANCE. Montrer que (R,n)–GROUPE–APPARTENANCE se réduit en temps polynomial à (R,n)–SEMIGROUPE–APPARTENANCE.*

Question 4.3. *Soit L et L' deux langages. Montrer que si L se réduit en temps polynomial vers L' et si $L' \in$ NP alors $L \in$ NP.*

5 Semi-groupes : le cas de la dimension 1

On s'intéresse tout d'abord au cas où $n = 1$, et on identifie les matrices de taille 1×1 avec R.

On rapelle que pour qu'un problème soit dans NP, il doit admettre un vérificateur polynomial et des certificats de taille **polynomial en la taille de l'entrée**.

Question 5.1. *Pourquoi est-ce qu'il n'est pas évident a priori que les problèmes définis dans la partie 4 sont dans* NP*, même pour $R = \mathbb{Z}$ et $n = 1$?*

Question 5.2. *Soit $A \subseteq \mathbb{Z}$ un ensemble fini et $t \in \mathbb{Z}$. Montrer que si $t \in [\![A]\!]$ alors il existe $a_1, \dots, a_m \in A$ tels que $t = a_1 \cdots a_m$ et $m \leqslant 1 + \log_2^+ |t|$.*

Question 5.3. *En déduire que tous les problèmes ci-dessus sont dans* NP *pour $R = \mathbb{Z}$ et $n = 1$.*

On suppose maintenant que $R = \mathbb{Q}$ (ce qui englobe le cas $R = \mathbb{Z}$ de toute façon). Fixons une instance (A, t) de $(\mathbb{Q}, 1)$–`SEMIGROUPE–APPARTENANCE` ou $(\mathbb{Q}, 1)$–`GROUPE–APPARTENANCE` . Sans perte de généralité, on peut supposer que $t \neq 0$ car le problème est trivial sinon. De plus, on peut supposer que $0 \notin A$ car 0 ne sera jamais utilisé dans la solution si $t \neq 0$.

Écrivons $A = \{a_1, \dots, a_k\}$ avec $a_j \neq 0$ et notons $p_1, \dots, p_\ell$ l'ensemble des facteurs premiers qui apparaissent dans les a_j et t. On décompose alors chaque a_j en facteurs premiers

$$a_j = p_1^{m_{1,j}} \cdots p_\ell^{m_{\ell,j}}$$

avec $m_{i,j} \in \mathbb{Z}$ (il peut y avoir des puissances négatives pour les rationnels). Par commutativité du produit dans $\mathbb{Q}$, on a donc que tout élément du semi-groupe $[\![A]\!]$ (resp. du groupe $(\!|A|\!)$) s'écrit sous la forme

$$a_1^{x_1} \cdots a_k^{x_k} = \prod_{i=1}^{\ell} p_i^{\sum_{j=1}^{k} x_j m_{i,j}} \tag{1}$$

avec $x_1, \dots, x_k \in \mathbb{N}$ (resp. $x_1, \dots, x_k \in \mathbb{Z}$). **Afin d'unifier les notations, on pose $E = \mathbb{N}$ si on regarde le problème d'appartenance à un semi-groupe et $E = \mathbb{Z}$ si on regarde un groupe.** Écrivons de même

$$t = p_1^{y_1} \cdots p_\ell^{y_\ell} \tag{2}$$

avec $y_1, \dots, y_\ell \in \mathbb{Z}$. On introduit la matrice $M_A = (m_{i,j})_{i,j} \in \mathbb{Z}^{\ell \times k}$, ainsi que le vecteur $y_A = (y_j)_j \in \mathbb{Z}^m$.

Question 5.4. *Montrer que (A, t) est une instance positive si et seulement s'il existe $x \in E^k$ tel que $M_A x = y_A$.*

On pourra admettre dans la suite le résultat suivant : il existe un algorithme `NPremiers` qui sur l'entrée $m \in \mathbb{N}$ renvoie les m premiers nombres premiers en temps polynomial en m (la valeur de m, pas sa taille !).

