Exercice 2.1. Soient X, Y et Z des ensembles. Soient $f\colon X \to Y$ et $g\colon Y \to Z$ des applications. On rappelle que $g \circ f$ est une application de X dans Z et est définie par $g \circ f(x) = g(f(x))$ pour tout $x \in X$. Prouver ou trouver un contre-exemple pour les faits suivants :

1. Si $g \circ f$ est surjective, alors f est surjective.
2. Si $g \circ f$ est surjective, alors g est surjective.
3. Si $g \circ f$ est injective, alors f est injective.
4. Si $g \circ f$ est injective, alors g est injective.

Exercice 2.2. Le but de cet exercice est de montrer que l'ensemble $\mathcal{P}_f(\mathbb{N})$ de toutes les parties finies de $\mathbb{N}$ est dénombrable.

1. Soit $n \in \mathbb{N}$. Montrer que l'ensemble des parties de $\mathbb{N}$ qui contiennent exactement n éléments est dénombrable.
2. Construire maintenant une injection de $\mathcal{P}_f(\mathbb{N})$ dans $\mathbb{N} \times \mathbb{N}$ et en déduire que $\mathcal{P}_f(\mathbb{N})$ est dénombrable.
3. Donner l'idée d'une autre preuve basée sur la représentation binaire d'un nombre entier.

Exercice 2.3. Soient x, y et z des variables booléennes.

1. Donner la table de vérité de $x \Leftrightarrow y$.
2. Montrer que $(x \Rightarrow y) \Leftrightarrow (\neg y \Rightarrow \neg x)$ est une tautologie (c'est le principe de contraposition).
3. Montrer que $(x \Rightarrow (y \Rightarrow z)) \Leftrightarrow ((x \wedge y) \Rightarrow z))$ est une tautologie.
4. $((x \wedge y) \Rightarrow z)) \Rightarrow ((x \vee y) \Rightarrow z))$ est-elle une tautologie ?

Exercice 2.4. Soit $f(x_1, \ldots, x_n) = x_1 \oplus \cdots \oplus x_n$. Montrer que $f(x_1, \ldots, x_n) = 0$ ssi un nombre pair des x_i vaut 1.

Exercice 2.5. Soit $f \in \mathcal{H}_4 \to \mathcal{H}_1$ une fonction booléenne qui vaut 1 uniquement sur les quadruplets qui contiennent exactement deux 1. Par exemple, $f(1,0,1,0) = 1$ alors que $f(0,1,1,1) = f(1,0,0,0) = 0$.

(a) Trouver une forme DNF pour f.

(b) Trouver une forme CNF pour f.

(c) Trouver une forme polynomiale pour f.

Correction.

Exercice 2.1. (a) - (d) Soient $f\colon \mathbb{N} \to \mathbb{Z}$ l'application donnée par $f(x) = x$ et $g\colon \mathbb{Z} \to \mathbb{N}$ donnée par $g(x) := |x|$. Alors $g \circ f$ est l'application identité sur $\mathbb{N}$: si $z \in \mathbb{N}$, alors $(g \circ f)(z) = g(f(z)) = g(z) = |z| = z$. Donc $g \circ f$ est injective et surjective. Mais f n'est pas surjective et g n'est pas injective. Donc les deux assertions (a) et (d) sont fausses.

(b) Supposons que $g \circ f$ est surjective et montrons que g l'est aussi. Soit $z \in Z$, montrons qu'il existe un $y \in Y$ tel que $g(y) = z$. A cette fin, utilisons la surjectivité de $g \circ f$ pour trouver un $x \in X$ tel que $(g \circ f)(x) = z$. Posons $y = f(x)$. Alors $g(y) = g(f(x)) = z$. Donc g est bien surjective.

(c) Supposons que $g \circ f$ est injective et montrons que f est injective. Nous allons démontrer la contraposée, c'est-à-dire l'assertion « f n'est pas injective implique que $g \circ f$ n'est pas injective ». Soient x et x' dans X tels que $f(x) = f(x')$. Alors, $(g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x')$. Donc $g \circ f$ n'est pas injective, cqfd.

Exercice 2.2. 1. Notons $\binom{\mathbb{N}}{n}$ l'ensemble des parties de $\mathbb{N}$ à n éléments. On définit une application $\iota_n\colon \binom{\mathbb{N}}{n} \to \mathbb{N}^n$ comme suit. Soit S un sous-ensemble de $\mathbb{N}$ avec n éléments. Sans perte de généralité, on peut supposer que S s'écrit $S = \{a_1, \ldots, a_n\}$ où $a_1 < a_2 < \cdots < a_n$. On pose $\iota_n(S) = (a_1, \ldots, a_n)$. Cette application ι_n est bien une injection. En effet, si $\iota_n(S) = \iota_n(S')$, alors S et S' sont formés des mêmes éléments donc sont égaux.

