# Informatique théorique III
# Série 1 solution

Prof. Nestmann, 2004

## 1. Ensemble des parties

Écrivez les ensembles suivants.
- $\mathcal{P}(\{1, 2\})$
- $\mathcal{P}(\mathcal{P}(\{1, 2\}))$ □

**Solution.** ■

## 2. Relations et fonctions

Soit $A$ et $B$ deux ensembles quelconques. Montrez qu'il existe une bijection entre
$\mathcal{P}(A \times B)$, l'ensemble des relations sur $A \times B$ et
$A \to \mathcal{P}(B)$, l'ensemble des applications de $A$ dans $\mathcal{P}(B)$.

Procédez de la manière suivante.

1. Commencez d'abord par vous représenter ces deux ensembles.
2. Définissez ensuite une application $\phi : \mathcal{P}(A \times B) \to (A \to \mathcal{P}(B))$ qui associe une fonction à chaque relation. Indice : prenez une relation et essayez de construire une fonction qui « représente » la relation sans perte d'information.
3. Démontrez que $\phi$ est effectivement bijective.

□

**Preuve.** Définissons $\phi$ comme suit,

$$\begin{aligned} \phi : \mathcal{P}(A \times B) &\to (A \to \mathcal{P}(B)) \\ R &\mapsto \begin{pmatrix} f_R : A \to \mathcal{P}(B) \\ \qquad x \mapsto \{y \mid xRy\} \end{pmatrix} \end{aligned}$$

A chaque relation $R$, $\phi$ associe une fonction $f_R$. Pour un $x$ donné, la fonction $f_R$ associe l'ensemble des éléments en relation avec $x$ dans $R$. Intuitivement, on voit bien qu'il est possible, à partir de la fonction, de déterminer si $(a, b) \in R$, il suffit de vérifier que $b \in f_R(a)$.

Montrons que $\phi$ est bijective. Par déf. nous devons montrer qu'elle est injective et surjective.

1. $\phi$ est injective. Par déf. nous devons montrer que

   $$\forall R, R' \in \mathcal{P}(A \times B) : \phi(R) = \phi(R') \Rightarrow R = R'$$

   Prenons $R$ et $R'$ quelconques (pour pouvoir généraliser) et supposons$^{(*)}$ que $\phi(R) = \phi(R')$. Cela signifie, par déf. de $\phi$, que $f_R = f_{R'}$.

   Nous devons montrer que $R = R'$. Par l'absurde supposons$^{(**)}$ que $R \neq R'$.

   Ceci signifie, par déf. de l'égalité des ensembles, qu'il existe un couple $(x, y)$ tel que $(x, y) \in R$ et $(x, y) \notin R'$ (ou vice-versa). Dès lors les ensembles $\{z \mid xRz\}$ et $\{z \mid xR'z\}$ ne peuvent pas être égaux et nous avons $f_R(x) \neq f_{R'}(x)$ et donc par déf. de l'égalité des fonctions $f_R \neq f_{R'}$ ce qui contredit $(*)$.

   L'hypothèse $(**)$ est donc erronée et nous avons $R = R'$ et donc $f$ est injective.

2. $\phi$ est surjective. Par déf. nous devons montrer que

$$\forall f \in A \to B : \exists R \in \mathcal{P}(A \times B) : \phi(R) = f$$

Prenons $f$ une application quelconque (pour pouvoir généraliser). Construisons l'ensemble suivant,

$$R \triangleq \{(a, b) \in A \times B \mid b \in f(a)\}$$

par définition nous avons $R \in \mathcal{P}(A \times B)$ et

$$\begin{aligned}\phi(R) &= \begin{pmatrix} f_R : A \to \mathcal{P}(B) \\ x \mapsto \{y \mid xRy\} \end{pmatrix} \overset{\text{(déf. de } R)}{=} \begin{pmatrix} f_R : A \to \mathcal{P}(B) \\ x \mapsto \{y \mid y \in f(x)\} \end{pmatrix} \\ &= \begin{pmatrix} f_R : A \to \mathcal{P}(B) \\ x \mapsto f(x) \end{pmatrix} = f\end{aligned}$$

Pour toute application $f$ nous pouvons donc construire une relation $R \in \mathcal{P}(A \times B)$, telle que $\phi(R) = f$. $\phi$ est donc injective.

