Nb : Les exercices 1 et 2 seront rédigés sur des feuilles séparées. Par ailleurs, on pourra admettre tout résultat intermédiaire afin de poursuivre la résolution d'un exercice.

Exercice 1 *Systèmes formels*

1.1 *Cadre du problème*

Un système formel est défini comme suit :

- D'abord on définit, par un schéma d'induction, l'ensemble $\mathcal{E}$ des entités bien formées : $\mathcal{E} = \langle \mathcal{B}, \mathcal{R} \rangle$.
- Puis, on définit comme suit, une partie $\mathcal{T} \subset \mathcal{E}$ des entités bien formées, qu'on appelle théorèmes.
  - On commence par définir un ensemble $\mathcal{A} \subset \mathcal{E}$ d'axiomes et on donne un ensemble de règles d'inférence.
  - L'ensemble des théorèmes contient les axiomes ($\mathcal{A} \subset \mathcal{T}$) ainsi que les nouvelles entités, bien formées, obtenues par application de la règle d'inférence aux théorèmes déjà produits.

Nb: Cette approche a été celle, suivie en cours, pour définir le système de déduction ($\mathcal{H}$) de Hilbert.
Les entités bien formées du système ($\mathcal{H}$) sont certaines formules du calcul des propositions et le sous-ensemble des théorèmes est constitué de celles de ces formules qui sont valides.

1.2 *Enoncé du problème*

On se propose d'étudier le système formel suivant.

a) Les entités bien formées sont les mots de l'alphabet $V = \{0, 1, s\}$ contenant une et une seule fois le symbole s.

b) L'ensemble $\mathcal{A}$ des axiomes est défini comme suit :

$$\forall \alpha \in \{0,1\}^*, \quad \alpha 0 s \alpha 1 \in \mathcal{A}$$

où $\{0,1\}^*$ désigne l'ensemble des mots (dont le mot vide) obtenu avec l'alphabet $\{0,1\}$.

c) La seule règle d'inférence est la suivante : Pour tout (α, β) de $(\{0,1\}^*)^2$,

$$\text{si} \quad \alpha s \beta \in \mathcal{T} \quad \text{alors} \quad \alpha 1 s \beta 0 \in \mathcal{T}.$$

1.3 *Travail demandé*

1. Donner une définition inductive $\langle \mathcal{B}, \mathcal{R} \rangle$ de l'ensemble des mots bien formés.
2. *Propriétés du système formel*
   - Prouver la consistance du système formel , c'est-à-dire que tout théorème est un mot bien formé, autrement dit $\mathcal{T} \subset \mathcal{E}$.
   - Prouver aussi que pour tout théorème $\alpha s \beta$ on a $|\alpha| = |\beta|$ où $|\alpha|$, $|\beta|$ désignent la longueur de α et β, respectivement, en nombre de symboles.
3. Examiner les deux mots bien formés suivants : $0111s1000$, $11s00$ et prouver qu'ils sont ou non des théorèmes.

.../...

4. Montrer comment le résultat précédent peut servir à prouver que le système formel n'est pas complet.

   I*ndication*: On montrera qu'il existe des mots bien formés $\alpha s \beta$ avec $|\alpha| = |\beta|$ qui ne sont pas des théorèmes.
5. On a défini les mots bien formés par la phrase : *"Ce sont les mots de l'alphabet* $V = \{0, 1, s\}$ *contenant une et une seule fois le symbole s"*.

   Fournir une phrase semblable qui définisse l'ensemble $\mathcal{T}$ des théorèmes.
6. Donner une définition inductive $\langle \mathcal{B}_A, \mathcal{R}_A \rangle$ pour l'ensemble $\mathcal{A}$ des axiomes, dont la base $\mathcal{B}_A$ soit finie.
7. Question bonus (non obligatoire mais valorisante...)

   Se servir du résultat précédent pour proposer une nouvelle définition du système formel étudié, à l'aide d'un seul axiome et de trois règles d'inférence.

Exercice 2 *Relations binaires*

Nb: On change de feuille !

