Unification dans les anneaux Booléens

Correction.

Documents autorisés (en particulier le poly).

Les questions sont annotées par un niveau de difficulté, variant de (0) (facile) à (3) (difficile). En comptant 3 minutes passées par problème facile, 6 minutes par problème de difficulté (1), 9 minutes par problème de difficulté (2), et 12 minutes par problème de difficulté (3), vous aurez besoin de 2h39 pour tout faire — 3h32 pour 4, 8, 12 et 16 minutes. Il peut y avoir plusieurs réponses aux questions; dans ce cas, n'en donnez qu'une. Les parties II et III sont indépendantes.

Le but de ce problème est d'étudier l'unification modulo la théorie d'un anneau Booléen.

Partie I.

On considère la logique classique propositionnelle sur le langage suivant. Les formules propositionnelles F, G, ... sont les variables propositionnelles A, B, C, ..., les constantes $\mathbf{0}$ (faux), $\mathbf{1}$ (vrai), les connecteurs logiques binaires $\oplus$ (ou exclusif) et $\wedge$ (et logique). Les tables de vérité de ces opérateurs sont les suivantes:

$\oplus$	faux	vrai
faux	faux	vrai
vrai	vrai	faux

$\wedge$	faux	vrai
faux	faux	faux
vrai	faux	vrai

d'où l'on déduit la sémantique des formules.

On note $F \equiv G$ le fait que F et G soient deux formules sémantiquement équivalentes (i.e., $\rho \models F$ si et seulement si $\rho \models G$).

On considérera dans cette partie des substitutions qui envoient des variables propositionnelles sur des formules. On appelle substitution close toute substitution ς telle que $\varsigma(A)$ est une formule close (sans variable libre) pour toute variable propositionnelle A. En particulier, pour toute formule F, $F\varsigma$ est une formule close.

Pour toutes substitutions closes ς et ς', on dit que $\varsigma \equiv \varsigma'$ si et seulement si pour toute variable A, $A\varsigma \equiv A\varsigma'$.

Pour toute substitution close ς, on définit $r(\varsigma)$ comme étant l'affectation qui à toute variable A associe vrai si $\models \varsigma(A)$, et faux sinon. (Ceci fabrique une affectation à partir d'une substitution close.)

Réciproquement, our toute affectation ρ, on définit $s(\rho)$ comme étant la substitution qui à toute variable A associe $\mathbf{1}$ si $\rho(A)$ est vrai, et $\mathbf{0}$ si $\rho(A)$ est faux.

1. (1) Proposer une méthode permettant de décider si une formule F dans le langage ci-dessus est satisfiable ou non, et si oui, de retourner une affectation satisfaisant F.

   La méthode la plus simple, mais pas la plus efficace, consiste à énumérer toutes les affectations ρ portant sur l'ensemble des variables propositionnelles libres dans F. Si une de celles-là rend F vraie, alors la retourner; sinon, retourner "insatisfiable".

   Une autre méthode, plus efficace en général, consiste à construire le BDD (pour un ordre donné des variables propositionnelles) de F. On construit le ou exclusif de deux BDD Φ_1 et Φ_2 par exemple comme $(\Phi_1 \vee \Phi_2) \wedge \neg(\Phi_1 \wedge \Phi_2)$, ou comme pour les autres connecteurs Booléens, en utilisant le fait que $\mathbf{0} \oplus F = F \oplus \mathbf{0} = F$, $\mathbf{1} \oplus F = F \oplus \mathbf{1}$ est la négation de F, $F \oplus F = \mathbf{0}$, et l'orthogonalité de $\oplus$: $(A \longrightarrow F_-; F_+) \oplus (A \longrightarrow G_-; G_+)$ est équivalent à $A \longrightarrow (F_- \oplus G_-); (F_+ \oplus G_+)$. La formule F est alors satisfiable si et seulement si son BDD n'est pas $\mathbf{0}$, et une affectation satisfaisant F est donnée par n'importe quel chemin allant de la racine vers $\mathbf{1}$. (Ceci est faisable sans backtracker, car suivre *une branche sortant d'un nœud qui n'aboutit pas directement à* $\mathbf{0}$ *mène à un sous-BDD qui contient nécessairement lui-même un chemin menant à* $\mathbf{1}$*.)*

On peut aussi définir un système de Gentzen pour le langage, dans lequel les règles sur $\mathbf{0}$, $\mathbf{1}$ *et* $\oplus$ *seraient par exemple:*

$$
\begin{array}{llll}
(\mathbf{0}L) & \dfrac{}{\Gamma, \mathbf{0} \longrightarrow \Delta} & (\mathbf{0}R) & \dfrac{\Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \mathbf{0}, \Delta} \\
(\mathbf{1}L) & \dfrac{\Gamma \longrightarrow \Delta}{\Gamma, \mathbf{1} \longrightarrow \Delta} & (\mathbf{1}R) & \dfrac{}{\Gamma \longrightarrow \mathbf{1}, \Delta} \\
(\oplus L) & \dfrac{\Gamma, F \longrightarrow G, \Delta \quad \Gamma, G \longrightarrow F, \Delta}{\Gamma, F \oplus G \longrightarrow \Delta} & (\oplus R) & \dfrac{\Gamma, F, G \longrightarrow \Delta \quad \Gamma \longrightarrow F, G, \Delta}{\Gamma \longrightarrow F \oplus G, \Delta}
\end{array}
$$

dont on montre la cohérence et la complétude (même sans contraction) comme dans le cours (théorème 2.3.21). Alors, pour n'importe quelle stratégie f *qui à tout séquent non-atomique associe une occurrence de formule non-atomique à expanser, soit le tableau obtenu à partir de la négation* $\mathbf{1} \oplus F$ *de* F *est clos et* F *est alors insatisfiable, soit ce tableau est non clos, et il contient donc un séquent atomique non clos* $A_1, A_2, \ldots, A_m \longrightarrow B_1, B_2, \ldots, B_n$ *(donc tel que* $A_i \neq B_j$ *pour tous* i, j*) tel que toute interprétation rendant ce séquent faux rend* $\mathbf{1} \oplus F$ *faux, donc* F *vraie : on prend n'importe quelle interprétation associant* $\mathbf{1}$ *aux* A_i *et* $\mathbf{0}$ *aux* B_j*.*

On peut enfin définir une traduction M *préservant la relation* $\rho \models \_$ *de l'espace des formules du problème vers celui des formules du cours par :* $M(\mathbf{0})$ *est n'importe quelle formule insatisfiable (par exemple* $A \wedge \neg A$*),* $M(\mathbf{1})$ *est n'importe quelle formule valide (par exemple* $A \vee \neg A$*),* $M(F \wedge G) = M(F) \wedge M(G)$*, et* $M(F \oplus G) = (M(F) \wedge \neg M(G)) \vee (M(G) \wedge \neg M(F))$*. Il ne reste plus qu'à utiliser une des méthodes du chapitre 2 sur la traduction* $M(F)$ *de la formule* F *en entrée. Par exemple, la méthode de Davis-Putnam-Logemann-Loveland répond "insatisfiable" si* $M(F)$*, donc* F*, est insatisfiable, et produit une affectation satisfaisant* $M(F)$*, donc* F*, sinon.*

2. (0) Montrer que pour toute affectation ρ, $r(s(\rho)) = \rho$.

   Pour toute variable A, $r(s(\rho))(A)$ *est vrai si et seulement si* $\models A(s(\rho))$*; or* $s(\rho)(A)$ *ne peut être que* $\mathbf{1}$ *ou* $\mathbf{0}$*, donc ceci est équivalent à* $s(\rho)(A) = \mathbf{1}$*, c'est-à-dire au fait que* $\rho(A)$ *soit vrai. Donc* $r(s(\rho)) = \rho$*.*

3. (0) Montrer que pour toute substitution close ς, $s(r(\varsigma)) \equiv \varsigma$.

   Pour toute variable A, $\models A(s(r(\varsigma)))$ *si et seulement si* $s(r(\varsigma))(A)$ *vaut* $\mathbf{1}$*, si et seulement si* $r(\varsigma)(A)$ *est vrai, si et seulement si* $\models \varsigma(A)$*, c'est-à-dire* $\models A\varsigma$*.*

4. (1) Montrer que pour toute formule F, pour toute substitution close ς, $F\varsigma$ est une formule close telle que $\models F\varsigma$ si et seulement si $r(\varsigma) \models F$.

