

Résolution de problèmes logiques par le calcul

Michel LAFOND, Lycée Le Castel à Dijon

- Voici deux problèmes qu'on classe habituellement dans les problèmes de "logique" :

PB-1 On retire d'une population les gros méchants, les gentils maigres, les grands gentils, les petits maigres, et les gentils petits gros. Qui reste ?

PB-2 Lors d'une enquête, trois suspects A, B, C sont interrogés. A dit que "B ment". B dit que "C ment". C dit que "A ou B ment". Qui ment ?

On peut parfaitement résoudre ces deux problèmes en raisonnant sans outil spécial, autre que les cellules grises, et ces deux exercices sont laissés au lecteur.

Mais il est intéressant de mettre au point une méthode (algèbre) qui permette la mise en équation et la résolution systématique (algorithmique) par le calcul dans cette algèbre.

C'est ce qu'a fait Monsieur George Boole vers 1850 en procédant à peu près ainsi :

- Première étape : définition des variables du problème.

On commence par définir après analyse du problème, une ou plusieurs "variables binaires" qui, comme leur nom ne l'indique pas, sont des fonctions qui, à chaque individu du problème, associent **deux** "valeurs logiques" ou "états logiques". Ces valeurs logiques, selon la nature du problème, seront par exemple :

"GROS ou MAIGRE" pour un individu du problème 1 ;

"DIT LA VÉRITÉ ou MENT" pour un individu du problème 2 ;

"PASSE ou NE PASSE PAS" pour le courant électrique d'une entrée ou une sortie de porte logique dans un ordinateur.

Etc.

Il est essentiel que les variables soient binaires, c'est-à-dire qu'elles ne puissent prendre que deux états.

Ainsi, la variable prenant pour un élève donné dans une matière donnée l'une des "valeurs logiques" MÉDIOCRE, MOYEN, BON ne pourrait pas, telle qu'elle, participer au calcul.

Dans PB-1 trois variables binaires notées a , b , c sont nécessaires dans un premier temps :

Elles sont définies ainsi :

$a(x) = 1$ si l'individu x est gros,
 $a(x) = 0$ si l'individu x est maigre,

$b(x) = 1$ si l'individu x est grand,
 $b(x) = 0$ si l'individu x est petit,

$c(x) = 1$ si l'individu x est gentil,
 $c(x) = 0$ si l'individu x est méchant.

L'algèbre de Boole qu'on va définir sera donc assez grossière, puisqu'on y est soit gros soit maigre, soit grand soit petit, soit gentil soit méchant !

Comme c'est l'usage, les "valeurs logiques" quelles qu'elles soient, seront codées 1 et 0, ce qui est commode pour le calcul futur, mais évidemment dangereux car on risque d'interpréter malgré soi ces symboles comme des nombres.

Comme dans toute nouvelle théorie, une des premières choses qu'on fait c'est des abus de notation !

Allons-y : On notera dans la suite pour un individu x donné, s'il n'y a pas ambiguïté :

$a = 1$ pour $a(x) = 1$ si l'individu x est gros,
 $a = 0$ pour $a(x) = 0$ si l'individu x est maigre,

et de même pour toutes les autres variables.

Remarque : le fait d'avoir choisi "1" pour le code de "gros" et "0" pour le code de "maigre" est arbitraire. On aurait aussi bien pu choisir le contraire.

Cette première étape est la plus facile.

- Deuxième étape : la mise en équation.

Cette étape va nécessiter de disposer d'autant d'opérations booléennes que d'"opérations logiques".

Toute la logique élémentaire (la nôtre !) peut être écrite avec les trois opérations (appelées aussi connecteurs) NON, ET, OU.

Par exemple : si A, B désignent des propositions logiques (caractérisées par leur valeur logique vrai ou faux, indépendamment de leur contenu), ces opérations sont :

La <u>négation</u> :	A	→	NON (A)
La <u>conjonction</u> :	(A ; B)	→	A ET B
La <u>disjonction</u> :	(A ; B)	→	A OU B

Pour les autres connecteurs, il suffit de combiner les 3 connecteurs précédents :

Ainsi :

- Pour exprimer "A mais pas B" on écrira : A ET (NON B)
- Pour exprimer "A ou bien B" on écrira :
(A ET (NON B)) OU (B ET (NON A)) [On reconnaît le OU exclusif]
- Pour exprimer "ni A ni B" on écrira : (NON A) ET (NON B)

Le plus difficile est l'implication logique :

- Pour exprimer "A implique B" on écrira : B OU (NON A)

En effet : "A implique B" est vraie (par définition) sauf si (A est vraie et B fausse).