Question 5.5. *Montrer qu'il existe un algorithme qui prend en entrée une matrice $B \in \mathbb{Z}^{\ell \times k}$ et un vecteur $z \in \mathbb{Z}^\ell$ et construit une instance (A, t), **en temps polynomial** en la taille de B et z, telle que*

- *$t \in [\![A]\!]$ si et seulement s'il existe $x \in \mathbb{N}^k$ tel que $Bx = z$,*
- *$t \in (\!|A|\!)$ si et seulement s'il existe $x \in \mathbb{Z}^k$ tel que $Bx = z$.*

Question 5.6. *Montrer que $(\mathbb{Q}, 1)$–`SEMIGROUPE–APPARTENANCE` est* NP*-complet.*

Question 5.7. *On admet[‡] que $\mathbb{Z}$–`SYS-LINEAIRE` est décidable en temps polynomial. Pourquoi la preuve de la question 5.6 ne marche pas pour $(\mathbb{Q}, 1)$–`GROUPE–APPARTENANCE` ? Pourquoi ne peut-on pas déduire de la question 5.4 que $(\mathbb{Q}, 1)$–`GROUPE–APPARTENANCE` est décidable en temps polynomial ?*

‡. Pour les curieux, c'est une conséquence assez immédiate du fait de pouvoir calculer en temps polynomial la forme normale de Smith d'une matrice.

6 Semi-groupes : le cas de la dimension 3

On s'intéresse maintenant au cas des matrices de taille 3×3. Étant donné un ensemble fini $\mathcal{U}$ de paires de mots sur un alphabet Σ (c'est à dire que $\mathcal{U} \subseteq \Sigma^* \times \Sigma^*$), on pose $\mathcal{U}^*$ l'ensemble des paires

$$(u_1 u_2 \cdots u_m, v_1 v_2 \cdots v_m)$$

avec $m \in \mathbb{N}$ et $(u_1, v_1), \ldots, (u_m, v_m) \in \mathcal{U}$. On rappelle/admettra que le problème suivant, dit de la correspondance de Post, est indécidable, même pour un alphabet Σ de taille 2.

PCP :

— **Donnée**: Un ensemble fini $\mathcal{U}$ paires de mots sur un alphabet fini Σ

— **Réponse**: Décider si $\mathcal{U}$ admet une solution : existe-t-il $u \in \Sigma^*$ tel que $(u, u) \in \mathcal{U}^*$?

A titre d'exemple, sur l'alphabet $\Sigma = \{a, b\}$, l'ensemble $\mathcal{U} = \{(a, baa), (ab, aa), (bba, bb)\}$ admet une solution car pour $u = bbaabbba$, $m = 4$, $(u_1, v_1) = (bba, bb)$, $(u_2, v_2) = (ab, aa)$, $(u_3, v_3) = (bba, bb)$ et $(u_4, v_4) = (a, baa)$, on a

$$(u, u) = (bba \cdot ab \cdot bba \cdot a, bb \cdot aa \cdot bb \cdot baa) \in \mathcal{U}^*.$$

A l'inverse, l'ensemble $\mathcal{U} = \{(a, aa)\}$ ne peut pas admettre de solution puisque

$$\mathcal{U}^* = \{(a^n, a^{2n}) : n \geqslant 1\}$$

et il impossible d'avoir $a^n = a^{2n}$ pour $n > 0$.

On fixe $\Gamma = \{1, 2, 3\}$ dans le reste de cet exercice. Pour tout mot $w \in \Gamma^*$, on introduit l'encodage $\langle w \rangle \in \mathbb{Z}$ défini par

$$\langle w \rangle = \sum_{i=1}^{|w|} w_i 4^{i-1}.$$

Intuitivement, $\langle w \rangle$ est l'entier dont l'écriture en base 4 est exactement le mot w.

Question 6.1. *Que vaut $\langle 1 \rangle$? $\langle 23 \rangle$? $\langle 123 \rangle$?*

Question 6.2. *Montrer que pour tous $u, v \in \Sigma^*$, $\langle uv \rangle = \langle u \rangle + 4^{|u|} \langle v \rangle$.*

Question 6.3. *Montrer que $\langle \cdot \rangle$ est injective sur Γ^*.*

Pour toute paire de mots $u, v \in \Sigma^*$, on pose la matrice

$$M(u, v) = \begin{pmatrix} 4^{|u|} & 0 & \langle u \rangle \\ 0 & 4^{|v|} & \langle v \rangle \\ 0 & 0 & 1 \end{pmatrix}.$$