   Puisque $F\varsigma$ *est clos,* $\models F\varsigma$ *est équivalent à* $\rho \models F\varsigma$*, pour n'importe quelle affectation* ρ*; en particulier* $\models F\varsigma$ *est équivalent à* $r(\varsigma) \models F\varsigma$*. Il suffit donc de montrer que* $r(\varsigma) \models F\varsigma$ *si et seulement si* $r(\varsigma) \models F$*.*

   On le montre par récurrence structurelle sur F*. Si* F *est une variable, alors soit* $r(\varsigma)(F)$ *est faux, donc* $r(\varsigma) \not\models F$*: alors* $r(\varsigma) \not\models F\varsigma$*, puisque* $r(\varsigma) \not\models \mathbf{0}$*; soit* $r(\varsigma)(F)$ *est vrai, et on a* $r(\varsigma) \models F$*: alors* $r(\varsigma) \models F\varsigma$ *parce que* $r(\varsigma) \models \mathbf{1}$*. Si* F *est* $\mathbf{1}$ *ou* $\mathbf{0}$*, l'équivalence souhaitée est évidente. Si* F *est une conjonction* $F_1 \wedge F_2$*, alors* $r(\varsigma) \models F\varsigma$ *si et seulement si* $r(\varsigma) \models F_1\varsigma \wedge F_2\varsigma$*, ssi* $r(\varsigma) \models F_1\varsigma$ *et* $r(\varsigma) \models F_2\varsigma$*, ssi* $r(\varsigma) \models F_1$ *et* $r(\varsigma) \models F_2$ *par hypothèse de récurrence; ceci est alors équivalent à* $r(\varsigma) \models F_1 \wedge F_2$*. Si* F *est un ou exclusif* $F_1 \oplus F_2$*, alors* $r(\varsigma) \models F\varsigma$ *si et seulement si* $r(\varsigma) \models F_1\varsigma \oplus F_2\varsigma$*, ce qui est équivalent au fait que* $r(\varsigma) \models F_1\varsigma$ *ou* $r(\varsigma) \models F_2\varsigma$ *mais pas les deux (c'est là qu'on a besoin de fixer l'affectation à gauche de* $\models$*: on n'a pas en général* $\models G_1 \oplus G_2$ *ssi* $\models G_1$ *ou exclusif* $\models G_2$*); et ceci est équivalent par hypothèse de récurrence au fait que* $r(\varsigma) \models F_1$ *ou* $r(\varsigma) \models F_2$ *mais pas les deux, c'est-à-dire à* $r(\varsigma) \models F_1 \oplus F_2$*.*

5. (0) En déduire un algorithme décidant si une formule F admet une substitution close ς telle que $\models F\varsigma$, et si oui, qui en retourne une. (On se ramènera au cas de la question I.1.)

   On teste si F *est satisfiable par l'algorithme de la question I.1.*

Si F est insatisfiable, alors il n'y a aucune substitution close ς telle que $\models F\varsigma$, sinon on aurait $r(\varsigma) \models F$ par la question I.4.

Sinon, alors soit ρ une affectation retournée par l'algorithme de la question I.1. Puisque $\rho \models F$, on a $r(s(\rho)) \models F$ par la question I.2, donc $\models F\ s(\rho)$ par la question I.4. Il suffit donc de retourner $s(\rho)$.

6. (2) Pour toute formule F, pour toute substitution close ς, on définit $S(F,\varsigma)$ comme étant la substitution qui à toute variable A associe $A\varsigma \oplus (F \wedge (A \oplus A\varsigma))$.

   Montrer que si $\models F\varsigma$, alors pour toute substitution ς', $\models F\ S(F,\varsigma)\varsigma'$. (Indication: examiner les valeurs de vérité de $A\ S(F,\varsigma)\varsigma'$ en fonction de celles de $F\varsigma'$, pour toutes les variables A.)

   Suivons l'indication donnée : $A\ S(F,\varsigma)\varsigma' = (A\varsigma \oplus (F \wedge (A \oplus A\varsigma)))\varsigma' = A\varsigma \oplus (F\varsigma' \wedge (A\varsigma' \oplus A\varsigma))$ puisque $A\varsigma$ est clos. Dans toute affectation ρ, si $F\varsigma'$ est vrai, alors $A\ S(F,\varsigma)\varsigma'$ a la même valeur de vérité que $A\varsigma \oplus (\mathbf{1} \wedge (A\varsigma' \oplus A\varsigma))$, soit que $A\varsigma \oplus (A\varsigma' \oplus A\varsigma)$, c'est-à-dire que $A\varsigma'$. Et si $F\varsigma'$ est faux, alors $A\ S(F,\varsigma)\varsigma'$ a la même valeur de vérité que $A\varsigma$.

   Donc, dans toute affectation ρ, on a l'un des deux cas suivants:

   - *$\rho \models F\varsigma'$, et alors $A\ S(F,\varsigma)\varsigma'$ et $A\varsigma'$ ont les mêmes valeurs de vérité dans ρ, pour chaque variable A. Par récurrence structurelle sur G, il s'ensuit que $G\ S(F,\varsigma)\varsigma'$ et $G\varsigma'$ ont même valeurs de vérité, pour toute formule G. En particulier, pour $G = F$, $F\ S(F,\varsigma)\varsigma'$ et $F\varsigma'$ ont même valeurs de vérité. Mais comme par hypothèse $\rho \models F\varsigma'$, on a $\rho \models F\ S(F,\varsigma)\varsigma'$.*
   - *Ou bien $\rho \not\models F\varsigma'$, et alors $A\ S(F,\varsigma)\varsigma'$ et $A\varsigma$ ont les mêmes valeurs de vérité dans ρ, pour chaque variable A. Par récurrence structurelle sur G de nouveau, il s'ensuit que $G\ S(F,\varsigma)\varsigma'$ et $G\varsigma$ ont même valeurs de vérité, pour toute formule G. En particulier, pour $G = F$, $F\ S(F,\varsigma)\varsigma'$ et $F\varsigma$ ont même valeurs de vérité. Mais comme $\models F\varsigma$, en particulier $\rho \models F\varsigma$, donc $\rho \models F\ S(F,\varsigma)\varsigma'$.*

   Dans tous les cas, $\rho \models F\ S(F,\varsigma)\varsigma'$. Donc $\models F\ S(F,\varsigma)\varsigma'$.

7. (1) Montrer que pour toutes substitutions closes ς, ς' telles que $\models F\varsigma$ et $\models F\varsigma'$, alors $\varsigma' \equiv S(F,\varsigma)\varsigma'$.

   Soit A une variable propositionnelle arbitraire; nous devons prouver que $\rho \models A\varsigma'$ ssi $\rho \models A\ S(F,\varsigma)\varsigma'$, pour toute affectation ρ. On a $A\ S(F,\varsigma)\varsigma' = A\varsigma \oplus (F \wedge (A \oplus A\varsigma))\varsigma' = A\varsigma \oplus (F\varsigma' \wedge (A\varsigma' \oplus A\varsigma))$. Comme $\models F\varsigma'$, en particulier $F\varsigma'$ est vrai dans ρ, donc $A\ S(F,\varsigma)\varsigma'$ a la même valeur de vérité que $A\varsigma \oplus (A\varsigma' \oplus A\varsigma)$, c'est-à-dire que $A\varsigma'$.

Partie II.

La langage des anneaux Booléens est un langage du premier ordre formé sur les constantes 0, 1, ainsi que des symboles de fonction binaires $+$ et $*$, et du symbole de prédicat binaire $\doteq$.

Les anneaux Booléens sont les anneaux commutatifs dont la multiplication est idempotente et l'addition est 2-nilpotente. Autrement dit, ce sont les modèles équationnels (c'est-à-dire dans lesquels $\doteq$ est interprété par la relation d'égalité) de la théorie $\mathcal{B}$ suivante :

$(\mathcal{B}1)$ $(u+v)+w \doteq u+(v+w)$	$(\mathcal{B}2)$ $u+v \doteq v+u$	$(\mathcal{B}3)$ $u+0 \doteq u$	$(\mathcal{B}4)$ $u+u \doteq 0$
$(\mathcal{B}5)$ $(u*v)*w \doteq u*(v*w)$	$(\mathcal{B}6)$ $u*v \doteq v*u$	$(\mathcal{B}7)$ $u*1 \doteq u$	$(\mathcal{B}8)$ $u*u \doteq u$
$(\mathcal{B}9)$ $(u+v)*w \doteq (u*w)+(v*w)$			

pour tous termes u, v, w du langage.