Donc : "A implique B" est vraie sauf si (A ET (NON B)) est vraie,

"A implique B" est vraie si et seulement si (A ET (NON B)) est fausse,

"A implique B" est vraie si et seulement si NON(A ET (NON B)) est vraie,

"A implique B" est vraie si et seulement si NON(A) OU B est vraie.

On a utilisé au passage les théorèmes logiques :

NON (NON X) équivaut* à X

NON (X ET Y) équivaut à (NON X) OU (NON Y)

qu'on démontrera plus tard par le calcul, en algèbre booléenne.

* [L'équivalence logique entre deux propositions, dont il est question plus haut, signifie simplement que ces propositions sont toutes deux vraies ou toutes deux fausses]

Voici les trois opérations booléennes correspondantes aux trois connecteurs précités :

A chaque variable booléenne a on définit sa complémentaire notée $\bar{a}$ par :

$$\bar{a} = 1 \Leftrightarrow a = 0 \text{ autrement dit } \text{NON } (a = 1)$$

A chaque couple de variables booléennes a, b on définit :

Leur produit p noté $p = a \cdot b$ défini par $a \cdot b = 1 \Leftrightarrow a = 1 \text{ ET } b = 1$

Leur somme s notée $s = a + b$ définie par $a + b = 1 \Leftrightarrow a = 1 \text{ OU } b = 1$

Le but de George Boole est presque atteint : toute affirmation d'un individu donné faisant intervenir un nombre fini de variables logiques pourra se traduire par une équation du type $E(a, b, c, \dots) = 1$ où $a, b, c, \dots$ sont les variables logiques intervenant dans l'affirmation, et E une expression composée de ces variables (éventuellement complémentées) et des opérations " ." ; "+" précédemment définies.

Ainsi : dans le problème 1, l'affirmation : " x est un méchant gros" qui signifie " x est méchant ET x est gros" se traduira par : " $c = 0 \text{ ET } a = 1$ " puis par " $\bar{c} = 1 \text{ ET } a = 1$ " et enfin par $\bar{c} \cdot a = 1$

En accord avec les définitions précédentes des opérations booléennes.

L'habitude est de définir les trois opérations booléennes par leur table de vérité, dans lesquelles ne figurent par économie, que les codes 0 ou 1 :

Voici la table de vérité de la complémentation traduisant la définition :

a	$\bar{a}$
0	1
1	0

$$\bar{a} = 1 \Leftrightarrow \text{NON } (a = 1)$$

Voici les tables de vérité des opérations produit et somme traduisant leur définition :

a	b	$a \cdot b$	$a + b$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1

$$a \cdot b = 1 \Leftrightarrow a = 1 \text{ ET } b = 1$$

$$a + b = 1 \Leftrightarrow a = 1 \text{ OU } b = 1$$

Si le produit booléen n'a rien de choquant puisque parfaitement identique au produit numérique dans le sous-ensemble de $\mathbb{R} : \{0 ; 1\}$, il n'en est pas de même pour la somme booléenne puisque " $1 + 1 = 1$ ".

Quand on enseigne ceci aux élèves (BTS informatique par exemple) c'est un peu difficile au début, mais on s'y fait vite.

Ce sont ces tables de vérité qui servent à câbler les portes logiques des ordinateurs, leur permettant de traiter la totalité de leurs tâches.