De (1) et (2) nous déduisons que $\phi$ est bijective. ■

## 3. Mot miroir

Soit $\Sigma$ un alphabet. Pour $w \in \Sigma^*$, le mot miroir $\overline{w}$ de $w$ est défini par,

$$\overline{\epsilon} \triangleq \epsilon \qquad (\mathrm{M}_1)$$

$$\overline{a \cdot w} \triangleq \overline{w} \cdot a \qquad (\mathrm{M}_2)$$

On admet, sans le démontrer, que $\forall w \in \Sigma^*, |w| = |\overline{w}|$.

1. Montrez que $\forall u, v \in \Sigma^* : \overline{u \cdot v} = \overline{v} \cdot \overline{u}$
2. En déduire que $\forall w \in \Sigma^* : \overline{\overline{w}} = w$
3. En utilisant $(1)$ donnez la forme des mots $w$ tels que $\overline{w} = w$.

□

**Preuve.** Remarquons d'abord que $\forall a \in \Sigma : \overline{a} = a$.

1. Soit $P$ le prédicat sur les mots défini par :

$$P(u) \triangleq \forall v \in \Sigma^* : \overline{u \cdot v} = \overline{v} \cdot \overline{u}$$

On montre que $\forall u \in \Sigma^* : P(u)$ par induction structurelle sur $u$.

(a) Cas de base : il s'agit de montrer que $P(\epsilon)$ est vrai.
Soit $v \in \Sigma^*$.
On a

$$\begin{aligned}\overline{\epsilon \cdot v} &= \overline{v} && \text{car } \epsilon \cdot v = v \\ &= \overline{v} \cdot \epsilon && \text{car } \overline{v} = \overline{v} \cdot \epsilon \\ &= \overline{v} \cdot \overline{\epsilon} && \text{par définition de } \overline{\epsilon}\end{aligned}$$

Le mot $v$ étant quelconque, on a montré $\forall v \in \Sigma^* : \overline{\epsilon \cdot v} = \overline{v} \cdot \overline{\epsilon}$, c'est-à-dire $P(\epsilon)$.

(b) Cas inductif. Soit $u \in \Sigma^*$ tel que $P(u)$ soit vrai. Soit $a \in \Sigma$. Montrons alors que $P(a \cdot u)$ est vrai.
Soit $v \in \Sigma^*$.
On a

$$\begin{aligned}
\overline{(a \cdot u) \cdot v} &= \overline{a \cdot (u \cdot v)} && \text{car } \cdot \text{ est associative} \\
&= \overline{u \cdot v} \cdot a && \text{par définition de } \overline{a \cdot (u \cdot v)} \\
&= (\overline{v} \cdot \overline{u}) \cdot a && \text{car } P(u) \text{ est vrai} \\
&= \overline{v} \cdot (\overline{u} \cdot a) && \text{car } \cdot \text{ est associative} \\
&= \overline{v} \cdot \overline{a \cdot u} && \text{par définition de } \overline{a \cdot u}
\end{aligned}$$

On a donc montré $P(a \cdot u)$.

On conclut par théorème d'induction de 1a et 1b que $\forall u \in \Sigma^* : P(u)$ ce qui est le résultat demandé.

2. Soit $P$ le prédicat sur les mots défini par :

$$P(u) \triangleq \overline{\overline{u}} = u$$

On montre par induction structurelle sur $u$ que $\forall u \in \Sigma^* : P(u)$.

(a) Cas de base : on veut montrer $P(\epsilon)$.
On a

$$\begin{aligned}
\overline{(\overline{\epsilon})} &= \overline{\epsilon} && \text{par définition de } \overline{\epsilon} \\
&= \epsilon && \text{par définition de } \overline{\epsilon}
\end{aligned}$$

D'où $P(\epsilon)$.

