le cnam

Algèbre de Boole, probabilités et arithmétique

Cours 11 Treillis de Boole

- Treillis

On rappelle qu'un treillis est la donnée d'un ensemble fini non vide E et d'une relation d'ordre notée $\leq$ sur E telle que pour tout couple (x,y) d'éléments de E, la borne inférieure $\inf(x,y) = x \wedge y$ et la borne supérieure $\sup(x,y) = x \vee y$ existent bien et ce sont des éléments de l'ensemble E. Ceci signifie d'une part que pour tout $(x,y) \in E \times E$, l'intersection de l'ensemble des minorants de x avec l'ensemble des minorants de y a un plus grand élément $x \wedge y$ et on a $x \wedge y \leq x$ et $y \wedge y \leq x$. D'autre part, l'intersection de l'ensemble des majorants de x avec l'ensemble des majorants de y a un plus petit élément $x \vee y$ et $x \leq x \vee y$ et $y \leq x \vee y$. Un treillis se note $(E, \wedge, \vee, \leq)$.

Un treillis a toujours un plus petit élément, noté 0 ou $\perp$ ainsi qu'un plus grand élément, noté 1 ou $\top$. On a également les propriétés de commutativité : $x \wedge y = y \wedge x$, $x \vee y = y \vee x$, d'associativité : $x \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge y \wedge z$, $x \vee (y \vee z) = (x \vee y) \vee z = x \vee y \vee z$ et d'idempotence : $x \wedge x = x$, $x \vee x = x$.

Si X est un ensemble fini, l'ensemble $\mathscr{P}(X)$ muni de l'inclusion devient le treillis $(\mathscr{P}(X), \cap, \cup, \subset)$. La figure 1 l'illustre si $X = \{a,b\}$ et $X = \{a,b,c\}$.

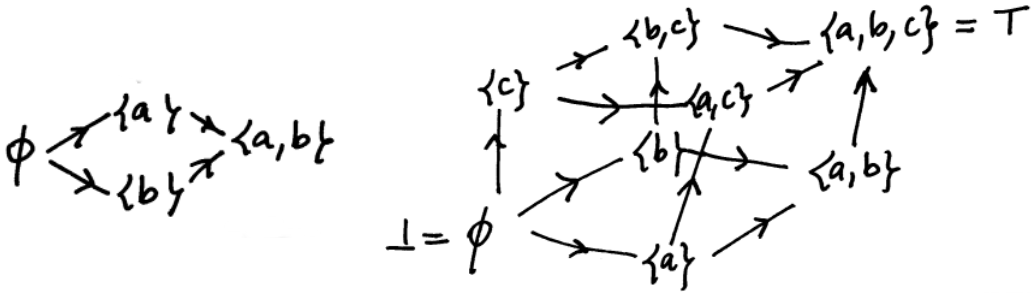

Figure 1. Treillis $(\mathscr{P}(X), \cap, \cup, \subset)$ de l'ensemble des parties pour $X = \{a,b\}$ et $X = \{a,b,c\}$.

Un autre exemple est donné par l'ensemble $D(n)$ des diviseurs de l'entier $n \geq 1$ et la relation d'ordre est la relation "divise". On a alors $x \wedge y =$ pgcd (x,y) et $x \vee y =$ ppcm (x,y).

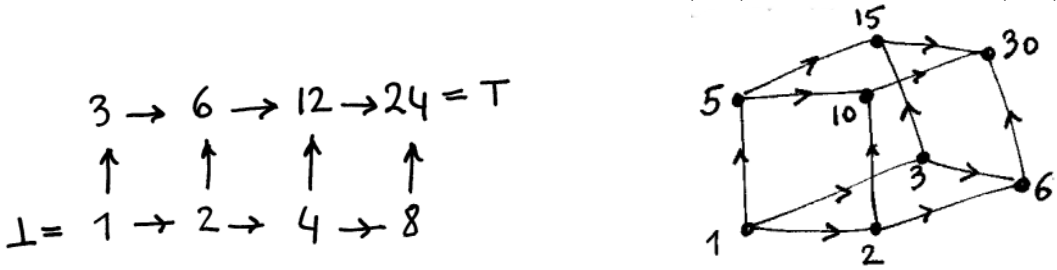

Figure 2. Treillis $(D(n), \wedge, \vee, |)$ de l'ensemble des diviseurs de $n = 24$ et $n = 30$.