Pour tous termes u, v, on notera $\models_{\mathcal{B}} u \doteq v$ pour dire que les valeurs de u et de v sont les mêmes dans tous les anneaux Booléens.

Le problème de l'unification modulo $\mathcal{B}$ est le suivant: étant donné deux termes u et v dans le langage de $\mathcal{B}$, trouver les substitutions σ telles que $\models_{\mathcal{B}} u\sigma \doteq v\sigma$.

1. (0) Montrer que $\models_{\mathcal{B}} u \doteq v$ si et seulement si $\models_{\mathcal{B}} u+v \doteq 0$. En déduire qu'on peut réduire le problème de l'existence d'un $\mathcal{B}$-unificateur à la question de l'existence d'une substitution σ telle que $\models_{\mathcal{B}} w\sigma \doteq 0$, pour un certain terme w.

Si $\models_{\mathcal{B}} u\doteq v$, *alors* $\models_{\mathcal{B}} u+v\doteq 0$ *par* $(\mathcal{B}4)$. *Réciproquement, si* $\models_{\mathcal{B}} u+v\doteq 0$, *alors d'un côté* $\models_{\mathcal{B}} u+(u+v)\doteq u+0\doteq u$ *(par* $(\mathcal{B}3)$*), et d'un autre côté* $\models_{\mathcal{B}} u+(u+v)\doteq(u+u)+v$ *(par* $(\mathcal{B}1)$*)* $\doteq 0+v$ *(par* $(\mathcal{B}4)$*)* $\doteq v$ *(par* $(\mathcal{B}2)$ *et* $(\mathcal{B}3)$*), donc* $\models_{\mathcal{B}} u\doteq v$ *par transitivité de l'interprétation de* $\doteq$ *(qui est l'égalité, puisqu'on se place dans un modèle équationnel).*

Il suffit donc de prendre $w=u+v$.

2. (0) Montrer qu'il existe σ tel que $\models_{\mathcal{B}} u\sigma\doteq v\sigma$ si et seulement s'il existe une substitution σ close (envoyant les variables libres de u et de v vers des termes clos) telle que $\models_{\mathcal{B}} u\sigma\doteq v\sigma$.

   La direction "si" est évidente. Montrons la direction "seulement si" : soit σ *une substitution quelconque telle que* $\models_{\mathcal{B}} u\sigma\doteq v\sigma$. *Soit* σ' *une substitution envoyant toute variable libre dans* $u\sigma$ *ou dans* $v\sigma$ *vers une constante (par exemple* 0*). Alors* $\models_{\mathcal{B}} u\sigma\sigma'\doteq v\sigma\sigma'$, *et* $\sigma\sigma'$ *est une substitution close par construction.*

3. (2) On considère la théorie suivante Eq, dite théorie de l'égalité sur le langage de $\mathcal{B}$:

   $(E1)$ $u\doteq u$ $\quad$ $(E2)$ $u\doteq v \Rightarrow v\doteq u$ $\quad$ $(E3)$ $u\doteq v \wedge v\doteq w \Rightarrow u\doteq w$
   $(E4)$ $u\doteq u' \wedge v\doteq v' \Rightarrow u+v\doteq u'+v'$ $\quad$ $(E5)$ $u\doteq u' \wedge v\doteq v' \Rightarrow u*v\doteq u'*v'$

   pour tous termes u, v, w, u', v'.

   Démontrer que dans tout modèle de $\mathcal{B}+Eq$ (la théorie ayant comme axiomes ceux de $\mathcal{B}$ et ceux de Eq), les formules suivantes sont valides:

   $$(\mathcal{B}10)\ 0+u\doteq u \quad (\mathcal{B}11)\ 0*u\doteq 0 \quad (\mathcal{B}12)\ u*0\doteq 0$$

   $(\mathcal{B}10)$ *: par* $(\mathcal{B}3)$, $u+0\doteq u$ *est valide, et par* $(\mathcal{B}2)$ $0+u\doteq u+0$ *tient; par modus ponens avec* $(E3)$*, il suit que* $0+u\doteq u$ *tient.*

   $(\mathcal{B}11)$ *: pour tout terme* v, $(v+v)*u\doteq 0*u$, *par* $(\mathcal{B}4)$ *et* $(E5)$. *Par* $(E2)$, $0*u\doteq(v+v)*u$. *Mais par* $(\mathcal{B}9)$, $(v+v)*u\doteq v*u+v*u$ *est valide, et par* $(\mathcal{B}4)$ $v*u+v*u\doteq 0$ *est valide. Appliquant* $(E3)$ *deux fois, il s'ensuit que* $0*u\doteq 0$.

   $(\mathcal{B}12)$ *: par* $(E2)$ $u*0\doteq 0*u$ *est valide, et par* $(\mathcal{B}11)$ $0*u\doteq 0$ *est valide. Donc par* $(E3)$ $u*0\doteq 0$ *est valide.*

4. (1) Vérifier que l'interprétation canonique I^C est un modèle de $\mathcal{B}+Eq$, où I^C est définie comme suit : le domaine D est celui des formules closes de la partie I, $I^C(0)=\mathbf{0}$, $I^C(1)=\mathbf{1}$, $I^C(+)(x,y)=x\oplus y$, $I^C(*)(x,y)=x\wedge y$, $I^C(\doteq)$ est la relation $\equiv$.

   Il suffit de vérifier les axiomes un à un :

   - $(\mathcal{B}1)$*:* $(u\oplus v)\oplus w$ *est vrai ssi* $u\oplus v$ *est vrai et* w *est faux, ou bien* $u\oplus v$ *est faux et* w *vrai, c'est-à-dire dans les quatre cas suivants: u vrai, v faux, w faux; u faux, v vrai, w faux; u vrai, v vrai, w vrai; u faux, v faux, w vrai.*

     $u\oplus(v\oplus w)$ *est vrai ssi* u *est vrai et* $v\oplus w$ *est faux, ou bien* u *est faux et* $v\oplus w$ *vrai, c'est-à-dire dans les quatre cas suivants: u vrai, v vrai, w vrai; u vrai, v faux, w faux; u faux, v vrai, w faux; u faux, v faux, w vrai.*

     On vérifie que ce sont les mêmes cas, donc $(u\oplus v)\oplus w\equiv u\oplus(v\oplus w)$.
   - $(\mathcal{B}2)$*:* $u\oplus v$ *est vrai ssi* u *ou* v *est vrai mais pas les deux, et de même pour* $v\oplus u$.
   - $(\mathcal{B}3)$*:* $u\oplus 0$ *est vrai ssi* u *est vrai et* 0 *est faux, ou bien* u *est faux et* 0 *est vrai. Mais ce dernier cas est impossible, et* 0 *est toujours faux, donc* $u\oplus 0$ *est vrai ssi* u *est vrai.*
   - $(\mathcal{B}4)$*:* $u\oplus u$ *est vrai ssi* u *est vrai et* u *est faux (impossible), ou* u *est faux et* u *est vrai (impossible). De même,* 0 *n'est jamais vrai.*
   - $(\mathcal{B}5)$*:* $(u\wedge v)\wedge w$ *et* $u\wedge(v\wedge w)$ *sont vrais ssi* u, v, w *sont tous vrais, donc* $(u\wedge v)\wedge w\equiv u\wedge(v\wedge w)$.
   - $(\mathcal{B}6)$*:* $u\wedge v$ *et* $v\wedge u$ *sont vrais ssi* u *et* v *sont tous les deux vrais, donc* $u\wedge v\equiv v\wedge u$.
   - $(\mathcal{B}7)$*:* $u\wedge\mathbf{1}$ *est vrai ssi* u *est vrai et* $\mathbf{1}$ *est vrai, c'est-à-dire ssi* u *est vrai.*

- $(\mathcal{B}8)$: *$u \wedge u$ est vrai ssi u est vrai et u est vrai, c'est-à-dire ssi u est vrai.*
- $(\mathcal{B}9)$: *$(u \oplus v) \wedge w$ est vrai ssi $u \oplus v$ est vrai et w est vrai, c'est-à-dire dans les deux cas suivants: u vrai, v faux, w vrai; u faux, v vrai, w vrai.*

  $(u \wedge w) \oplus (v \wedge w)$ est vrai ssi $u \wedge w$ est vrai et $v \wedge w$ est faux (auquel cas u et w sont vrais, et v doit être faux), ou $u \wedge w$ est faux et $v \wedge w$ est vrai (auquel cas v et w sont vrais, et u doit être faux).