(b) Cas inductif. Soit $u \in \Sigma^*$ et supposons $P(u)$. Soit $a \in \Sigma$ et montrons que $P(a \cdot u)$.
On a

$$\begin{aligned}
\overline{\overline{a \cdot u}} &= \overline{\overline{u} \cdot a} && \text{par définition de } \overline{a \cdot u} \\
&= \overline{a} \cdot \overline{\overline{u}} && \text{d'après 1} \\
&= a \cdot u && \text{car } \overline{a} = a \text{ et } P(u)
\end{aligned}$$

D'où $P(a \cdot u)$.

On conclut par théorème d'induction de 2a et 2b que $\forall u \in \Sigma^* : P(u)$ ce qui est le résultat demandé.

3. Soit $P \triangleq \{u \cdot \overline{u} \mid u \in \Sigma^*\} \cup \{u \cdot a \cdot \overline{u} \mid u \in \Sigma^* \wedge a \in \Sigma\}$ et $Q \triangleq \{u \in \Sigma^* \mid \overline{u} = u\}$.
On veut montrer que $P = Q$, $Q$ étant l'ensemble des *palindromes* de $\Sigma^*$.

(a) Montrons que $P \subseteq Q$.
Soit $w \in P$.
– Premier cas : $w = u \cdot \overline{u}$ pour un certain $u \in \Sigma^*$.
Alors

$$\begin{aligned}
\overline{w} &= \overline{u \cdot \overline{u}} \\
&= \overline{\overline{u}} \cdot \overline{u} && \text{par (1)} \\
&= u \cdot \overline{u} && \text{par (2)} \\
&= w
\end{aligned}$$

– Second cas : $w = u \cdot a \cdot \overline{u}$ pour un certain $u \in \Sigma^*$ et $a \in \Sigma$.
Alors

$$\begin{aligned}
\overline{w} &= \overline{u \cdot (a \cdot \overline{u})} && \\
&= \overline{a \cdot \overline{u}} \cdot \overline{u} && \text{par (1)} \\
&= (\overline{\overline{u}} \cdot \overline{a}) \cdot \overline{u} && \text{par (1)} \\
&= (u \cdot a) \cdot \overline{u} && \text{par (2) et car } \overline{a} = a \\
&= w
\end{aligned}$$

Dans les deux cas, on a montré $\overline{w} = w$ donc $w \in Q$. On en conclut que $P \subseteq Q$.

(b) Montrons que $Q \subseteq P$.
Soit $w \in Q$. On raisonne par cas sur la parité de la longueur de $w$ :
– $|w|$ est paire (ceci inclut le cas du mot vide).
Il existe alors $u, v \in \Sigma^*$ tels que $w = u \cdot v$ et $|u| = |v|$.
Comme $w \in Q$, on a $\overline{w} = \overline{u \cdot v} = \overline{v} \cdot \overline{u} = w = u \cdot v$.
Comme $|u| = |v| = |\overline{v}|$, on en déduit que $\overline{v} = u$ et donc que $v = \overline{\overline{v}} = \overline{u}$.
Ainsi $w = u \cdot v = u \cdot \overline{u}$ et $w \in P$.
– $|w|$ est impaire.
Il existe alors $u, v \in \Sigma^*, a \in \Sigma$ tels que $w = u \cdot a \cdot v$ et $|u| = |v|$.
Comme $w \in Q$, on a $\overline{w} = \overline{v} \cdot a \cdot \overline{u} = w = u \cdot a \cdot v$.
Comme $|u| = |v| = |\overline{v}|$, on en déduit que $\overline{v} = u$ et donc que $v = \overline{\overline{v}} = \overline{u}$.
Ainsi $w = u \cdot a \cdot \overline{u}$ et $w \in P$.
Dans les deux cas, on a montré que $w \in P$. On en conclut que $Q \subseteq P$.

De 3a et 3b, on déduit que $P = Q$.

■