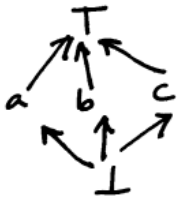

Figure 3. Un treillis qui ne vérifie pas une des propriétés de distributivité

Un treillis n'est pas forcément distributif. L'exemple de la figure 3 ci-dessus l'illustre puisque $a \wedge (b \vee c) = a \wedge \top = a$ et $a \wedge b = a \wedge c = \bot$ donc $a = a \wedge (b \vee c) \neq (a \wedge b) \vee (a \wedge c) = \bot$.

Le complément d'un élément $x \in E$ est un élément $x' \in E$ qui satisfait aux relations $x \wedge x' = \bot$ et $x \vee x' = \top$.

Dans le treillis $(\mathscr{P}(X), \cap, \cup, \subset)$, une partie $A \subset X$ admet pour complément A' sa partie complémentaire : $A' = \complement_X A = X \backslash A = A^c$. On bien en effet $A \cap A^c = \varnothing$ et $A \cup A^c = X$. Observons que cette propriété du complément peut être en défaut. Dans le treillis $D(24)$ par exemple (voir la figure 2, à gauche), on peut se rendre compte rapidement que le nombre 6 n'a pas de compément pour la relation de divisibilité.

- Treillis de Boole

Par définition, un treillis de Boole $(E, \wedge, \vee, ', \leq, \bot, \top)$ est un treillis $(E, \wedge, \vee, \leq)$ qui est de plus doublement distributif et pour lequel tout élément x admet un complément x'. Nous le nommons de cette façon en hommage à George Boole, mathématicien britannique (1815-1864). On a donc $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ et $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ pour tout triplet $(x, y, z) \in E \times E \times E$ et pour tout $x \in E$, il existe un complément $x' \in E$ de sorte que $x \wedge x' = \bot$ et $x \vee x' = \top$.

Par exemple, le treillis $(\mathscr{P}(X), \cap, \cup, \subset)$ de l'ensemble des parties d'un ensemble fini X est un treillis de Boole.

Observons que dans un treillis de Boole, le complément est unique. C'est une conséquence de la définition du complément et surtout de la distributivité.

Dans un treillis de Boole, les lois de De Morgan sont satisfaites. On a $(x \wedge y)' = x' \vee y'$: le complément de la borne inférieure est égal à la borne supérieure des compléments. De plus, on a $(x \vee y)' = x' \wedge y'$: le complément de la borne supérieure est égal à la borne inférieure des compléments. Compte tenu de l'unicité du complément, il suffit de vérifier d'une part que $x' \vee y'$ a toutes les propriétés du complément de $x \wedge y$, c'est à dire $(x' \vee y') \wedge (x \wedge y) = \bot$ et $(x' \vee y') \vee (x \wedge y) = \top$ et d'autre part que $x' \wedge y'$ a les propriétés qui caractérisent le complément de $x \vee y$, c'est à dire $(x' \wedge y') \wedge (x \vee y) = \bot$ et $(x' \wedge y') \vee (x \vee y) = \top$.

Nous avons nommé la structure $(E, \wedge, \vee, ', \leq, \bot, \top)$ "treillis de Boole", afin de bien la distinguer de l'"algèbre de Boole" $(E, \wedge, \vee, ', \bot, \top)$ où l'on abandonne la référence à une relation d'ordre pour ne garder que les trois opérations de borne inférieure, borne supérieure et complémentation. À notre connaissance, ce point de vue a été développé pour la première fois en 1921 par Emil Post (1897-1954). Nous aurions peut-être dû intituler ce chapitre "Treillis de Post".

- Bits

L'ensemble $\mathbb{B}$ des bits est défini par $\mathbb{B} = \{0, 1\}$ ou $\mathbb{B} = \{\bot, \top\}$. Il est muni de l'ordre naturel induit par la relation $0 \leq 1$. C'est un treillis de Boole noté $(\mathbb{B}, \wedge, \vee, \neg, \leq, 0, 1)$. On a bien

entendu les relations suivantes : $0 \wedge 0 = 0$, $0 \wedge 1 = 1 \wedge 0 = 0$, $1 \wedge 1 = 1$, $0 \vee 0 = 0$, $0 \vee 1 = 1 \vee 0 = 1$, $1 \vee 1 = 1$, $\overline{0} = 1$ et $\overline{1} = 0$.