  Les cas où ces deux formules sont vraies sont les mêmes, donc $(u \oplus v) \wedge w \equiv (u \wedge w) \oplus (v \wedge w)$.
- $(E1)$: *$u \equiv u$ est évident.*
- $(E2)$: *il est clair que si $u \equiv v$, alors $v \equiv u$.*
- $(E3)$: *il est clair que si $u \equiv v$ et $v \equiv w$, alors $u \equiv w$.*
- $(E4)$: *si $u \equiv u'$ et $v \equiv v'$, alors dans toute affectation (u, v) et (u', v') repèrent la même case dans la table de vérité de $\oplus$, donc $u \oplus v$ et $u' \oplus v'$ ont la même valeur de vérité. L'affectation étant arbitraire, $u \oplus v \equiv u' \oplus v'$.*
- $(E5)$: *même argument que pour $(E4)$, en utilisant la table de $\wedge$.*

5. (2) Vérifier que tout modèle équationnel de $\mathcal{B}$ est un modèle de $\mathcal{B} + Eq$. Réciproquement, montrer que, pour tout modèle I de domaine D de $\mathcal{B}$, on peut fabriquer une interprétation $I/I(\doteq)$, que l'on appellera modèle quotient, et qui est un modèle équationnel de $\mathcal{B}$.

   Que tout modèle équationnel de $\mathcal{B}$ est un modèle de $\mathcal{B} + Eq$ est clair: il suffit de vérifier que la relation d'égalité vérifie tous les axiomes de Eq. Et l'égalité est effectivement réflexive, symétrique, transitive, et passe au contexte.

   Réciproquement, soit I un modèle de $\mathcal{B}$, et $I(0)$, $I(1)$, $I(+)$, $I(*)$, $I(\doteq)$ les interprétations des symboles de $\mathcal{B}$. $I(\doteq)$ est par définition une relation d'équivalence (par $(E1)$, $(E2)$, $(E3)$), on peut donc définir $D/I(\doteq)$ comme étant l'ensemble D quotienté par $I(\doteq)$, et définir $I(0)/I(\doteq)$ comme étant la classe déquivalence de $I(0)$, $I(1)/I(\doteq)$ comme étant la classe déquivalence de $I(1)$, $I(+)/I(\doteq)(X, Y)$ comme étant la classe des $I(+)(x, y)$ lorsque $x \in X$, $y \in Y$ (qui est unique par $(E4)$), et $I(*)/I(\doteq)(X, Y)$ comme étant la classe des $I(*)(x, y)$ lorsque $x \in X$, $y \in Y$ (qui est unique par $(E5)$). On pose aussi $I(\doteq)/I(\doteq)$ la relation R telle que $X\ R\,Y$ si et seulement s'il existe $x \in X$ et $y \in Y$ tels que $x\ I(\doteq)\ y$. R est exactement la relation d'égalité sur $D/I(\doteq)$: si $X\ R\ Y$, alors il existe $x \in X$ et $y \in Y$ tels que $x\ I(\doteq)\ y$, donc y est dans la classe X de x, et x est dans la classe Y de y, donc $X = Y$; et réciproquement, si $X = Y$ alors $X\ R\ Y$ car les classes d'équivalence sont non vides.

   Soit $I/I(\doteq)$ l'interprétation $(D/I(\doteq), I(0)/I(\doteq), I(1)/I(\doteq), I(+)/I(\doteq), I(*)/I(\doteq), R)$. Il est clair que tous les axiomes de $\mathcal{B}$ sont vrais dans I; et comme R est l'égalité, les axiomes de Eq le sont aussi. Donc $I/I(\doteq)$ est un modèle équationnel de $\mathcal{B}$.

6. (2) On appelle modèle de Herbrand équationnel de $\mathcal{B}$ tout modèle de la forme $I/I(\doteq)$, où I est un modèle de Herbrand de $\mathcal{B}$.

   Montrer que tous les modèles de Herbrand équationnels de $\mathcal{B}$ sont finis, et les décrire. (Indication: montrer que dans tous les modèles de Herbrand I de $\mathcal{B} + Eq$, pour tout élément u de l'univers de Herbrand, $I \models u \doteq 0$ ou $I \models u \doteq 1$.)

   Par définition, le domaine d'un modèle de Herbrand I pour $\mathcal{B}$ est l'ensemble des termes clos du langage. Soit u un terme clos quelconque, on montre par récurrence structurelle sur u que $u\ I(\doteq)\ 0$ ou $u\ I(\doteq)\ 1$, autrement dit $I \models u \doteq 0$ ou $I \models u \doteq 1$.

   Si $u = 0$ ou $u = 1$, c'est trivial.

   Si u est une somme $u_1 + u_2$, alors par hypothèse de récurrence $I \models u_1 \doteq 0$ ou $I \models u_1 \doteq 1$, et $I \models u_2 \doteq 0$ ou $I \models u_2 \doteq 1$. Si $I \models u_1 \doteq 0$ et $I \models u_2 \doteq 0$, ou bien si $I \models u_1 \doteq 1$ et $I \models u_2 \doteq 1$, alors $I \models u_1 \doteq u_2$, donc parce que I valide l'axiome $(\mathcal{B}4)$, on a aussi $I \models u_1 + u_2 \doteq 0$, c'est-à-dire $I \models u \doteq 0$. Sinon, si $I \models u_1 \doteq 0$ et $I \models u_2 \doteq 1$, alors $I \models u \doteq 1$ par $(\mathcal{B}2)$ et $(\mathcal{B}3)$. Et si $I \models u_1 \doteq 1$ et $I \models u_2 \doteq 0$, alors $I \models u \doteq 1$ par $(\mathcal{B}3)$.

Si u est un produit $u_1 * u_2$, alors par hypothèse de récurrence $I \models u_1 \doteq 0$ ou $I \models u_1 \doteq 1$, et $I \models u_2 \doteq 0$ ou $I \models u_2 \doteq 1$. Si $I \models u_1 \doteq 0$, alors par ($\mathcal{B}12$), $I \models u \doteq 0$. Si $I \models u_2 \doteq 0$, alors par ($\mathcal{B}11$), $I \models u \doteq 0$. Finalement, si $I \models u_1 \doteq 1$ et $I \models u_2 \doteq 1$, alors par ($\mathcal{B}7$), $I \models u \doteq 1$.

Il n'y a donc qu'au plus deux éléments dans le domaine d'un modèle de Herbrand équationnel de $\mathcal{B}$: $I(0)$ et $I(1)$. Le seul degré de liberté qui nous reste est de décider si $I(0) = I(1)$ ou non. Il n'y a donc que deux modèles de Herbrand équationnels de $\mathcal{B}$:

- *Le modèle trivial à un élément (les interprétations des symboles sont alors immédiates);*
- *et le modèle à deux éléments $I(0)$ et $I(1)$ distincts, où $I(+)$ et $I(*)$ sont décrites par les tables:*

$I(+)$	$I(0)$	$I(1)$
$I(0)$	$I(0)$	$I(1)$
$I(1)$	$I(1)$	$I(0)$

$I(*)$	$I(0)$	$I(1)$
$I(0)$	$I(0)$	$I(0)$
$I(1)$	$I(0)$	$I(1)$

On remarque au passage que ce dernier modèle est isomorphe au modèle quotient de celui de la question 4.

7. (3) On suppose donnée une correspondance bijective $x \mapsto A_x$ entre variables du premier ordre x et variables propositionnelles.

   On définit la traduction canonique suivante des termes de $\mathcal{B}$ vers les formules de la partie I par : $T(0) = \mathbf{0}$, $T(1) = \mathbf{1}$, $T(x) = A_x$, $T(u+v) = T(u) \oplus T(v)$, $T(u * v) = T(u) \wedge T(v)$. On remarquera que, si u est clos, $T(u)$ est la valeur de u dans le modèle canonique de la question II.4.

   Déduire des questions précédentes que, pour tous termes clos u et v, $\models_{\mathcal{B}} u \doteq v$ si et seulement si $\models T(u+v) \oplus \mathbf{1}$.

   Si $\models_{\mathcal{B}} u \doteq v$, alors par la question II.1 $\models_{\mathcal{B}} u + v \doteq 0$. Par la question II.4, l'interprétation canonique de $u+v$ est équivalente à celle de 0, c'est-à-dire $T(u+v) \equiv T(0)$, i.e. $T(u+v) \equiv \mathbf{0}$. Ceci est équivalent à $T(u+v) \oplus \mathbf{1} \equiv \mathbf{1}$, par inspection de la table de vérité de $\oplus$, et revient donc à dire $\models T(u+v) \oplus \mathbf{1}$.