La deuxième étape est presque terminée, il reste à préciser ce qu'on entend par "égalité de deux variables booléennes u et v ". Rien de plus naturel, et on n'a pas le choix ! :

On dit que deux variables booléennes u et v sont égales si elles ont la même table de vérité, ou ce qui revient au même : si pour tout individu x : $u(x) = v(x)$

Effectuons la mise en équation du problème 1 :

Puisque la question était : Qui reste après avoir retiré les "gros méchants" ... ?, il nous faut une quatrième variable disons r pour coder les individus retirés. On pose donc :

$$r = 1 \quad \Leftrightarrow \quad x \text{ est retiré de la population } [r = 0 \text{ sinon}].$$

On a alors :

$$r = 1 \quad \Leftrightarrow \quad x \text{ est retiré} \quad \Leftrightarrow \quad (x \text{ est gros ET } x \text{ est méchant}) \text{ OU } (x \text{ est gentil ET } x \text{ est maigre}) \text{ OU } (x \text{ est grand ET } x \text{ est gentil}) \text{ OU } (x \text{ est petit ET } x \text{ est maigre}) \text{ OU } (x \text{ est gentil ET } x \text{ est petit ET } x \text{ est gros}).$$

Pour obtenir l'équation, la seule précaution à prendre est de tout coder avec "1" quitte à utiliser la complémentation, après quoi, il suffit de remplacer ET par "." et OU par "+". Enfin :

$$\begin{aligned} r = 1 & \quad \Leftrightarrow \quad x \text{ est retiré} \\ \Leftrightarrow & \quad (a = 1 \text{ ET } c = 0) \text{ OU } (c = 1 \text{ ET } a = 0) \text{ OU } (b = 1 \text{ ET } c = 1) \text{ OU } (b = 0 \text{ ET } a = 0) \\ & \quad \text{OU } (c = 0 \text{ ET } b = 0 \text{ ET } a = 1) \\ \Leftrightarrow & \quad (a = 1 \text{ ET } \bar{c} = 1) \text{ OU } (c = 1 \text{ ET } \bar{a} = 1) \text{ OU } (b = 1 \text{ ET } c = 1) \text{ OU } (\bar{b} = 1 \text{ ET } \bar{a} = 1) \\ & \quad \text{OU } (\bar{c} = 1 \text{ ET } \bar{b} = 1 \text{ ET } a = 1) \\ \Leftrightarrow & \quad (a \cdot \bar{c} = 1) \text{ OU } (c \cdot \bar{a} = 1) \text{ OU } (b \cdot c = 1) \text{ OU } (\bar{b} \cdot \bar{a} = 1) \text{ OU } (\bar{c} \cdot \bar{b} \cdot a = 1) \\ \Leftrightarrow & \quad a \cdot \bar{c} + c \cdot \bar{a} + b \cdot c + \bar{b} \cdot \bar{a} + \bar{c} \cdot \bar{b} \cdot a = 1 \end{aligned}$$

La suppression des parenthèses n'étant possible qu'à condition de convenir que la multiplication est prioritaire sur l'addition, ce qu'on s'empresse de faire.

Si l'on examine les deux extrémités de la chaîne d'équivalences précédente, et si on se réfère à la définition de l'égalité booléenne, on a :

$$r = 1 \quad \Leftrightarrow \quad a \cdot \bar{c} + c \cdot \bar{a} + b \cdot c + \bar{b} \cdot \bar{a} + \bar{c} \cdot \bar{b} \cdot a = 1$$

ce qui permet d'écrire :

$$r = a \cdot \bar{c} + c \cdot \bar{a} + b \cdot c + \bar{b} \cdot \bar{a} + \bar{c} \cdot \bar{b} \cdot a$$

On peut dire que r est le "polynôme" associé à l'ensemble des individus retirés.

D'une manière générale, à tout ensemble d'individus E définis à partir d'un nombre fini de variables binaires $a, b, c, \dots$, on peut, comme ci-dessus, associer un "polynôme" $P(a, b, c, \dots)$. Il s'agit effectivement d'une somme (booléenne) de "monômes" avec la particularité que chaque variable peut être complémentée ou non.

Ce polynôme s'interprète ainsi : $x \in E \Leftrightarrow P(a, b, c, \dots) = 1$.

- Troisième étape : la résolution de l'équation. (Et la solution du problème !)

Pour résoudre l'équation $r = 0$ c'est-à-dire trouver les codes (0 ou 1) des trois variables a, b, c des individus qui restent (puisque $r = 1$ code ceux qui sont retirés), on a besoin de connaître les règles de calcul de cette algèbre un peu spéciale.

Mais avant, il faut encore définir les deux "constantes" booléennes : **0** ; **1**

Ce sont les variables (fonctions constantes) :

$$\begin{aligned} \mathbf{0} & \quad (\text{qui vaut 0 pour tout individu } x) \\ \mathbf{1} & \quad (\text{qui vaut 1 pour tout individu } x) \end{aligned}$$

Toutes les règles de calcul booléen se démontrent facilement à l'aide des tables de vérité.