- Vecteurs booléens

On se donne un entier $n \geq 1$. L'ensemble des vecteurs formés de n bits définit l'ensemble $\mathbb{B}^n$. Il est constitué des n-uplets $x = (x_1, x_2, \ldots, x_j, \ldots, x_n)$ tels que pour tout entier j compris entre 1 et n, on a $x_j \in \mathbb{B}$, c'est à dire $x_j = 0$ ou $x_j = 1$. Si $y = (y_1, y_2, \ldots, y_j, \ldots, y_n)$ est un autre vecteur de $\mathbb{B}^n$, on définit la relation $x \leq y$ par la condition $x_j \leq y_j$ pour tout entier j tel que $1 \leq j \leq n$. On peut montrer sans difficulté que $\leq$ est une relation d'ordre dans $\mathbb{B}^n$ et que les opérations de borne inférieure $x \wedge y$ et de borne supérieure $x \vee y$ sont définis pour les vecteurs de bits. Notons que l'on a $(x_1, x_2, \ldots, x_j, \ldots, x_n) \wedge (y_1, y_2, \ldots, y_j, \ldots, y_n) = (x_1 \wedge y_1, x_2 \wedge y_2, \ldots, x_j \wedge y_j, \ldots, x_n \wedge y_n)$ et $(x_1, x_2, \ldots, x_j, \ldots, x_n) \vee (y_1, y_2, \ldots, y_j, \ldots, y_n) = (x_1 \vee y_1, x_2 \vee y_2, \ldots, x_j \vee y_j, \ldots, x_n \vee y_n)$. La preuve est proposée en exercice.
Nous allons montrer que $\mathbb{B}^n$ est un treillis "isomorphe" au treillis des parties $\mathscr{P}(X)$ d'un ensemble fini X comportant n éléments. Cette propriété permettra d'établir que $\mathbb{B}^n$ permet de définir un treillis de Boole.

- Treillis isomorphes

On se donne deux treillis $(X, \wedge, \vee, \leq)$ et $(Y, \wedge, \vee, \leq)$. Une application bijective f de X sur Y est un isomorphisme de treillis si et seulement si elle respecte les bornes inférieures et les bornes supérieures : pour tout couple $(x, y) \in X \times X$, $f(x \wedge y) = f(x) \wedge f(y)$ et $f(x \vee y) = f(x) \vee f(y)$. On peut alors démontrer (voir les exercices !) qu'alors l'application f respecte les relations d'ordre : si $x \leq y$, alors $f(x) \leq f(y)$ pour tout $(x, y) \in X \times X$. L'isomorphisme f respecte aussi les plus petits et les plus grands éléments : $f(\bot) = \bot$ et $f(\top) = \top$.
Si X est un treillis de Boole, alors $Y = f(X)$ est également un treillis de Boole et on peut alors démontrer que f respecte la complémentation : $f(x') = (f(x))'$ pour tout $x \in X$.

- Isomorphisme de l'ensemble des parties d'un ensemble sur les vecteurs de bits

On se donne un entier naturel $n \geq 1$ et un ensemble X composé de n éléments distincts. Son cardinal est égal à n, c'est à dire $|X| = n$. Nous choisissons de numéroter les éléments de cet ensemble : $X = \{x_1, x_2, \ldots, x_j, \ldots, x_n\}$. Nous construisons un isomorphisme f de $\mathscr{P}(X)$ sur $\mathbb{B}^n$ de la façon suivante : pour toute partie $A \subset X$, on pose $f(A) = (b_1, b_2, \ldots, b_j \ldots, b_n)$ et les n bits $b_1, b_2, \ldots, b_j \ldots, b_n$ sont choisis de sorte que $b_j = 1$ si et seulement si $x_j \in A$, c'est à dire $b_j = 0$ si et seulement si $x_j \notin A$.
Si l'ensemble X contient au moins deux éléments, on a par exemple $f(\{x_1, x_2\}) = (1, 1, 0, \ldots, 0)$. Avec l'application f, on "code" une partie $A \subset X$ avec un $n-$uplet de bits, une suite de n valeurs égales à zéro ou un. Alors $f(A \cap B) = f(A) \wedge f(B)$ et $f(A \cup B) = f(A) \vee f(B)$. De plus, $f(A^c) = \overline{f(A)} = (\overline{b_1}, \overline{b_2}, \ldots, \overline{b_j} \ldots, \overline{b_n})$.