D'après le théorème 1.14(d) on sait que le produit $A \times B$ de deux ensembles A et B dénombrables est dénombrable. Mais alors $\mathbb{N} \times \mathbb{N}$ est dénombrable et par récurrence, $\mathbb{N}^n = \mathbb{N}^{n-1} \times \mathbb{N}$ est aussi dénombrable. Soit $f : \mathbb{N}^n \to \mathbb{N}$ une fonction de comptage de $\mathbb{N}^n$. Alors $g_n := f \circ \iota_n\colon \binom{\mathbb{N}}{n} \to \mathbb{N}$ est une fonction de comptage de $\binom{\mathbb{N}}{n}$.

2. Soit g_n une fonction de comptage de $\binom{\mathbb{N}}{n}$ comme construit par exemple à la question précédente. Construisons à présent l'injection $\varphi\colon A \to \mathbb{N} \times \mathbb{N}$ comme suit : si S est un ensemble fini de $\mathbb{N}$ avec t éléments, alors $\varphi(S) = (t, g_t(S))$. Cette application est injective : supposons en effet que S et T soient deux sous-ensembles différents de $\mathbb{N}$. Si S et T comptent un nombre différent d'éléments, alors $\varphi(S)$ et $\varphi(T)$ diffèrent en leur première coordonnée et sont donc différents. S'ils ont le même cardinal n, alors $g_n(S)$ et $g_n(T)$ diffèrent puisque g_n est une fonction de comptage de $\binom{\mathbb{N}}{n}$ et donc $\varphi(S)$ et $\varphi(T)$ sont différents.

   On sait que $\mathbb{N} \times \mathbb{N}$ est équipotent à $\mathbb{N}$, donc A est aussi dénombrable.

3. On peut construire directement une injection χ de A vers $\mathbb{N}$ en posant $\chi(S) = \sum_{s \in S} 2^s$. Comme S est fini, la somme en question est bien définie. L'application χ est en fait la fonction caractéristique de S si on lit $\chi(S)$ comme un nombre écrit en notation binaire. Comme la représentation binaire d'un entier est unique, cette application est bien une injection (et même une bijection).

Exercice 2.3. 1. On a $(x \Leftrightarrow y) = (x \Rightarrow y) \wedge (y \Rightarrow x)$. Donc

x	y	$x \Rightarrow y$	$y \Rightarrow x$	$x \Leftrightarrow y$
0	0	1	1	**1**
0	1	1	0	**0**
1	0	0	1	**0**
1	1	1	1	**1**

,

si bien que $(x \Leftrightarrow y) = \neg(x \oplus y)$.

2. On a

x	y	$x \Rightarrow y$	$\neg y \Rightarrow \neg x$	$(x \Rightarrow y) \Leftrightarrow (\neg y \Rightarrow \neg x)$
0	0	1	1	**1**
0	1	1	1	**1**
1	0	0	0	**1**
1	1	1	1	**1**

,

ce qui prouve l'assertion.

3. De la table de vérité de $x \Rightarrow y$ on trouve que la représentation polynomiale de $x \Rightarrow y$ est $1+x+xy$. D'où, la représentation polynomiale de $(x \Rightarrow (y \Rightarrow z))$ est celle de $x \Rightarrow (1+y+yz)$ qui est $1+x+x(1+y+yz) = 1 + xy + xyz$. D'autre part, la représentation polynomiale de $((x \wedge y) \Rightarrow z)$ est $1 + xy + xyz$, ce qui est la même chose que celle de $(x \Rightarrow (y \Rightarrow z))$. D'où l'assertion.

4. Ceci n'est pas une tautologie. Supposons que $x = z = 0$, $y = 1$. Alors $(x \wedge y) \Rightarrow z$ vaut « $0 \Rightarrow 0$ » ce qui vaut 1. De plus, $(x \vee y) \Rightarrow z$ s'évalue en « $1 \Rightarrow 0$ » qui vaut 0. Mais $1 \Rightarrow 0$ vaut 0 et non 1. Donc la formule n'est pas une tautologie.