Ainsi : la propriété $\overline{\overline{a}} = a$ se démontre instantanément en comparant les tables de vérité des deux membres :

a	$\overline{a}$	$\overline{\overline{a}}$
0	1	0
1	0	1

De même, les fameuses lois de Morgan comme $\overline{a+b} = \overline{a} \cdot \overline{b}$ se démontrent de la même manière, en comparant les tables de vérité des deux membres :

a	b	$\overline{a}$	$\overline{b}$	$a+b$	$\overline{a+b}$	$\overline{a} \cdot \overline{b}$
0	0	1	1	0	1	1
0	1	1	0	1	0	0
1	0	0	1	1	0	0
1	1	0	0	1	0	0

La propriété $a + \overline{a} = 1$ où intervient la constante **1** se démontre ainsi :

a	$\overline{a}$	$a + \overline{a}$
0	1	1
1	0	1

On constate que $a + \overline{a}$ est la variable qui vaut toujours 1 ; celle qu'on a précisément notée **1**. D'où l'égalité voulue.

Remarquons la distinction entre le code "1" et la variable booléenne constante **1**.

Voici le formulaire complet :

(Ce formulaire est "isomorphe" à celui du calcul ensembliste dans un référentiel Ω , où les notations booléennes **0** ; **1** ; $\overline{a}$; $a + b$; $a \cdot b$ deviennent :

$\emptyset$; Ω ; $\overline{A}$; $A \cup B$; $A \cap B$.

L'embêtant avec le calcul ensembliste c'est que les expressions deviennent vite illisibles.)

$\overline{0}=1$ $\overline{1}=0$	$\overline{\overline{a}} = a$
$a + b = b + a$ $a + 0 = a$ $a + 1 = 1$ $a + a = a$ $a + \overline{a} = 1$	$a \cdot b = b \cdot a$ $a \cdot 0 = 0$ $a \cdot 1 = a$ $a \cdot a = a$ $a \cdot \overline{a} = 0$
$\overline{a+b} = \overline{a} \cdot \overline{b}$ $\overline{a \cdot b} = \overline{a} + \overline{b}$	les fameuses lois de MORGAN que les élèves ont bien du mal à appliquer
$a + (b + c) = (a + b) + c$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ a + b \cdot c &= (a + b) \cdot (a + c) \end{aligned}$	

Cette dernière propriété semble curieuse et pourtant, si on compare les colonnes 5 et 8 :

a	b	c	$b \cdot c$	$a + b \cdot c$	$a + b$	$a + c$	$(a + b) \cdot (a + c)$
0	0	0	0	0	1	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	1	0	0
0	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	1	1	1	1	1	1

Mentionnons aussi les lois dites d'absorption, très utiles pour les simplifications algébriques :

$$a + a \cdot b = a$$

$$a + \bar{a} \cdot b = a + b$$

dont les démonstrations sont immédiates à partir du formulaire précédent :

$$a + a \cdot b = a \cdot \mathbf{1} + a \cdot b = a \cdot (\mathbf{1} + b) = a \cdot \mathbf{1} = a$$

$$a + \bar{a} \cdot b = (a + \bar{a}) \cdot (a + b) = \mathbf{1} \cdot (a + b) = a + b$$

On va enfin pouvoir "calculer" le code des individus qui restent dans le problème 1 :

Les individus retirés vérifient l'équation : $r = a \cdot \bar{c} + c \cdot \bar{a} + b \cdot c + \bar{b} \cdot \bar{a} + \bar{c} \cdot \bar{b} \cdot a = 1$

Donc ceux qui restent vérifient l'équation $r = 0$ ou $\bar{r} = 1$

D'après les lois de Morgan :

$\bar{r} = (\bar{a} + c) \cdot (\bar{c} + a) \cdot (\bar{b} + \bar{c}) \cdot (b + a) \cdot (c + b + \bar{a})$ qu'on développe en utilisant la distributivité, et qu'on simplifie avec le formulaire, essentiellement $a \cdot \bar{a} = \mathbf{0}$ et $a + \mathbf{0} = a$:

$$\bar{r} = \underbrace{(\bar{a} + c) \cdot (\bar{c} + a)}_{\text{effectué.}} \cdot (\bar{b} + \bar{c}) \cdot (b + a) \cdot (c + b + \bar{a}) \quad (\text{les accolades signalent le produit})$$

effectué.)