- "Atomes" d'un treillis de Boole

On se donne un treillis de Boole $(E, \wedge, \vee, ', \leq, \bot, \top)$. Les successeurs immédiats du plus petit élément $\bot$ sont appelés les atomes du treillis de Boole. L'élément $a \in E$ est un atome si et seulement si d'une part $\bot \leq a$ et d'autre part $(\bot \leq x \leq a) \Rightarrow \big((x = \bot) \text{ ou } (x = a)\big)$

- Théorème de Stone

Marsall Stone (1903-1989) a établi les propriétés suivantes qui disent en résumé que les treillis de Boole ne peuvent pas êre différents des exemples déjà vus plus haut dans cette leçon. En effet, le théorème de Stone énonce que le nombre d'éléments d'un treillis de Boole fini est une puissance de 2, que pour tout entier $n \geq 1$, il existe un treillis de Boole de cardinal 2^n et que tous les treillis de Boole avec 2^n éléments sont isomorphes. Un treillis de Boole avec 2^n éléments a exactement n atomes. Il est isomorphe à $\mathbb{B}^n$ et son diagramme de Hasse est un $n-$cube.

- $n-$cube

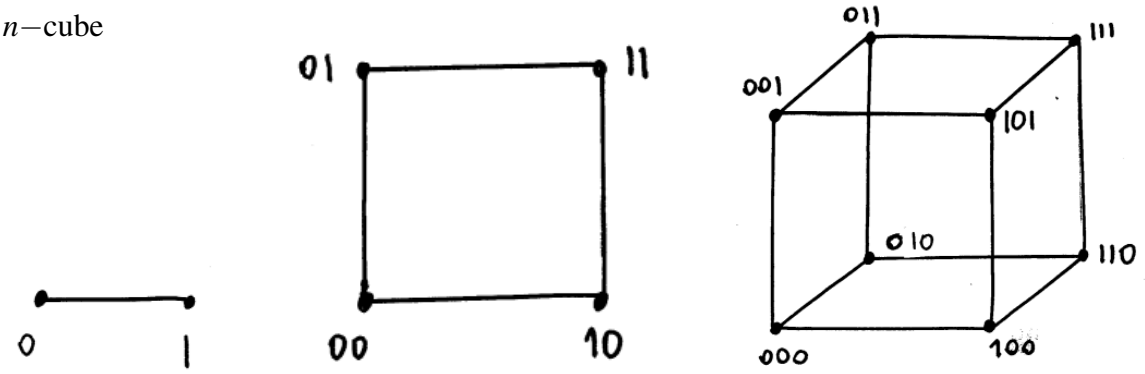

Figure 4. Les diagrammes de Hasse des treillis de Boole $\mathbb{B}$, $\mathbb{B}^2$ et $\mathbb{B}^3$ constituent les cubes booléens de dimension 1, 2 et 3 : un segment, un carré et un cube ordinaire en dimension trois.

Le diagramme de Hasse de l'ensemble $\mathbb{B}^n$ des vecteurs de n bits est un hypercube de dimension n, un "$n-$cube". Nous l'avons représenté aux figures 4 et 5 pour les valeurs de l'entier n entre 1 et 4.

