Feuille 1 : Algèbre de Boole

Exercice 1 Démontrer les propriétés suivantes en utilisant les règles du calcul booléen :

1) $(a+b).(\overline{a}+b) = b$

2) $a + \overline{b.a} = 1$

3) $\overline{a.b + \overline{a} + \overline{b}} = 0$

4) $(a \Rightarrow b) = \overline{a} + a.b$ puis $(a \Rightarrow b) = \overline{a} + b$

5) $\overline{(a \Rightarrow b)} = a.\overline{b}$

6) $(a \Rightarrow b) = (\overline{b} \Rightarrow \overline{a})$ (raisonnement par contraposée)

7) $a = (\overline{a} \Rightarrow 0)$ (raisonnement par l'absurde)

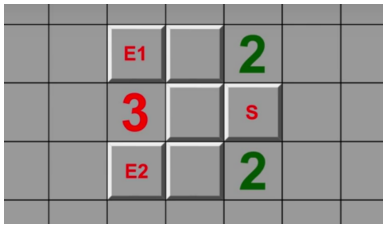
8) $(a \Leftrightarrow b) = (a \Rightarrow b).(b \Rightarrow a)$

9) $(a \Rightarrow (b+c)) = ((a.\overline{b}) \Rightarrow c)$

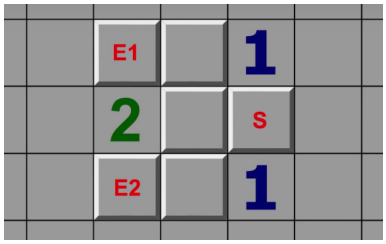
10) $(a+b).(a+c) = a + b.c$

11) $a.b.c + a.b.\overline{c} + a.\overline{b}.c + a.\overline{b}.\overline{c} = a$

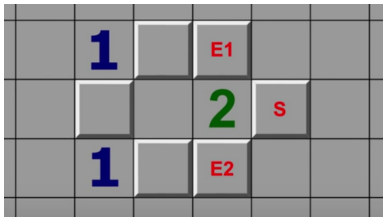
Exercice 2 **1)** On peut réaliser des portes logiques avec le démineur de Windows. Montrer que la porte suivante correspond à la porte OU (on note 1 s'il y a une mine)



2) Montrer que la porte suivante correspond à ET



3) Montrer que la porte suivante correspond à XOR



Exercice 3 Simplifier le circuit logique présenté dans le cours.

Exercice 4 **1)** On considère un ensemble E muni d'une structure d'algèbre de Boole. Soit S l'expression

$$S = a.b.c + a.\overline{b}.c + \overline{a}.b.c.$$

Montrer, par un calcul direct que $S = a.c + \overline{a}.b.c$ puis que $S = a.c + b.c$.

2) Un immeuble comprend six logements dont les surfaces figurent dans le tableau ci-dessous :

Logement	1	2	3	4	5	6
Superficie	55	105	112	228	247	253

Les logements 1 et 3 appartiennent à Monsieur A, les logements 2 et 4 appartiennent à Madame B, les 5 et 6 appartiennent à Monsieur C. Chacun détient à l'assemblée des copropriétaires un nombre de voix égal à la superficie totale de ses logements, exprimée en m^2. Ainsi, Monsieur A dispose de : $55 + 112 = 167$ voix.
Une proposition concernant le remplacement de la chaudière est mise au vote à l'assemblée. Pour être adoptée, elle doit recueillir la majorité des voix, soit 501 voix. Si A vote « pour », son vote favorable est désigné par a. S'il vote « contre », ou s'il s'abstient, son vote est désigné par $\overline{a}$. De même pour B et C.

a) Quelle situation de vote traduit le produit booléen $\overline{a}.\overline{b}.c$?

b) Écrire l'expression booléenne qui exprime la condition V pour que la proposition soit adoptée.

c) En utilisant les résultats de la question **1)**, écrire cette condition sous forme simplifiée, puis la traduire par une phrase explicative.

