Chapitre 5 : Décidabilité et classes de complexité

1 Formalisme et outils mathématiques

1.1 Relations et fonctions

Définition 1.1

Une relation $\mathcal{R}$ de $X \times Y$ est dite :
- ***déterministe** dès lors que $\forall(x, y, y') \in X \times Y \times Y, ((x, y) \in \mathcal{R}$ et $(x, y') \in \mathcal{R}) \Rightarrow y = y'$,*
- ***totale à gauche** dès lors que $\forall x \in X, \exists y \in Y, (x, y) \in \mathcal{R}$.*

Définition 1.2

*Étant donnés deux ensembles X et Y, une **fonction partielle** f de X dans Y est une relation déterministe $\mathcal{R} \subseteq X \times Y$. Le **domaine de définition** de f est alors la projection sur X de $\mathcal{R}$, soit dom$(f) = \{x \in X \mid \exists y \in Y, (x, y) \in \mathcal{R}\}$. Pour $x \in$ dom(f), on note $f(x)$ l'unique élément $y \in Y$ tel que $(x, y) \in \mathcal{R}$.*

Définition 1.3

*Étant donnés deux ensembles X et Y, une **fonction totale** f de X dans Y est une relation déterministe et totale à gauche de $X \times Y$.*

Autrement dit, la différence entre une fonction partielle et une fonction totale est qu'une fonction partielle peut n'être pas définie sur tout son ensemble de départ.
Étant donné un ensemble Y tel que $\diamondsuit \notin Y$, on peut compléter[♣] une fonction partielle $f \in X \rightharpoonup Y$ en une fonction totale définie comme suit.

$$\left(\begin{array}{lll} X & \rightarrow Y \cup \{\diamondsuit\} \\ x & \mapsto \begin{cases} f(x) & \text{si } x \in \text{dom}(f) \\ \diamondsuit & \text{sinon} \end{cases} \end{array}\right)$$

Notation 1.4

Soient X et Y deux ensembles. On note alors
- *$X \rightarrow Y$ l'ensemble des fonctions totales de X dans Y ;*
- *$X \rightharpoonup Y$ l'ensemble des fonctions partielles de X dans Y.*

Exercice de cours 1.5

- La relation $\{(n^2, n) \mid n \in \mathbb{Z}\}$ de $\mathbb{Z} \times \mathbb{Z}$ est-elle déterministe ? totale à gauche ? une fonction partielle ? une fonction totale ?
- Mêmes questions pour la relation $\{(n^2, n) \mid n \in \mathbb{Z}\}$ de $\mathbb{N} \times \mathbb{Z}$.
- Mêmes questions pour la relation $\{(n^2, n) \mid n \in \mathbb{N}\}$ de $\mathbb{N} \times \mathbb{N}$.
- Mêmes questions pour la relation $\{(n, n^2) \mid n \in \mathbb{N}\}$ de $\mathbb{N} \times \mathbb{N}$.

♣. à ne pas confondre avec prolonger la fonction, qui reviendrait à ajouter à la relation des couples (x, y) avec $x \notin X$

1.2 Notion de problème

Définition 1.6

*Étant donnés deux ensembles $\mathcal{E}$ et $\mathcal{S}$, on appelle **problème** une relation $\mathcal{R} \subseteq \mathcal{E} \times \mathcal{S}$ totale à gauche, i.e. qui vérifie $\forall e \in \mathcal{E}, \exists s \in \mathcal{S}, (e, s) \in \mathcal{R}$. Les éléments de $\mathcal{E}$ sont appelés les **entrées** (ou **instances**) du problème et ceux de $\mathcal{S}$ sont appelés ses **sorties**.*

Remarque 1.7

- Un problème est donc vu comme l'ensemble des liens entrées/sorties qu'il définit.
- Un problème n'est pas nécessairement une fonction, même partielle. En effet, il peut exister plusieurs sorties associées à une même entrée. En revanche, pour chaque entrée, il faut qu'il existe au moins une sortie associée.

Notation 1.8

Lorsque Q est un problème, on note $\mathcal{E}_Q$ (resp. $\mathcal{S}_Q$) l'ensemble des entrées (resp. celui des sorties) du problème Q.

Exemple 1.9
Considérons par exemple le problème :

$$\textsc{Prime} : \begin{cases} \textbf{Entrée} & : \quad \text{Un entier } n \in \mathbb{N} \\ \textbf{Sortie} & : \quad n \text{ est-il premier ?} \end{cases}$$

Ce problème peut être représenté par l'ensemble de couples : $\{(0, \mathsf{F}), (1, \mathsf{F}), (2, \mathsf{V}), (3, \mathsf{V}), (4, \mathsf{F}), \ldots\} \subseteq \mathbb{N} \times \mathbb{B}$.