Soit $E = \{e_1, e_2, e_3\}$ un ensemble de trois éléments distincts.

2.1 On considère la matrice $\mathcal{R}$ de $\mathcal{M}_3(\{0, 1\})$ définie par :

$$\mathcal{R} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

Fournir sous forme ensembliste la relation binaire R interne sur E de matrice associée $\mathcal{R}$.

2.2 *Puissances de* $\mathcal{R}$: exemples

(a) Déterminer la matrice $\mathcal{R}^2$. Quelle relation binaire interne sur E, donnée sous forme ensembliste, représente-t-elle?

(b) Mêmes questions pour $\mathcal{R}^3$ puis $\mathcal{R}^4$.

2.3 *Etude générale des puissances de* $\mathcal{R}$

Les théorèmes d'existence qui vont suivre, proviennent du fait que $\mathbb{N}$ est bien ordonné; propriété évidemment admise ici mais que nous rappelons.

$\mathbb{N}$ est bien ordonné ssi toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

(a) Déterminer le nombre des matrices de $\mathcal{M}_3(\{0, 1\})$.

(b) Soit k et k' des éléments de $\mathbb{N}^*$.

b1) Montrer qu'il existe des k et k' distincts tels que: $\mathcal{R}^k = \mathcal{R}^{k'}$.

b2) On considère l'ensemble P_1 des k de $\mathbb{N}$ vérifiant la propriété (Q_k) suivante:

$$(Q_k): \quad \text{il existe un } \ k' > k \ \text{ tel que } \ \mathcal{R}^k = \mathcal{R}^{k'}.$$

- Déduire de b1) que la partie P_1 de $\mathbb{N}$ est non vide. (Nb: On pourra raisonner par l'absurde.)
- Déduire du bon ordre de $\mathbb{N}$ qu'il existe un plus petit entier naturel non nul k vérifiant (Q_k). On le note désormais k_0.

.../...

(c) Pour cet élément k_0 , désormais d'existence assurée, on considère la partie P_2 des k' de $\mathbb{N}$ vérifiant la propriété (Q_{k_0}), c'est-à-dire:

$$(Q_{k_0}): \quad \text{il existe un } \ k' > k_0 \ \text{ tel que } \ \mathcal{R}^{k_0} = \mathcal{R}^{k'}.$$

- Déduire de b2) que la partie P_2 de $\mathbb{N}$ est non vide.
- En déduire l'existence d'un plus petit k' de $\mathbb{N}$ vérifiant $k' > k_0$ et $\mathcal{R}^{k_0} = \mathcal{R}^{k'}$. On note ce plus petit élément:
  $$k' = k_0 + c \text{ avec } c \text{ (comme cycle...) vérifiant } c \geq 1.$$
- Soit K un élément de $\mathbb{N}^*$ supérieur ou égal à k_0 et tel que $\mathcal{R}^{k_0} = \mathcal{R}^K$. Montrer que $K - k_0$ est un multiple de c.
  Nb: On fera la division de $K - k_0$ par c et on montrera que le reste est nécessairement nul.

(d) Bilan

En utilisant les questions précédentes, montrer que les puissances de $\mathcal{R}$ vérifient les propriétés suivantes:

$$\left\{ \begin{array}{l} \text{Il existe un } k_0 \text{ de } \mathbb{N}^* \text{ tel que: } \mathcal{R}^1, ..., \mathcal{R}^{k_0} \text{ sont distinctes;} \\ \text{au delà de } k_0 \text{ les puissances de } \mathcal{R} \text{ sont cycliques.} \\ \text{La longueur du cycle est } c \text{ vu sous la question (c).} \end{array} \right. .$$

(e) *Applications*

- Déterminer pour la matrice $\mathcal{R}$ donnée, l'entier k_0 ainsi que la longueur du cycle.
- Donner, sans calculs presque..., $\mathcal{R}^{2007}$.

2.4 *Généralisation*

- Les propriétés obtenues pour $\mathcal{R}$ se généralisent-elles ?
- Quelles sont les propriétés cruciales qui fondent votre réponse ?