Exercice 5 (Registre à décalage à rétroaction linéraire)

1) On considère la suite de bits $(S_n)_{n\geq 1}$ définie par

$$S_{n+2} = S_{n+1} \oplus S_n, \quad n \geq 1,$$

initialisée par la graine $S = (S_1, S_2)$.

a) On suppose que $S = (1, 0)$. Trouver les prochains bits de la suite. Vérifier que la suite est périodique et déterminer la période.

b) Même question avec les graines $S = (0, 1)$ puis $S = (1, 1)$.

2) On considère la suite de bits $(S_n)_{n\geq 1}$ définie par

$$S_{n+4} = S_{n+2} \oplus S_n, \quad n \geq 1,$$

initialisée par la graine $S = (S_1, S_2, S_3, S_4)$.

a) On suppose que $S = (1, 1, 0, 1)$. Trouver les prochains bits de la suite. Vérifier que la suite est périodique et déterminer la période.

b) Même question avec les graines $S = (1, 0, 1, 0)$ puis $S = (0, 1, 1, 1)$.

c) Montrer que pour toute condition initiale, une telle suite est périodique de période (au plus) 6, i.e. que pour tout $n \geq 1$,

$$S_{n+6} = S_n.$$

3) On considère maintenant la suite

$$S_{n+4} = S_{n+1} \oplus S_n, \quad n \geq 1,$$

initialisée par $S = (S_1, S_2, S_3, S_4)$.

a) Étudier la suite initialisée à $S = (1, 0, 1, 1)$. Trouver la longueur du cycle de ce générateur.

b) Montrer que pour toute condition initiale, une telle suite est périodique de période (au plus) 15.

Exercice 6 (Chiffre de Vernam) On considère un message M que l'on veut chiffrer, à l'aide d'une clé secrète K (uniquement connue par l'émetteur et le destinataire). On suppose que M et K sont codés en binaires et sont de même longueur. Le message chiffré est obtenu par $C = M \oplus K$.

1) Calculer C pour $M = 0101010110$ et $K = 1100010101$.

2) Montrer que l'on reconstitue M à l'aide de la formule $M = C \oplus K$.

3) Montrer comment un attaquant peut trouver K à l'aide d'un seul message M et de sa version chiffrée C. *Remarque : c'est pour cela qu'il faut changer de clé secrète à chaque utilisation.*

Exercice 7 **A)** Soit f la fonction booléenne de quatre variables booléennes a, b, c, d définie par :

$$f(a, b, c, d) = ab + bcd + \overline{a}b\overline{c}d + \overline{a}\overline{b}c + a\overline{b}c\overline{d}.$$

Si d prend la valeur 1, on note g la fonction de trois variables définie par :

$$g(a, b, c) = f(a, b, c, 1).$$

1) Expliciter $g(a, b, c)$.

2) Simplifier la fonction g.

3) Déterminer la fonction $\overline{g}$, complémentaire de la fonction g.

B) Dans une entreprise, les personnes pouvant bénéficier de l'attribution d'une prime sont les suivantes :

- Toute personne de plus de 40 ans, ayant plus de 10 ans d'ancienneté.
- Toute personne de plus de 10 ans d'ancienneté ayant suivi un stage de formation dans les cinq dernières années, et gagnant moins de 1500 € par mois.
- Toute personne de moins de 40 ans, qui n'a pas suivi de stage de formation dans les cinq dernières années, mais ayant plus de 10 ans d'ancienneté et gagnant moins de 1500 € par mois.
- Toute personne de moins de 40 ans, ayant moins de 10 ans d'ancienneté mais qui a suivi un stage de formation dans les cinq dernières années.
- Toute personne de plus de 40 ans, de moins de 10 ans d'ancienneté qui a suivi un stage de formation dans les cinq dernières années bien qu'elle gagne plus de 1500 € par mois.

On note a, b, c et d les quatre variables booléennes caractérisant respectivement les propriétés « être une personne de plus de 40 ans », « avoir plus de 10 ans d'ancienneté », « avoir suivi un stage de formation dans les cinq dernières années » et « gagner moins de 1500 € par mois ».

1) **a)** Quelle situation traduit le produit booléen $a\overline{b}c\overline{d}$?

b) Exprimer à l'aide d'une fonction booléenne les conditions caractérisant l'attribution de la prime.