Exemple 1.10
Considérons le problème :

$$\textsc{Find}_0 : \begin{cases} \textbf{Entrée} & : \quad n \in \mathbb{N}, T \text{ un tableau de } n \text{ entiers contenant au moins un } 0 \\ \textbf{Sortie} & : \quad \text{Un entier } i \in [\![0, n-1]\!] \text{ tel que } T[i] = 0 \end{cases}$$

Ce problème peut être représenté par l'ensemble de couples suivant.

$$\{((3, \texttt{\{1, 0, 1\}}), 1), ((3, \texttt{\{0, 0, 1\}}), 1), ((4, \texttt{\{0, 0, 0, 1\}}), 0), \ldots\}$$

Exercice de cours 1.11

Les relations suivantes sont-elles des problèmes ? Si oui les reformuler sous la forme **Entrée : ...**, **Sortie : ...**.

- $\{(n, n^2) \mid n \in \mathbb{N}\}$;
- $\{(n^2, n) \mid n \in \mathbb{N}\}$;
- $\{(n^2, n) \mid n \in \mathbb{Z}\}$;
- $\{(n, \mathsf{V}) \mid n \in C\} \cup \{(n, \mathsf{F}) \mid n \in \mathbb{Z} \setminus C\}$, où $C = \{n^2 \mid n \in \mathbb{N}\}$;
- $\{(n^2, n) \mid n \in \mathbb{Z}\}$ comme relation sur $C \times \mathbb{Z}$.

On préfère souvent la représentation d'un problème par la donnée classique des **Entrée/Sortie**.

Représentation des données. Considérons le problème de l'égalité de deux langages réguliers.

$$\textsc{Égalité} : \begin{cases} \textbf{Entrée} & : \quad \text{Deux langages réguliers } L_1 \text{ et } L_2. \\ \textbf{Sortie} & : \quad \text{A-t-on } L_1 = L_2 \text{ ?} \end{cases}$$

Le chapitre automates et langages réguliers nous assure qu'il est possible d'écrire un algorithme permettant de répondre à ce problème. Toutefois il est clair que l'algorithme que nous allons devoir mettre en place dépend fortement de la représentation initiale des deux langages. Sont-ils donnés sous la forme d'expressions régulières ? Sous la forme d'automates déterministes complets ? Sous la forme d'automates avec ε-transitions ? Aussi afin de lever l'ambiguïté de la description **Entrée/Sortie** d'un problème, on précise parfois la représentation choisie pour les entrées/sorties.

Exemple 1.12
Le test de primalité d'un entier peut se décliner en l'un ou l'autre des deux problèmes ci-dessous. Il sera beaucoup plus simple de résoudre $\textsc{Prime}_f$ que $\textsc{Prime}$.

$$\textsc{Prime} : \begin{cases} \textbf{Entrée} & : \text{Un entier } n \in \mathbb{N}, \text{ représenté par la suite de ses bits en base } 2 \\ \textbf{Sortie} & : n \text{ est-il premier ?} \end{cases}$$

$$\textsc{Prime}_f : \begin{cases} \textbf{Entrée} & : \text{Un entier } n \in \mathbb{N}, \text{ représenté par sa décomposition en facteurs premiers} \\ \textbf{Sortie} & : n \text{ est-il premier ?} \end{cases}$$

Dans la suite, lorsque ce n'est pas précisé les entiers manipulés par les problèmes sont représentés en binaire. Ce sont donc des mots sur l'alphabet $\{0, 1\}$.
On distingue dans la suite deux types de problèmes particuliers : les problèmes de décisions, qui sont au cœur de ce chapitre, et les problèmes d'optimisation. Ces derniers, déjà rencontrés pour les schémas algorithmiques qu'ils appellent à mettre en place, ne sont pas directement l'objet de ce chapitre, mais on montre qu'ils sont naturellement associés à des problèmes de décision.

1.3 Problème de décision

Définition 1.13

*On appelle **problème de décision** un problème $\mathcal{R} \subseteq \mathcal{E} \times \mathbb{B}$ tel que $\forall e \in \mathcal{E}, \exists! s \in \mathbb{B}, (e, s) \in \mathcal{R}$. Un tel problème peut donc être vu comme une fonction totale de $\mathcal{E}$ dans $\mathbb{B}$.*
*On appelle alors **instances positives** (resp. **instances négatives**) les entrées pour lesquelles la sortie est V (resp. F).*

Notation 1.14

Lorsque Q est un problème de décision, on note Q^+ (respectivement Q^-) l'ensemble de ses instances positives (respectivement négatives). On dit de Q que c'est un problème trivial dès lors que $Q^+ = \emptyset$ ou $Q^- = \emptyset$.

Exemple 1.15
Pour $L \subseteq \Sigma^\star$, $\textsc{appartient}_L : \begin{cases} \textbf{Entrée :} \ w \in \Sigma^\star \\ \textbf{Sortie :} \ \text{A-t-on } w \in L\,? \end{cases}$ est un problème de décision, et $\textsc{appartient}_L^+ = L$, $\textsc{appartient}_L^- = L^c$.

Définition 1.16

*Soit Q un problème de décision. Le **co-problème** associé à Q, ou **problème complémentaire**, est le problème de décision sur $\mathcal{E}_Q$ défini par $Co - Q \overset{\text{déf}}{=} \{(e, \overline{s}) \mid (e, s) \in Q\}$.*

Remarque 1.17

Informellement, le co-problème pose la question "inverse" du problème initial. Cela revient à intervertir le rôle des réponses V et F. On note donc que le co-problème du co-problème est le problème initial.