   Réciproquement, si $\models T(u+v) \oplus \mathbf{1}$, alors l'interprétation canonique de $u+v$ est équivalente à celle de 0, c'est-à-dire que $u+v \doteq 0$ est vrai dans le modèle de Herbrand équationnel à deux éléments de $\mathcal{B}$. D'un autre côté, $u+v \doteq 0$ est vrai dans le modèle de Herbrand équationnel à un élément, parce que $I(\doteq)$ y est réflexive. Donc $u+v \doteq 0$ est vrai dans tous les modèles de Herbrand équationnels de $\mathcal{B}$.

   Choisissons alors un modèle de Herbrand I quelconque de $\mathcal{B} + Eq$. Comme la formule $u+v \doteq 0$ est close, on a $I \models u+v \doteq 0$ ou $I \models \neg(u+v \doteq 0)$. Dans le deuxième cas, on aurait $I/I(\doteq) \models \neg(u+v \doteq 0)$ par la question II.5, deuxième partie. Mais c'est impossible, parce que $I/I(\doteq)$ est l'un des deux modèles sus-cités, où $u+v \doteq 0$ est vrai. Donc $u+v \doteq 0$ est vrai dans tout modèle de Herbrand de $\mathcal{B} + Eq$.

   Choisissons alors un modèle I quelconque de $\mathcal{B} + Eq$. L'ensemble des formules atomiques closes qui sont vraies dans I détermine un modèle de Herbrand de $\mathcal{B} + Eq$, qui valide donc $u+v \doteq 0$. Il s'ensuit que $I \models u+v \doteq 0$ (c'est le lemme 6.5.7 du cours, par exemple).

   Pour tout modèle équationnel I de $\mathcal{B}$, par la question II.5 première partie, I est aussi un modèle de $\mathcal{B} + Eq$, donc $I \models u+v \doteq 0$. Donc $I \models u \doteq v$ par la question II.1. Comme I est arbitraire, on en conclut que $\models_{\mathcal{B}} u \doteq v$.

8. (1) On définit $\vec{T}$ par: $\vec{T}(\sigma)$ est la substitution qui à toute variable propositionnelle A_x associe $T(x\sigma)$. Montrer que T et $\vec{T}$ sont bijectives, et que pour tous termes u, toutes substitutions σ, $T(u\sigma) = T(u)\,\vec{T}(\sigma)$.

   On définit T^{-1} par récurrence structurelle sur les formules comme suit: $T^{-1}(A_x) = x$, $T^{-1}(\mathbf{0}) = 0$, $T^{-1}(\mathbf{1}) = 1$, $T^{-1}(F \oplus G) = T^{-1}(F) + T^{-1}(G)$, $T^{-1}(F \wedge G) = T^{-1}(F) * T^{-1}(G)$. Une récurrence structurelle simple montre alors que $T(T^{-1}(F)) = F$ pour toute formule F, et $T^{-1}(T(u)) = u$ pour toute terme u.

   On définit $\vec{T}^{-1}(\varsigma)$ comme la substitution qui à tout x associe $T^{-1}(A_x\varsigma)$. $\vec{T}(\vec{T}^{-1}(\varsigma))$ associe alors à tout A_x la formule $T(T^{-1}(A_x\varsigma))$, et est donc égale à ς. Réciproquement, $\vec{T}^{-1}(\vec{T}(\sigma))$ associe à tout x le terme $T^{-1}(T(x\sigma))$, et est donc égale à σ.

Finalement, on montre que $T(u\sigma) = T(u)\,\vec{T}(\sigma)$ par récurrence structurelle sur u. Si u est une variable, alors $T(u)\,\vec{T}(\sigma) = A_u\,\vec{T}(\sigma) = T(u\sigma)$ par définition. Les cas où u est 0, 1, une somme ou un produit sont des utilisations directes de l'hypothèse de récurrence sur les sous-termes immédiats.

9. (2) Déduire des questions précédentes et de la question I.5 un algorithme décidant si deux termes de $\mathcal{B}$ ont un $\mathcal{B}$-unificateur, et si oui, qui en retourne un. Existe-t-il un algorithme en temps polynomial pour résoudre ce problème ? (On admettra que le problème de la satisfiabilité dans la logique de la partie I est NP-complet.)

   Soient u et v deux termes quelconques de $\mathcal{B}$. Par la question II.2, u et v sont $\mathcal{B}$-unifiables si et seulement s'il existe une substitution close σ telle que $\models_{\mathcal{B}} u\sigma \doteq v\sigma$. Comme $u\sigma$ et $v\sigma$ sont clos, par la question II.7, $\models_{\mathcal{B}} u\sigma \doteq v\sigma$ est équivalent à $\models T(u\sigma + v\sigma) \oplus \mathbf{1}$. Mais $u\sigma + v\sigma = (u+v)\sigma$, et par la question II.8, $T(u\sigma + v\sigma) = T(u+v)\,\vec{T}(\sigma)$, donc $T(u\sigma + v\sigma) \oplus \mathbf{1} = (T(u+v) \oplus \mathbf{1})\,\vec{T}(\sigma)$. En résumé, u et v sont $\mathcal{B}$-unifiables si et seulement s'il existe une substitution propositionnelle ς de la forme $\vec{T}(\sigma)$, où σ est une substitution du premier ordre, telle que $\models (T(u+v) \oplus \mathbf{1})\varsigma$.

   Mais puisque $\vec{T}$ est bijective, toutes les substitutions propositionnelles ς sont de la forme $\vec{T}(\sigma)$ pour un certain σ (il suffit de prendre $\sigma = \vec{T}^{-1}(\varsigma)$). De plus, les $\mathcal{B}$-unificateurs σ de u et v sont exactement les $\vec{T}^{-1}(\varsigma)$, lorsque ς est tel que $\models (T(u+v) \oplus \mathbf{1})\varsigma$. On en déduit l'algorithme suivant: appliquer l'algorithme de la question I.5 sur la formule $T(u+v) \oplus \mathbf{1}$; si la réponse est "insatisfiable", retourner "non unifiable"; sinon, soit ς la substitution propositionnelle retournée, et renvoyer $\vec{T}^{-1}(\varsigma)$.

   Le problème de l'unifiabilité modulo $\mathcal{B}$ est donc équivalent à traductions en temps polynomial près au problème de la satisfiabilité en logique propositionnelle classique fondée sur les symboles $\mathbf{0}$, $\mathbf{1}$, $\oplus$, $\wedge$. On peut montrer (même si ce n'est pas le langage du problème SAT) que ce problème est NP-complet, ce que l'on a demandé d'admettre. Il n'existe donc aucun algorithme de $\mathcal{B}$-unifiabilité en temps polynomial, sauf si $P = NP$.

10. (3) On dit de deux substitutions σ et σ' qu'elles sont $\mathcal{B}$-équivalentes, et on note $\sigma \equiv_{\mathcal{B}} \sigma'$, si et seulement si pour toute variable x, $\models_{\mathcal{B}} x\sigma \doteq x\sigma'$. On dit que σ est plus $\mathcal{B}$-général que σ', et on note $\sigma \leq_{\mathcal{B}} \sigma'$, si et seulement s'il existe une substitution σ'' telle que $\sigma\sigma'' \equiv_{\mathcal{B}} \sigma'$.

    Déduire des constructions précédentes et des questions I.6 et I.7 que la $\mathcal{B}$-unification est unitaire, c'est-à-dire que pour tous termes u et v dans le langage de $\mathcal{B}$, soit u et v ne sont pas unifiables, soit ils ont un unificateur le plus $\mathcal{B}$-général.

    Soient u et v deux termes quelconques dans le langage de $\mathcal{B}$, et supposons que u et v soient $\mathcal{B}$-unifiables. Alors il existe une substitution close σ telle que $\models_{\mathcal{B}} u\sigma \doteq v\sigma$, donc $\models (T(u+v) \oplus \mathbf{1})\,\vec{T}(\sigma)$. Par la question I.6, $\models (T(u+v) \oplus \mathbf{1})\,S(T(u+v) \oplus \mathbf{1}, \vec{T}(\sigma))\varsigma'$ pour toute substitution ς'. Choisissons pour ς' la substitution identité. Alors $\models (T(u+v) \oplus \mathbf{1})\,S(T(u+v) \oplus \mathbf{1}, \vec{T}(\sigma))$, c'est-à-dire $\models T(u\sigma_0 + v\sigma_0) \oplus \mathbf{1}$, où $\sigma_0 = \vec{T}^{-1}(S(T(u+v) \oplus \mathbf{1}, \vec{T}(\sigma)))$.