2) Parmi les personnes gagnant moins de 1500 € par mois :

a) Monsieur H a plus de 10 ans d'ancienneté. Peut-il obtenir la prime ?

b) Même question pour Madame F qui a plus de 40 ans et moins de 10 ans d'ancienneté.

c) Quelles sont les catégories d'employés qui auront la prime ?

Exercice 8 La société Jurabois exploite des coupes constituées exclusivement de feuillus et de résineux. Elle désire simplifier le règlement que ses salariés doivent appliquer pour la coupe du bois. Actuellement le règlement dit qu'un arbre est à abattre dans les quatre cas suivants :

- si c'est un résineux au tronc droit mesurant plus de 20 m de hauteur ;
- si c'est un feuillu de 50 ans ou plus ;
- s'il a moins de 50 ans et mesure plus de 20 m de hauteur ;
- s'il est tordu.

Pour un arbre quelconque, on définit les variables booléennes suivantes par :

$a = 1$ si l'arbre est un résineux ;
$b = 1$ si l'arbre a moins de 50 ans ;
$c = 1$ si l'arbre mesure plus de 20 m de hauteur ;
$d = 1$ si l'arbre est tordu.

1) Écrire la fonction booléenne $f(a, b, c, d)$, qui traduit le règlement actuel d'abattage d'un arbre.

Grâce à une bonne gestion des forêts que la société exploite, il n'y a maintenant plus d'arbres tordus.

2) Montrer que le nouveau règlement d'abattage se traduit par la fonction

$$g(a, b, c) = a.c + \overline{a}.\overline{b} + b.c.$$

3) Simplifier au maximum cette fonction.

4) Écrire la nouvelle régie d'abattage d'un arbre sous la forme la plus simple possible.

Exercice 9 Un règlement administratif concerne les trois catégories d'individus suivantes :

- les hommes de moins de 50 ans ;
- les non-salariés ayant 50 ou plus de 50 ans ;
- les femmes qui sont soit salariées, soit non salariées et qui ont moins de 50 ans.

On définit quatre variables booléennes h, a, s, r. Ainsi x désignant un individu quelconque,

$h = 1$ si x est un homme ;
$a = 1$ si x est âgé de 50 ou plus de 50 ans ;
$s = 1$ si x est salarié ;
$r = 1$ si x est concerné par le règlement.

1) Quels sont les individus x pour lesquels on a $h.\overline{a} = 1$?

2) Montrer que la catégorie de personnes concernées par ce règlement est donnée par la fonction booléenne

$$r = h.\overline{a} + \overline{s}.a + \overline{h}.(s + \overline{s}.\overline{a}).$$

3) Montrer que r peut se simplifier en

$$r = \overline{a} + \overline{s} + \overline{h}.$$

4) Simplifier le règlement.

Exercice 10 Un coffre-fort est muni de n serrures et peut être ouvert uniquement lorsque ces n serrures sont simultanément ouvertes. Cinq personnes, nommées A, B, C, D, E, doivent recevoir des clés correspondant à certaines serrures. Chaque clé peut être disponible en autant d'exemplaires qu'on le souhaite. On demande de choisir pour l'entier n la plus petite valeur possible, et de lui associer une répartition des clés entre les cinq personnes, de telle manière que le coffre puisse être ouvert si et seulement si on se trouve dans une au moins des situations suivantes :

- présence simultanée de A et B ;
- présence simultanée de A, C et D ;
- présence simultanée de B, D et E.

On désigne par a l'assertion : « A est présent », et on définit de même les assertions b, c, d, e.

1) Exprimer par une formule logique F dépendant des variables a, b, c, d, e la condition pour que le coffre puisse être ouvert.

2) Montrer que l'on peut écrire F sous la forme

$$F(a, b, c, d, e) = (a + b).(a + d).(a + e).(b + c).(b + d).$$

3) En déduire la valeur minimale de n et une répartition adéquate des clés.

Réponse : A possède les clés S_1, S_2, S_3, B possède les clés S_1, S_4, S_5, C possède la clé S_4, D possède les clés S_2, S_5 et E possède la clé S_3.