$$\bar{r} = (\bar{a} \cdot \bar{c} + a \cdot c) \cdot \underbrace{(\bar{b} + \bar{c}) \cdot (b + a)}_{\text{effectué.}} \cdot (c + b + \bar{a})$$

$$\bar{r} = (\bar{a} \cdot \bar{c} + a \cdot c) \cdot \underbrace{(\bar{b} \cdot a + \bar{c} \cdot b + \bar{c} \cdot a)}_{\text{effectué.}} \cdot (c + b + \bar{a})$$

$$\bar{r} = (\bar{a} \cdot \bar{c} + a \cdot c) \cdot (a \cdot \bar{b} \cdot \bar{c} + a \cdot \bar{c} \cdot b + \bar{a} \cdot b \cdot \bar{c} + b \cdot \bar{c}) \quad \text{On utilise ici la propriété : } x + x = x$$

En multipliant les deux facteurs restant, on trouve : $\bar{r} = \bar{a} \cdot b \cdot \bar{c}$ (tous les autres termes étant nuls).

Puisque les individus qui restent vérifient l'équation $\bar{r} = 1$, il n'y a plus qu'à résoudre :

$$\bar{a} \cdot b \cdot \bar{c} = 1$$

$$\text{c'est-à-dire : } \bar{a} = 1 \quad \text{ET} \quad b = 1 \quad \text{ET} \quad \bar{c} = 1$$

$$\text{c'est-à-dire : } a = 0 \quad \text{ET} \quad b = 1 \quad \text{ET} \quad c = 0$$

Traduisons : les individus qui restent sont donc les "**grands méchants maigres**".

- Résolvons pour finir le Problème 2 (un peu plus difficile) :

Pour rester dans le binaire, on est obligé de supposer qu'un individu : ou bien ment toujours, ou bien dit toujours la vérité. On va retrouver nos 3 étapes :

- Première étape : définition des variables du problème.
- Deuxième étape : la mise en équation.
- Troisième étape : la résolution de l'équation.

Posons :

$$\begin{array}{lll} a = 1 & \text{si A dit la vérité,} & b = 1 & \text{si B dit la vérité,} & c = 1 & \text{si C dit la vérité,} \\ a = 0 & \text{si A ment,} & b = 0 & \text{si B ment,} & c = 0 & \text{si C ment.} \end{array}$$

"A dit que B ment" signifie : (A dit la vérité ET B ment) OU (A ment ET B dit la vérité)
qui se traduit par : $(a = 1 \text{ ET } \bar{b} = 1) \text{ OU } (\bar{a} = 1 \text{ ET } b = 1)$ soit $a \cdot \bar{b} + \bar{a} \cdot b = 1$

De même : "B dit que C ment" se traduit par : $b \cdot \bar{c} + \bar{b} \cdot c = 1$

Enfin "C dit que (A ou B ment)" signifie :

(C dit la vérité ET (A ment OU B ment)) OU (C ment ET (A dit la vérité ET B dit la vérité))

Ce qui se traduit par : $c \cdot (\bar{a} + \bar{b}) + a \cdot b \cdot \bar{c} = 1$

Le problème 2, qui est la conjonction des trois affirmations a donc pour équation :

$$(a \cdot \bar{b} + \bar{a} \cdot b) \cdot (b \cdot \bar{c} + \bar{b} \cdot c) \cdot (c \cdot \bar{a} + c \cdot \bar{b} + a \cdot b \cdot \bar{c}) = 1$$

On résout comme dans PB-1 par multiplications et simplifications, ce qui amène à

$$a \cdot \bar{b} \cdot c = 1 \text{ soit } a = 1 \text{ ET } \bar{b} = 1 \text{ ET } c = 1$$

Ce qui prouve que la seule solution au problème est : **seul B ment.**

- Un exercice pour finir :
 - A dit que "ou bien B ment ou bien C ment"
 - B dit que "A ou C ment"
 - C dit que "si D ment alors A aussi"
 - D dit que "A et B disent la vérité"

Qui ment ?