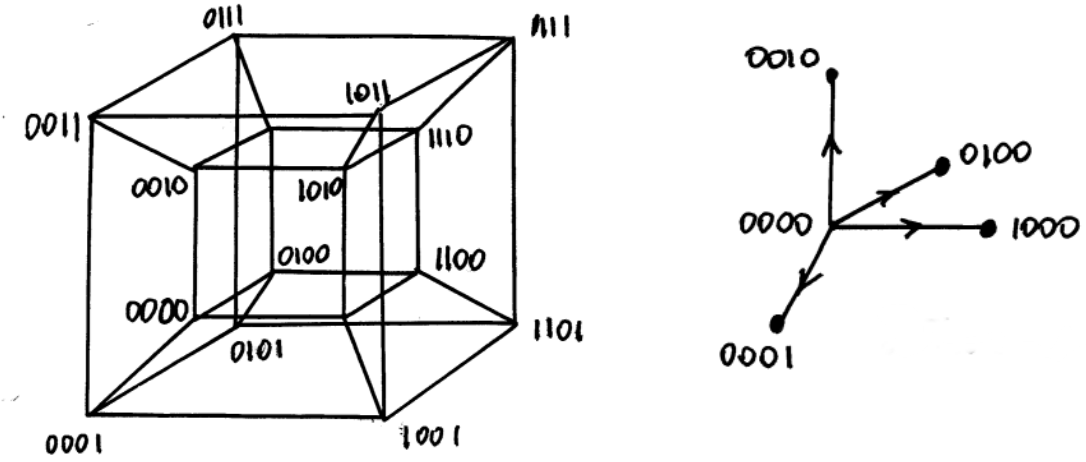

Figure 5. Représentation du "4-cube" (à gauche) et de ses "atomes" (à droite), les vecteurs "les plus proches" de l'origine.

- Addition

On se donne un treillis de Boole $(E, \wedge, \vee, \bar{\ }, \leq, \bot, \top)$. On peut définir une nouvelle loi de composition, l'addition, à partir des trois lois de borne inférieure, borne supérieure et complément déjà existantes. Par définition, $x+y = (x \vee y) \wedge (\bar{x} \vee \bar{y}) = (x \wedge \bar{y}) \vee (\bar{x} \wedge y)$. La somme $x+y$ correspond à la conjonction logique du "ou exclusif".

Un premier exemple est donné par l'ensemble $\mathbb{B} = \{0, 1\}$ des bits. Rappelons que $\overline{0} = 1$ et $\overline{1} = 0$. On peut établir avec un calcul simple la table d'addition suivante :
$0+0=1,\ 1+0=0+1=1$ et surtout $1+1=0$.
Un second exemple est donné dans l'ensemble des parties d'un ensemble. On a dans ce cas $A+B=(A\cap B^{\mathrm{c}})\cup(A^{\mathrm{c}}\cap B)$. L'ensemble $A+B$ se note de façon classique $A\Delta B$ et s'appelle la "différence symétrique". Il est illustré à la figure 6. On a aussi $A\Delta B=(A\cup B)\backslash(A\cap B)$.

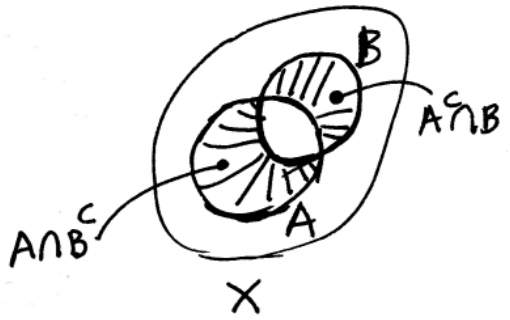

Figure 6. "Différence symétrique" $A\Delta B=(A\cap B^{\mathrm{c}})\cup(A^{\mathrm{c}}\cap B)$ entre les ensembles A et B.

- Structure de groupe commutatif pour l'addition

Muni de l'addition définie par $x+y=(x\wedge y)\vee(\overline{x}\wedge\overline{y})$, l'ensemble E qui nous a permis de définir un treillis de Boole a une structure de groupe commutatif. L'addition est commutative, associative, possède un élément neutre et tout élément de E possède un opposé.
La commutativité $x+y=y+x$ est une conséquence directe de la commutatiité des opérateurs $\wedge$ et $\vee$. L'associativité $x+(y+z)=(x+y)+z$ demande un calcul assez long qui est laissé au lecteur à titre d'exercice. Le plus petit élément est élément neutre : $x+\bot=\bot+x=x$ et on peut écrire $0=\bot$. Enfin l'existence de l'opposé est la plus étonnante puisque $x+x=\bot$. L'opposé de $x\in E$ est l'élément x lui-même ! On a $-x=x$; on dit qu'on fait des calculs "en caractéristique deux".