Exercice 2.4. On raisonne par récurrence sur n. Si $= 1$, alors $f(x_1) = x_1$ est vaut 0 ssi $x_1 = 0$, c'est-à-dire ssi un nombre pair (à savoir 0) de x_i vaut 1. Soit à présent un entier $n \geq 2$. Soit $(g_1, \ldots, x_{n-1}) = x_1 \oplus \cdots \oplus x_{n-1}$, de telle sorte que $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_{n-1}) \oplus x_n$. En utilisant la table de vérité de $\oplus$ de la section 2.4.3, on voit que $f(x_1, \ldots, x_n) = 0$ ssi ou bien $g(x_1, \ldots, x_{n-1}) = x_n = 0$, ou bien $g(x_1, \ldots, x_{n-1}) = x_n = 1$. D'après l'hypothèse de récurrence, $g(x_1, \ldots, x_{n-1}) = 0$ ssi un nombre pair de x_i vaut 1. Aussi, dans le premier cas, un nombre pair de x_i parmi les $x_1, \ldots, x_{n-1}$ vaut 1 et $x_n = 0$, si bien qu'un nombre pair de x_i parmi $x_1, \ldots, x_n$ vaut 1. Dans le second cas, un nombre impair de x_i parmi les $x_1, \ldots, x_{n-1}$ vaut 1 et $x_n = 1$, donc encore une fois un nombre pair de x_i parmi les $x_1, \ldots, x_n$ vaut 1.

Exercice 2.5. (a) On a

$$\begin{aligned} f^{-1}(0) &= \{(0,0,0,0),(0,0,0,1),(0,0,1,0),(0,1,0,0),(0,1,1,1) \\ &\quad (1,0,0,0),(1,0,1,1),(1,1,0,1),(1,1,1,0),(1,1,1,1)\}. \end{aligned}$$

Aussi, on obtient la clause CNF suivante pour f :

$$\begin{aligned} f(x_1,x_2,x_3,x_4) &= (x_1 \vee x_2 \vee x_3 \vee x_4) \wedge (x_1 \vee x_2 \vee x_3 \vee \neg x_4) \wedge (x_1 \vee x_2 \vee \neg x_3 \vee x_4) \wedge \\ &\quad (x_1 \vee \neg x_2 \vee x_3 \vee x_4) \wedge (x_1 \vee \neg x_2 \vee \neg x_3 \vee \neg x_4) \wedge \\ &\quad (\neg x_1 \vee x_2 \vee x_3 \vee x_4) \wedge (\neg x_1 \vee x_2 \vee \neg x_3 \vee \neg x_4) \wedge \\ &\quad (\neg x_1 \vee \neg x_2 \vee x_3 \vee \neg x_4) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_3 \vee x_4) \wedge \\ &\quad (\neg x_1 \vee \neg x_2 \vee \neg x_3 \vee \neg x_4). \end{aligned}$$

(b) On a

$$\begin{aligned} f^{-1}(1) &= \{(1,1,0,0),(1,0,1,0),(1,0,0,1) \\ &= \quad (0,1,1,0),(0,1,0,1),(0,0,1,1)\}. \end{aligned}$$

Aussi, on obtient la clause DNF suivante pour f :

$$\begin{aligned} f(x_1,x_2,x_3,x_4) &= (x_1 \wedge x_2 \wedge \neg x_3 \wedge \neg x_4) \vee (x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4) \vee \\ &\quad (x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge x_4) \vee (\neg x_1 \wedge x_2 \wedge x_3 \wedge \neg x_4) \vee \\ &\quad (\neg x_1 \wedge x_2 \wedge \neg x_3 \wedge x_4) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3 \wedge x_4). \end{aligned}$$

(c) On remarque que f est invariant par permutation des variables. Ceci nous suggère de chercher une solution invariante sous le groupe des permutations. Nous allons chercher à exprimer f en fonction des polynômes symétriques élémentaires. Notons w le nombre de coordonnées non-nulle de x. On a alors le tableau de valeurs suivant :

$p \ \backslash \ w$	0	1	2	3	4
$\epsilon_0 = 1$	1	1	1	1	1
$\epsilon_1 = \sum_{1 \leq i \leq 4} x_i$	0	1	0	1	0
$\epsilon_2 = \sum_{1 \leq i < j \leq 4} x_i x_j$	0	0	1	1	0
$\epsilon_3 = \sum_{i \leq i < j < k \leq 4} x_i x_j x_k$	0	0	0	1	0
$\epsilon_4 = x_1 x_2 x_3 x_4$	0	0	0	0	1
f	0	0	1	0	0

On remarque que $f = \epsilon_2 + \epsilon_3$.
La réponse est donc

$$\begin{aligned} f(x_1,x_2,x_3,x_4) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 + \\ &\quad x_1x_2x_3 + x_1x_2x_4 + x_2x_3x_4 + x_1x_3x_4, \end{aligned}$$