    Donc σ_0 est un $\mathcal{B}$-unificateur de u et v. Nous montrons maintenant, à l'aide de la question I.7, qu'il est un unificateur le plus général. Soit donc σ' un autre $\mathcal{B}$-unificateur clos de u et v. On a $\models (T(u+v) \oplus \mathbf{1})\,\vec{T}(\sigma')$. Mais par la question I.7, et comme $\models (T(u+v) \oplus \mathbf{1})\,\vec{T}(\sigma)$ par hypothèse, $\vec{T}(\sigma') \equiv S(T(u+v) \oplus \mathbf{1}, \vec{T}(\sigma))\,\vec{T}(\sigma')$. C'est-à-dire que pour toute variable A_x, $A_x\vec{T}(\sigma') \equiv A_x S(T(u+v) \oplus \mathbf{1}, \vec{T}(\sigma))\,\vec{T}(\sigma')$. Donc, par la question II.7, $\models_{\mathcal{B}} T^{-1}(A_x\vec{T}(\sigma')) \doteq T^{-1}(A_x S(T(u+v) \oplus \mathbf{1}, \vec{T}(\sigma))\,\vec{T}(\sigma'))$, c'est-à-dire $\models_{\mathcal{B}} x\sigma' \doteq x\vec{T}^{-1}(S(T(u+v) \oplus \mathbf{1}, \vec{T}(\sigma))\,\vec{T}(\sigma'))$. Comme x est arbitraire, $\sigma' \equiv_{\mathcal{B}} \vec{T}^{-1}(S(T(u+v) \oplus \mathbf{1}, \vec{T}(\sigma))\,\vec{T}(\sigma'))$.

    Maintenant, $\vec{T}^{-1}(S(T(u+v) \oplus \mathbf{1}, \vec{T}(\sigma))\,\vec{T}(\sigma')) = \vec{T}^{-1}(S(T(u+v) \oplus \mathbf{1}, \vec{T}(\sigma)))\,\vec{T}^{-1}(\vec{T}(\sigma'))$ par la question II.8, autrement dit $\vec{T}^{-1}(S(T(u+v) \oplus \mathbf{1}, \vec{T}(\sigma))\,\vec{T}(\sigma')) = \sigma_0\sigma'$. En particulier, $\sigma' \equiv_{\mathcal{B}} \sigma_0\sigma'$, donc il existe σ'' tel que $\sigma' \equiv_{\mathcal{B}} \sigma_0\sigma''$ (il suffit de prendre $\sigma'' = \sigma'$), c'est-à-dire que $\sigma_0 \leq_{\mathcal{B}} \sigma'$.

Partie III.

Le but de cette partie est de montrer que le langage de la partie I permet de trouver une structure aux propriétés analogues aux BDD, et analogues aux formes de Reed-Muller.

On se place donc dans le langage des formules propositionnelles de la partie I.

1. (1) Montrer que pour toute formule F, pour toute variable propositionnelle A, il existe deux formules F_1 et F_2 uniques à équivalence ($\equiv$) près, telles que $F \equiv (F_1 \wedge A) \oplus F_2$, et A n'est libre ni dans F_1 ni dans F_2.

   Supposons que F_1 et F_2 existent, alors nécessairement $F[\mathbf{0}/A] = (F_1 \wedge \mathbf{0}) \oplus F_2$, puisque A n'est pas libre dans F_1 ou F_2, donc $F[\mathbf{0}/A] \equiv F_2$, et en particulier F_2 est uniquement à équivalence près. D'un autre côté, $F[\mathbf{1}/A] = (F_1 \wedge \mathbf{1}) \oplus F_2 \equiv F_1 \oplus F_2$, donc $F_1 \equiv F[\mathbf{1}/A] \oplus F_2$, et F_1 est donc elle aussi unique à équivalence près.

   Montrons maintenant l'existence de F_1 et F_2. Posons $F_2 = F[\mathbf{0}/A]$, et $F_1 = F[\mathbf{1}/A] \oplus F[\mathbf{0}/A]$. Alors A n'est pas libre dans F_1 ou F_2 par construction, et $(F_1 \wedge A) \oplus F_2 = ((F[\mathbf{1}/A] \oplus F[\mathbf{0}/A]) \wedge A) \oplus F[\mathbf{0}/A]$. Dans toute affectation, si A est vraie, alors $(F_1 \wedge A) \oplus F_2$ a la même valeur de vérité que $(F[\mathbf{1}/A] \oplus F[\mathbf{0}/A]) \oplus F[\mathbf{0}/A]$, c'est-à-dire que $F[\mathbf{1}/A]$, c'est-à-dire que F, puisque A est vraie. Et si A est fausse, alors $(F_1 \wedge A) \oplus F_2$ a la même valeur de vérité que $F[\mathbf{0}/A]$, c'est-à-dire que F encore une fois. Donc $F \equiv (F_1 \wedge A) \oplus F_2$.

2. (1) On dit qu'une formule F est indépendante d'une variable A si et seulement s'il existe une formule G dans laquelle A n'est pas libre, et telle que $F \equiv G$.

   Soient F_1 et F_2 deux formules dans lesquelles A n'est pas libre. Montrer que $(F_1 \wedge A) \oplus F_2$ est indépendante de A si et seulement si $F_1 \equiv \mathbf{0}$.

   Si $F_1 \equiv 0$, alors dans toute affectation, $(F_1 \wedge A) \oplus F_2$ a la même valeur de vérité que F_2. Donc $(F_1 \wedge A) \oplus F_2 \equiv F_2$, et comme A n'est pas libre dans F_2, $(F_1 \wedge A) \oplus F_2$ est indépendante de A.

   Réciproquement, si $(F_1 \wedge A) \oplus F_2$ est indépendante de A, soit F une formule dans laquelle A n'est pas libre telle que $F \equiv (F_1 \wedge A) \oplus F_2$. Mais on a aussi $F \equiv (\mathbf{0} \wedge A) \oplus F$. Par la question III.1, F_1 et F_2 sont uniques, donc $F_1 \equiv \mathbf{0}$ et $F_2 \equiv F$.

3. (2) On appelle forme de Reed-Muller ordonnée réduite une structure de style BDD définie comme suit. On se fixe un ordre total strict $<$ sur les variables propositionnelles. Les formes de Reed-Muller ordonnées réduites (RMO) sont définies inductivement comme étant $\mathbf{0}$, $\mathbf{1}$, et $A/\Phi_1;\Phi_2$, où Φ_1 et Φ_2 sont des RMO n'utilisant que des variables B telles que $A < B$, et $\Phi_1 \neq \mathbf{0}$.

   On définit la fonction suivante, qui retrouve une formule à partir d'un RMO: $f(\mathbf{0}) = \mathbf{0}$, $f(\mathbf{1}) = \mathbf{1}$, $f(A/\Phi_1;\Phi_2) = (f(\Phi_1) \wedge A) \oplus f(\Phi_2)$, et on définit la sémantique des RMO par: $\rho \models \Phi$ si et seulement si $\rho \models f(\Phi)$.

   Montrer que, pour deux RMO Φ_1 et Φ_2, $\Phi_1 \equiv \Phi_2$ si et seulement si $\Phi_1 = \Phi_2$. (Autrement dit, les RMO sont des formes canoniques de formules Booléennes.)

   Si $\Phi_1 = \Phi_2$, alors il est trivial que $\Phi_1 \equiv \Phi_2$.

   Réciproquement, supposons $\Phi_1 \equiv \Phi_2$, et soit $A_n < A_{n-1} < \ldots < A_1$ une énumération ordonnée des variables apparaissant dans Φ_1 ou dans Φ_2. Nous montrons que $\Phi_1 = \Phi_2$ par récurrence sur n. Si $n = 0$, alors Φ_1 et Φ_2 doivent être chacun soit $\mathbf{0}$ soit $\mathbf{1}$; mais $\mathbf{0} \not\equiv \mathbf{1}$, donc soit $\Phi_1 = \Phi_2 = \mathbf{0}$, soit $\Phi_1 = \Phi_2 = \mathbf{1}$.