- Multiplication

On note simplement $x.y$ ou $xy=x\wedge y$ la borne inférieure. Cette notation multiplicative se justifie par les propriétés suivantes :
la multiplication est associative : on a $x(yz)=(xy)z$ pour tous les éléments x, y et z de E,
la multiplication est commutative : $xy=yx$,
la multiplication admet un élément unité : $1=\top$ puisque $x\wedge\top=\top\wedge x=x$,
la multiplication est distributive par rapport à l'addition : $x(y+z)=(xy)+(xz)$. Seule cette dernière propriété demande quelques lignes de calcul pour la démonstration.

- Anneau de Boole

Muni de l'addition et de la multiplication définies dans les paragraphes précédents, l'ensemble E qui a permis de définir la structure de treillis a une nouvelle structure. On lui donne un nouveau nom ; on pose $A=E$ et le triplet $(A,+,.)$ est un anneau commutatif unitaire. Cette dénomination signifie qu'il a toutes les propriétés listées ci-dessus. D'une part, l'addition est commutative, associative, possède un élément neutre et tout élément de E possède un opposé.

D'autre part, la multiplication est associative, commutative, admet un élément unité et elle est distributive par rapport à l'addition.
Dans le cas de l'ensemble $\mathbb{B}$ des bits, l'anneau correspondant utilise la notation $\mathbb{F}_2$ et l'anneau $(\mathbb{F}_2, +, .)$ est même un corps commutatif. En effet, tout élément non nul admet un inverse puisqu'on a simplement $1 \times 1 = 1$.
Un "anneau de Boole" est caractérisé par l'idempotence de la multiplication :
$\forall x \in E,\ xx = x$. Cette propriété n'est qu'une reformulation de la relation $x \wedge x = x$. Un anneau avec unité $(A, +, .)$ tel que $x.x = x$ pour tout $x \in A$ est par définition un anneau de Boole. Nous retenons que dans un anné de Boole, tout élément est égal à son carré.
On a alors les propriétés suivantes : tout élément est égal à son opposé et l'anneau est commutatif. La première propriété s'obtient en élevant $x+x$ au carré : $(x+x)(x+x) = x+x$. La seconde propriété est une conséquence du calcul de $x+y$ au carré puisque $(x+y)(x+y) = x+y$.

Nous terminons par une remarque importante concernant les notations. Dans beaucoup d'ouvrages d'informatique ou d'électronique, la borne supérieure $x \vee y$ est notée $x+y$. Ceci peut prêter à confusion, car ces deux lois sont différentes ; on a vu que $1 \vee 1 = 1$ dans un treillis de Boole alors que $1+1=0$ dans un anneau de Boole.

- Reconstruction d'un treillis de Boole à partir d'un anneau de Boole

On se donne dans ce paragraphe un anneau unitaire commutatif $(A, +, .)$ qui est un anneau de Boole : on a $xx = x$ pour tout $x \in A$. Peut-on toujours reconstruire un treillis de Boole $(E, \wedge, \vee, \ ^-, \leq, 0, 1)$ avec $E = A$? La difficulté est de définir la relation d'ordre $\leq$, la borne inférieure $\wedge$, la borne supérieure $\vee$ et le complément $^-$.
L'exercice est loin d'être immédiat. Toutefois, il suffit de poser $x \leq y$ si et seulement si $x = xy$. On peut démontrer qu'alors $x \wedge y = xy$, $x \vee y = x+y+xy$ et $\overline{x} = 1+x$. La borne supérieure est à rapprocher de la relation $A \cup B = (A \Delta B) \Delta (A \cap B)$ valable dans l'ensemble des parties d'un ensemble X (voir la figure 6). Le complément prend dans ce cas la forme $\overline{A} = X \Delta A = A^c$.

Exercices

- Quelques calculs dans un treillis

On se donne un treillis $(E, \wedge, \vee, \leq)$.
a) Une condition d'égalité. Montrer que si on a l'égalité $x \wedge y = x \vee y$, alors $x = y$.
b) Montrer que pour tout $x \in E$, on a $x \wedge (x \vee y) = x$.
c) Défaut de distributivité ; montrer que $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$ pour tout triplet $(x, y, z) \in E \times E \times E$.
c) Second défaut de distributivité ; montrer que $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$ pour tout triplet $(x, y, z) \in E \times E \times E$.