Question 6.4. *Montrer que pour tous $u, v \in \Sigma^*$, $M(u, v)$ est inversible.*

Question 6.5. *Montrer que pour tous $u, v, u', v' \in \Sigma^*$, $M(u, v)M(u', v') = M(uu', vv')$.*

Soit $\mathcal{U}$ un ensemble fini de paires de mots de Γ^*. On pose $\mathcal{M}(\mathcal{U}) = [\![\{M(u, v) : (u, v) \in \mathcal{U}\}]\!]$ le semi-groupe généré par les matrices qui encodent les paires de $\mathcal{U}$.

Question 6.6. *Montrer que $\mathcal{M}(\mathcal{U}) = \{M(u, v) : (u, v) \in \mathcal{U}^*\}$.*

On introduit maintenant les matrices suivantes :

$$S = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Ces matrices ont été choisies pour satisfaire les équations suivantes, pour tout $u, v \in \Gamma^*$,

$$S \cdot M(u,v) \cdot T = (\langle u1\rangle - \langle v\rangle)ST, \qquad S \cdot M(u,v) \cdot S = (4^{|u|} + 4^{|v|})S, \tag{3}$$

$$T \cdot M(u,v) \cdot T = \langle u1\rangle T, \qquad T \cdot M(u,v) \cdot S = 4^{|u|}TS. \tag{4}$$

On ne demande pas de vérifier ces équations.

On pose $\mathcal{S}(\mathcal{U}) = [\![\{S,T\} \cup \{M(u,v) : (u,v) \in \mathcal{U}\}]\!]$ le semi-groupe généré par les mêmes matrices que $\mathcal{M}(\mathcal{U})$, ainsi que S et T.

Question 6.7. *Montrer que tout élément de $\mathcal{S}(\mathcal{U})$ peut s'écrire sous la forme*

$$\alpha_1 \cdots \alpha_k XAY \tag{5}$$

avec $A \in [\![S,T]\!] \cup \{I_3\}$, $X, Y \in \mathcal{M}(\mathcal{U}) \cup \{I_3\}$ et pour tout $i = 1, \ldots, k$,

$$\alpha_i \in \{1, \langle x_i 1\rangle - \langle y_i\rangle, 4^{|x_i|} + 4^{|y_i|}, 4^{|x_i|}, \langle x_i 1\rangle\}$$

pour une certaine paire $(x_i, y_i) \in \mathcal{U}^*$.

On admettra, car il s'agit d'un simple calcul, qu'on a les relations suivantes :

$$S^2 = 2S, \qquad T^2 = T, \qquad STS = S, \qquad TST = T. \tag{6}$$

Question 6.8. *Montrer que $0 \notin [\![S,T]\!]$.*

Question 6.9. *Montrer que le produit (5) est nul alors nécessairement l'un des α_i est nul.*

Question 6.10. *Montrer que si $0 \in \mathcal{S}(\mathcal{U})$ alors existe $(x,y) \in \mathcal{U}^*$ tels que $x1 = y$.*

Question 6.11. *Montrer que s'il existe $(x,y) \in \mathcal{U}^*$ tels que $x1 = y$ alors $0 \in \mathcal{S}(\mathcal{U})$.*

On rappelle que $\Gamma = \{1,2,3\}$ et on pose $\Sigma = \{2,3\}$. Soit $\mathcal{U}$ un ensemble fini de paires de mots **sur Σ**. On pose

$$\tilde{\mathcal{U}} = \mathcal{U} \cup \{(u, v1) : (u,v) \in \mathcal{U}\}$$

qui est un ensemble fini de paires de mots **sur Γ**.

Question 6.12. *Montrer qu'il existe $w \in \Sigma^*$ tel que $(w,w) \in \mathcal{U}^*$ si et seulement s'il existe $x \in \Gamma^*$ tel que $(x, x1) \in \tilde{\mathcal{U}}^*$.*

Question 6.13. *Montrer que $(\mathbb{Z},3)$–`SEMIGROUPE–MORTALITÉ` et $(\mathbb{Z},3)$–`SEMIGROUPE–APPARTENANCE` sont indécidables.*