   Si $n > 0$, alors Φ_1 s'écrit $A_n/\Phi_{11};\Phi_{12}$ ou Φ_2 s'écrit $A_n/\Phi_{21};\Phi_{22}$. Sans perte de généralité, supposons que Φ_1 s'écrive $A_n/\Phi_{11};\Phi_{12}$. Comme le RMO Φ_1 est réduit, $\Phi_{11} \neq \mathbf{0}$, donc par hypothèse de récurrence $\Phi_{11} \not\equiv \mathbf{0}$, c'est-à-dire $f(\Phi_{11}) \not\equiv \mathbf{0}$. Donc, par la question III.2, $f(\Phi_1)$ n'est pas indépendante de A_n. Comme $f(\Phi_1) \equiv f(\Phi_2)$ par hypothèse, $f(\Phi_2)$ n'est pas indépendante de A. En particulier, Φ_2 n'est ni $\mathbf{0}$ ni $\mathbf{1}$, donc Φ_2 est de la forme $B/\Phi_{21};\Phi_{22}$, où $A_n = B$ ou $A_n < B$ ($B < A_n$ est exclu parce que par hypothèse A_n est la plus petite des variables apparaissant dans Φ_1 ou Φ_2). Mais forcément $A_n = B$, parce que sinon les seules variables libres de Φ_2 seraient supérieures à A_n, et $f(\Phi_2)$ serait donc indépendante de A_n.

   Maintenant, $f(\Phi_1) \equiv f(\Phi_2)$ implique $(f(\Phi_{11}) \wedge A) \oplus f(\Phi_{12}) \equiv (f(\Phi_{21}) \wedge A) \oplus f(\Phi_{22})$, et comme A n'est libre dans aucun des Φ_{ij}, $1 \leq i,j \leq 2$, par unicité (question III.1), $f(\Phi_{11}) \equiv f(\Phi_{21})$ et $f(\Phi_{12}) \equiv f(\Phi_{22})$, c'est-à-dire $\Phi_{11} \equiv \Phi_{21}$ et $\Phi_{12} \equiv \Phi_{22}$. Par hypothèse de récurrence, on en déduit que $\Phi_{11} = \Phi_{21}$ et $\Phi_{12} = \Phi_{22}$, donc que $\Phi_1 = \Phi_2$.

4. (3) Écrire des fonctions $+$ et $*$ prenant deux RMO en argument et retournant un RMO telles que $f(\Phi_1 + \Phi_2) \equiv f(\Phi_1) \oplus f(\Phi_2)$ et $f(\Phi_1 * \Phi_2) \equiv f(\Phi_1) \wedge f(\Phi_2)$, et en déduire un algorithme de construction du RMO représentant une formule donnée. (Autrement dit, trouver une fonction f^{-1} qui à toute formule F associe un RMO $f^{-1}(F)$, tel que $f(f^{-1}(F)) \equiv F$.)

   Définissons d'abord la fonction de construction d'un nouveau nœud: $RMOmake(A, \Phi_1, \Phi_2)$ *retourne* $A/\Phi_1; \Phi_2$ *si* $\Phi_1 \neq \mathbf{0}$, *et* Φ_2 *sinon.*

   Définissons ensuite la fonction de négation d'un RMO, par récurrence sur le nombre de variables libres dans l'argument: $RMOneg(\mathbf{0}) = \mathbf{1}$, $RMOneg(\mathbf{1}) = \mathbf{0}$, *et* $RMOneg(A/\Phi_1; \Phi_2) = RMOmake(A, \Phi_1, RMOneg(\Phi_2))$.

   On définit + par récurrence sur le nombre de variables libres dans ses deux arguments:

   - $\mathbf{0} + \Phi = \Phi$;
   - $\Phi + \mathbf{0} = \Phi$;
   - *(On peut aussi rajouter la clause:* $\Phi + \Phi = \mathbf{0}$, *qui accélère le calcul dans les cas où on tombe dessus;)*
   - $\mathbf{1} + \Phi = RMOneg(\Phi)$;
   - $\Phi + \mathbf{1} = RMOneg(\Phi)$;
   - *Si* $\Phi_1 = A_1/\Phi_{11}; \Phi_{12}$ *et* $\Phi_2 = A_2/\Phi_{21}; \Phi_{22}$, *alors* $\Phi_1 + \Phi_2$ *vaut:*
     - $RMOmake(A_1, \Phi_{11}, \Phi_{12} + \Phi_2)$ *si* $A_1 < A_2$;
       (justifié par le fait que $f(A_1/\Phi_{11}; \Phi_{12}) \oplus f(\Phi_2) \equiv ((f(\Phi_{11}) \wedge A_1) \oplus f(\Phi_{12})) \oplus f(\Phi_2) \equiv (f(\Phi_{11}) \wedge A_1) \oplus (f(\Phi_{12}) \oplus f(\Phi_2)) \equiv f(A_1/\Phi_{11}; (\Phi_{12} + \Phi_2))$*)*
     - $RMOmake(A_2, \Phi_{21}, \Phi_1 + \Phi_{22})$ *si* $A_2 < A_1$; *(symétriquement)*
     - $RMOmake(A_1, \Phi_{11} + \Phi_{21}, \Phi_{12} + \Phi_{22})$ *si* $A_1 = A_2$
       (justifié par $f(A_1/\Phi_{11}; \Phi_{12}) \oplus f(A_1 \Phi_{21}; \Phi_{22}) \equiv ((f(\Phi_{11}) \wedge A_1) \oplus f(\Phi_{12})) \oplus ((f(\Phi_{21}) \wedge A_1) \oplus f(\Phi_{22})) \equiv ((f(\Phi_{11}) \oplus f(\Phi_{21})) \wedge A_1) \oplus (\Phi_{12} \oplus \Phi_{22})$*).*

   On définit de même $*$ *:*

   - $\mathbf{0} * \Phi = \mathbf{0}$;
   - $\mathbf{1} * \Phi = \Phi$;
   - $\Phi * \mathbf{0} = \mathbf{0}$;
   - $\Phi * \mathbf{1} = \Phi$;
   - *(*$\Phi * \Phi = \Phi$ *optionnellement);*
   - *Si* $\Phi_1 = A_1/\Phi_{11}; \Phi_{12}$ *et* $\Phi_2 = A_2/\Phi_{21}; \Phi_{22}$, *alors* $\Phi_1 * \Phi_2$ *vaut:*
     - $RMOmake(A_1, \Phi_{11} * \Phi_2, \Phi_{12} * \Phi_2)$ *si* $A_1 < A_2$;
       (justifié par le fait que $f(A_1/\Phi_{11}; \Phi_{12}) \wedge f(\Phi_2) \equiv ((f(\Phi_{11}) \wedge A_1) \oplus f(\Phi_{12})) \wedge f(\Phi_2) \equiv (f(\Phi_{11}) \wedge f(\Phi_2) \wedge A_1) \oplus (f(\Phi_{12}) \wedge f(\Phi_2)) \equiv f(A_1/(\Phi_{11} * \Phi_2); (\Phi_{12} * \Phi_2))$*)*
     - $RMOmake(A_2, \Phi_1 * \Phi_{21}, \Phi_1 * \Phi_{22})$ *si* $A_2 < A_1$; *(symétriquement)*
     - $RMOmake(A_1, (\Phi_{11} * \Phi_{21}) + (\Phi_{12} * \Phi_{21}) + (\Phi_{11} * \Phi_{22}), \Phi_{12} * \Phi_{22})$ *si* $A_1 = A_2$
       (justifié par $f(A_1/\Phi_{11}; \Phi_{12}) \wedge f(A_1 \Phi_{21}; \Phi_{22}) \equiv ((f(\Phi_{11}) \wedge A_1) \oplus f(\Phi_{12})) \wedge ((f(\Phi_{21}) \wedge A_1) \oplus f(\Phi_{22})) \equiv (f(\Phi_{11}) \wedge f(\Phi_{21}) \wedge A_1) \oplus (f(\Phi_{12}) \wedge f(\Phi_{21}) \wedge A_1) \oplus (f(\Phi_{11}) \wedge f(\Phi_{22}) \wedge A_1) \oplus (f(\Phi_{12}) \wedge f(\Phi_{22})) \equiv (((f(\Phi_{11}) \wedge f(\Phi_{21})) \oplus (f(\Phi_{12}) \wedge f(\Phi_{21})) \oplus (f(\Phi_{11}) \wedge f(\Phi_{22}))) \wedge A_1) \oplus (f(\Phi_{12}) \wedge f(\Phi_{22}))$*).*

   L'allocation de $A/\Phi_1; \Phi_2$ *est, comme pour les BDD, faite par hash-consing, et les fonctions* `RMOneg`, $+$ *et* $*$ *sont mémoïsées, c'est-à-dire que l'on maintient une table de hachage pour chaque qui évite de recalculer les résultats déjà calculés.*

   Le RMO d'une formule F *est alors calculé par récurrence structurelle sur* F *par:* $f^{-1}(\mathbf{0}) = \mathbf{0}$, $f^{-1}(\mathbf{1}) = \mathbf{1}$, $f^{-1}(F \oplus G) = f^{-1}(F) + f^{-1}(G)$, $f^{-1}(F \wedge G) = f^{-1}(F) * f^{-1}(G)$. *À la sortie* F *est satisfiable si et seulement si* $f^{-1}(F) \neq \mathbf{0}$.