- Isomorphismes de treillis

On se donne deux treillis $(X, \wedge, \vee, \leq)$ et $(Y, \wedge, \vee, \leq)$ et une application bijective f de X sur Y telle que pour tout couple $(x, y) \in X \times X$, $f(x \wedge y) = f(x) \wedge f(y)$ et $f(x \vee y) = f(x) \vee f(y)$. On dit que f est un isomorphisme de treillis.

a) Montrer qu'alors l'application f respecte les relations d'ordre : si $x \leq y$, alors $f(x) \leq f(y)$ pour tout $(x, y) \in X \times X$.
b) Montrer que $f(\bot) = \bot$ et $f(\top) = \top$.
c) Montrer que si X est un treillis de Boole, alors $Y = f(X)$ est également un treillis de Boole et qu'en particulier, l'isomorphisme f respecte la complémentation : $f(x') = (f(x))'$ pour tout $x \in X$.

- Ordre dans l'ensemble des vecteurs booléens

On rappelle que $\mathbb{B}^n$ est l'ensemble des vecteurs $x = (x_1, x_2, \ldots, x_j, \ldots, x_n)$ tels que pour tout entier j compris entre 1 et n, on a $x_j \in \mathbb{B}$, c'est à dire $x_j = 0$ ou $x_j = 1$. Si $y = (y_1, y_2, \ldots, y_j, \ldots, y_n)$ est un autre vecteur de $\mathbb{B}^n$, la relation $x \leq y$ est définie par la condition $x_j \leq y_j$ pour tout entier j tel que $1 \leq j \leq n$.
a) Montrer que le vecteur $x \wedge y$ a pour composante numéro j le bit $x_j \wedge y_j$: $(x \wedge y)_j = x_j \wedge y_j$.
b) Même question pour la borne supérieure : montrer que $(x \vee y)_j = x_j \vee y_j$.

- Cas d'un ordre total

On suppose que la relation $\leq$ définit un ordre total dans l'ensemble non vide E.
a) Montrer que les bornes inférieure $x \wedge y$ et supérieure $x \vee y$ de deux éléments quelconques x et y de E sont toujours bien définis.
b) Montrer qu'on a bien les relations de distributivité entre ces deux opérations :
$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ et $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ pour tout triplet $(x, y, z) \in E \times E \times E$.

- Distributivité du pgcd relativement au ppcm et du ppcm relativement au pgcd.

Cet exercice suppose connu le résultat de l'exercice précédent dans le cas de la relation $\leq$ entre nombres entiers naturels. On se donne deux entiers naturels x et y que l'on écrit sous la forme d'un produit de facteurs premiers : $x = \Pi_{j=1}^{K} p_j^{\alpha_j}$ et $y = \Pi_{j=1}^{K} p_j^{\beta_j}$, avec $\alpha_j \in \mathbb{N}$ et $\beta_j \in \mathbb{N}$. On rappelle que le pgcd et le ppcm sont respectivement la borne inférieure $\wedge$ et la borne supérieure $\vee$ pour la relation "divise" dans l'ensemble $\mathbb{N}$ des nombres entiers : $x \wedge y = \text{pgcd}\,(x, y)$ et $x \vee y = \text{ppcm}\,(x, y)$.
a) Montrer que $x \wedge y = \Pi_{j=1}^{K} p_j^{\alpha_j \wedge \beta_j}$ et $x \vee y = \Pi_{j=1}^{K} p_j^{\alpha_j \vee \beta_j}$.
b) Démontrer la double distributivité des opérations ppcm et ppcm pour un triplet (x, y, z) quelconque d'entiers naturels supérieurs ou égaux à 1 : $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ et $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

- Structure de treillis de Boole pour l'ensemble des diviseurs d'un entier

Cet exercice suppose connus les résultats de l'exercice précédent. On se donne un nombre entier $n = \Pi_{j=1}^{K} p_j$, produit de nombres premiers distincts. On appelle $D(n)$ l'ensemble de ses diviseurs. On rappelle que muni de la relation "divise", $(D(n), \wedge, \vee, |)$ est un treillis.
a) Montrer que $(D(n), \wedge, \vee, ', |, 1, n)$ est un treillis de Boole. Préciser en particulier la valeur du complément m' d'un nombre arbitraire $m \in D(n)$.
b) Pourquoi $D(24)$ n'est pas un treillis de Boole ?