Exemple 1.18
Le problème de savoir si un entier est composé, *i.e.* le problème $\textsc{Composé}$ est le co-problème de $\textsc{prime}$.
Pour $L \subseteq \Sigma^\star$, le co-problème de $\textsc{appartient}_L$ est $\textsc{appartient}_{L^c}$.

1.4 Problème d'optimisation

Définition 1.19

> *Soit $Q \subseteq \mathcal{E} \times \mathbb{R}$ un problème dont les sorties sont des réels.*
> *S'il existe, pour toute entrée $e \in \mathcal{E}$, un ensemble $\mathsf{sol}(e)$, et une fonction $c_e \in \mathsf{sol}(e) \to \mathbb{R}$ tels que $\min\{c_e(s) \mid s \in \mathsf{sol}(e)\}$ est bien défini et est la seule valeur associée à e selon Q, alors on dit que Q est un **problème de minimisation**.*
>
> *En remplaçant $\min$ par $\max$ on obtient la définition d'un **problème de maximisation**.*
> *Dans les deux cas, on parle de **problème d'optimisation***

Cette définition, donnée sous forme d'existence, peut recouvrir tous les problèmes de décision. Cependant, on retiendra qu'un problème d'optimisation est un problème qui définit, pour chaque entrée e, un maximum ou un minimum à calculer, et ce en fixant l'**ensemble des solutions** $\mathsf{sol}(e)$ et la **fonction objectif** c_e. On appelle alors **valeur optimale** pour l'entrée e la valeur $\mathrm{opt}\{c_e(s) \mid s \in \mathsf{sol}(e)\}$ (pour $\mathrm{opt} = \min$ ou $\mathrm{opt} = \max$ selon les cas), et **solution optimale** pour l'entrée e toute solution $s \in \mathsf{sol}(e)$ telle que $c_e(s)$ est la valeur optimale.

Remarque 1.20

> On appelle aussi problème d'optimisation le problème associant à chaque entrée e, non pas la valeur optimale, mais toutes les solutions optimales.

Définition 1.21

> *Le **problème de décision associé** à un problème d'optimisation Q_O est obtenu en ajoutant aux entrées de Q une valeur de seuil et en demandant s'il est possible ou non, de trouver une solution dont la valeur est meilleure que le seuil.*
>
> *Problème de minimisation Q_O*
> $$\begin{cases} \textbf{\textit{Entrée}} & : \quad e \in \mathcal{E}_Q \\ \textbf{\textit{Sortie}} & : \quad \min\limits_{s \in \mathsf{sol}(e)} c_e(s) \end{cases}$$
> *Problème de décision associé Q*
> $$\begin{cases} \textbf{\textit{Entrée}} & : \quad e \in \mathcal{E}_Q,\ K \in \mathbb{N} \\ \textbf{\textit{Sortie}} & : \quad \textit{Existe-t-il } s \in \mathsf{sol}(e) \textit{ tel que } c_e(s) \leqslant K \textit{ ?} \end{cases}$$
>
> *Problème de maximisation Q_O*
> $$\begin{cases} \textbf{\textit{Entrée}} & : \quad e \in \mathcal{E}_Q \\ \textbf{\textit{Sortie}} & : \quad \max\limits_{s \in \mathsf{sol}(e)} c_e(s) \end{cases}$$
> *Problème de décision associé Q*
> $$\begin{cases} \textbf{\textit{Entrée}} & : \quad e \in \mathcal{E}_Q,\ K \in \mathbb{N} \\ \textbf{\textit{Sortie}} & : \quad \textit{Existe-t-il } s \in \mathsf{sol}(e) \textit{ tel que } c_e(s) \geqslant K \textit{ ?} \end{cases}$$

Exemple 1.22
Dans le cas du problème du plus court chemin dans un graphe connexe, le problème de décision associé au problème d'optimisation présenté plus haut est le problème suivant.

$$\begin{cases} \textbf{Entrée} & : \quad \text{Un graphe orienté pondéré } G = (S, A, c), \text{ deux sommets } s \text{ et } t \text{ de } S, \text{ un seuil } K \in \mathbb{N} \\ \textbf{Sortie} & : \quad \text{Existe-t-il un chemin de } s \text{ à } t \text{ dans } G \text{ de longueur} \leqslant K\text{ ?} \end{cases}$$

Exercice de cours 1.23

> On considère le problème du rendu de monnaie suivant : étant donnés un entier $n \in \mathbb{N}^\star$, une famille de pièces $(p_1, p_2, \ldots, p_n) \in \mathbb{N}^n$ tels que $p_1 = 1$, et un montant M à rendre, on cherche à trouver un rendu de monnaie pour le montant M, utilisant le moins de pièces possible. Par exemple pour le système monétaire $(1, 2, 5)$ il est possible de rendre le montant $M = 6$ au moyen de $2 + 2 + 2$ ou $5 + 1$, cette deuxième solution étant préférée. Formaliser le problème du rendu de monnaie comme un problème d'optimisation. Donner le problème de décision associé. Justifier que ces problèmes sont bien définis.