5. (3) Soient F_1 et F_2 deux formules dans lesquelles A n'apparaît pas libre. Montrer que l'équation $(F_1 \wedge A) \oplus F_2 \equiv \mathbf{0}$ a une solution en A si et seulement si $(F_1 \wedge F_2) \oplus F_2 \equiv \mathbf{0}$, et qu'alors ses solutions sont exactement les formules équivalentes à $((F_1 \oplus \mathbf{1}) \wedge F) \oplus F_2$, pour F quelconque.

   En déduire un algorithme de $\mathcal{B}$-unification travaillant directement sur les RMO.

   Supposons que l'équation $(F_1 \wedge A) \oplus F_2 \equiv \mathbf{0}$ a une solution en A, c'est-à-dire qu'il existe une formule F telle que $(F_1 \wedge F) \oplus F_2 \equiv \mathbf{0}$. Alors $F_1 \wedge ((F_1 \wedge F) \oplus F_2) \equiv F_1 \wedge \mathbf{0} \equiv \mathbf{0}$. Mais $F_1 \wedge ((F_1 \wedge F) \oplus F_2) \equiv (F_1 \wedge (F_1 \wedge F)) \oplus (F_1 \wedge F_2)$ (par distributivité) $\equiv (F_1 \wedge F) \oplus (F_1 \wedge F_2)$. Donc $(F_1 \wedge F) \oplus (F_1 \wedge F_2) \equiv \mathbf{0} \equiv (F_1 \wedge F) \oplus F_2$ parce que F est solution de l'équation. Additionnons $(F_1 \wedge F) \oplus F_2$ de part et d'autre, il vient que $(F_1 \wedge F_2) \oplus F_2 \equiv \mathbf{0}$ par nilpotence de $\oplus$.

   Réciproquement, supposons que $(F_1 \oplus \mathbf{1}) \wedge F_2 \equiv \mathbf{0}$, et montrons que l'équation a alors une solution. Montrons en fait que la solution indiquée est effectivement une solution : si $A \equiv ((F_1 \oplus \mathbf{1}) \wedge F) \oplus F_2$, où F est une formule propositionnelle quelconque, $(F_1 \wedge A) \oplus F_2 \equiv (F_1 \wedge (((F_1 \oplus \mathbf{1}) \wedge F) \oplus F_2)) \oplus F_2 \equiv (F_1 \wedge ((F_1 \oplus \mathbf{1}) \wedge F)) \oplus (F_1 \wedge F_2) \oplus F_2$ (par distributivité) $\equiv (F_1 \wedge ((F_1 \wedge F) \oplus F)) \oplus (F_1 \wedge F_2) \oplus F_2$ (par distributivité) $\equiv (F_1 \wedge F_1 \wedge F) \oplus (F_1 \wedge F) \oplus (F_1 \wedge F_2) \oplus F_2$ (par distributivité) $\equiv (F_1 \wedge F) \oplus (F_1 \wedge F) \oplus (F_1 \wedge F_2) \oplus F_2$, (par idempotence de $\wedge$) $\equiv (F_1 \wedge F_2) \oplus F_2$ (par nilpotence de $\oplus$) $\equiv \mathbf{0}$ (par hypothèse).

   Montrons maintenant qu'il n'y a pas d'autre solution. Soit en effet F une solution de l'équation, c'est-à-dire $(F_1 \wedge F) \oplus F_2 \equiv \mathbf{0}$. Alors $((F_1 \oplus \mathbf{1}) \wedge F) \oplus F_2 \equiv (F_1 \wedge F) \oplus F \oplus F_2$ (par distributivité) $\equiv F$ (parce que F est solution de l'équation). Il s'ensuit que $F \equiv ((F_1 \oplus \mathbf{1}) \wedge F) \oplus F_2$, c'est-à-dire que F est bien de la forme demandée.

   On en déduit l'algorithme suivant. Étant donnés deux RMO Φ_1 et Φ_2, on souhaite trouver des substitutions ς les plus générales (à équivalence logique près) envoyant des variables propositionnelles vers des RMO, telles que $\Phi_1\varsigma = \Phi_2\varsigma$. (L'égalité portant sur les RMO, il s'agit bien de la représentation de la relation $\equiv$.) L'algorithme commence par produire le RMO $\Phi_1 + \Phi_2$, et tente de trouver les ς telles que $\Phi\varsigma = \mathbf{0}$. Si $\Phi = \mathbf{1}$, alors l'algorithme répond "non unifiable", sinon l'algorithme calcule $RMOzero(\Phi)$, qui est une substitution ς la plus générale telle que $\Phi\varsigma = \mathbf{0}$, de domaine inclus dans l'ensemble des variables libres de Φ. $RMOzero$ est défini par récurrence sur le nombre de variables dans son argument Φ — qui est un RMO différent de $\mathbf{1}$ —, comme suit :

   - *Si $\Phi = \mathbf{0}$, alors $RMOzero(\Phi)$ est la substitution identité (qui est bien la ς la plus générale telle que $\mathbf{0}\varsigma = \mathbf{0}$).*
   - *Sinon, Φ est de la forme $A/\Phi_1; \Phi_2$. Calculer $\varsigma' = RMOzero((\Phi_1 * \Phi_2) + \Phi_2)$ (la condition de solvabilité de l'équation; on notera que $(\Phi_1 * \Phi_2) + \Phi_2$ ne peut pas valoir $\mathbf{1}$, car sinon on aurait $\Phi_1 * ((\Phi_1 * \Phi_2) + \Phi_2) = \Phi_1$, soit après développement $\mathbf{0} = \Phi_1$, ce qui est exclu par la condition de normalisation des RMO. Donc* `RMOzero` *est applicable sur $(\Phi_1 * \Phi_2) + \Phi_2$).*

     Ensuite, les solutions de l'équation sont donc les $A\varsigma$ tels que $A\varsigma = ((\Phi_1\varsigma' + \mathbf{1}) * \Phi) + \Phi_2\varsigma'$, pour Φ un RMO quelconque. On pose donc $RMOzero(\Phi) = [((\Phi_1 + \mathbf{1}) * A') + \Phi_2/A]\varsigma'$, où A' est une nouvelle variable. (L'invariant selon lequel le domaine de ς ne lie que des variables libres dans Φ reste alors vérifié.)

   En fait, on peut même choisir pour A' la variable A elle-même. Les contraintes d'ordonnancement de variables font alors qu'on peut construire la solution comme $[(A/(\Phi_1 + \mathbf{1}); \Phi_2)/A]\varsigma'$.

   La composition de substitutions demande à effectuer des remplacements de variables par des RMO dans des RMO. Ceci s'effectue de façon similaire aux BDD. Mais il y a plus simple : on peut en effet laisser l'unificateur sous forme triangulaire, c'est-à-dire sous forme de la liste ordonnée des remplacements à faire, qui sont donc de la forme A remplacé par $A/(\Phi_1 + \mathbf{1}); \Phi_2$.

   On remarquera finalement que tout le développement de la partie III s'est fait en utilisant uniquement les lois algébriques des anneaux Booléens (la théorie $\mathcal{B}$), et est donc valable dans tous les anneaux Booléens, pas seulement celui des formules propositionnelles modulo $\equiv$. Ceci montre par exemple que la méthode s'étend aux anneaux Booléens enrichis de constantes a_1, a_2, ... (la technique fondée sur les univers de Herbrand quotient ne fonctionne plus dans ce cas-là). On peut même ajouter d'autres symboles de fonctions non constants, mais le problème d'unification devient plus complexe.