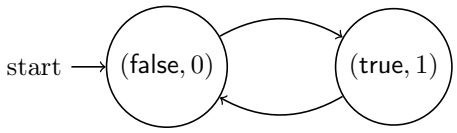
SAP — TD5 (corrigé) — *Model-checking*

18 mars 2011

1 États accessibles

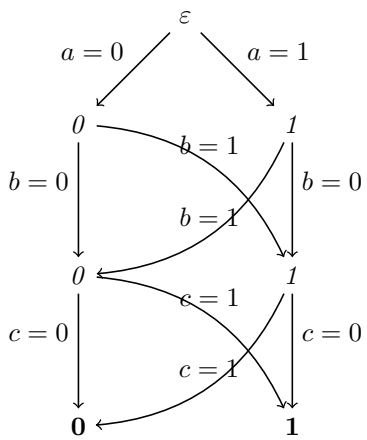
On peut énumérer manuellement l'ensemble des états accessibles (il n'y en a que deux) et construire l'automate fini correspondant :



2 BDD

2.1 Ou exclusif

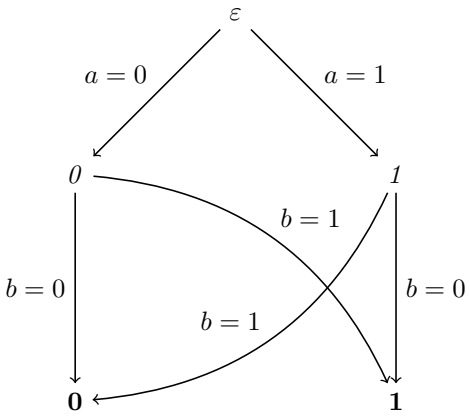
Les nœuds internes, étiquetés en italique, portent la valeur du ou-exclusif des arêtes menant de l'origine jusqu'au nœud (a, $a \oplus b$), les nœuds finaux, étiquetés en gras, portent la valeur de $a \oplus b \oplus c$.



On voit bien que l'on pourrait représenter la relation $a_1 \oplus \cdots \oplus a_n$ par un BDD à $2n - 1$ nœuds internes, plus les feuilles 0 et 1.

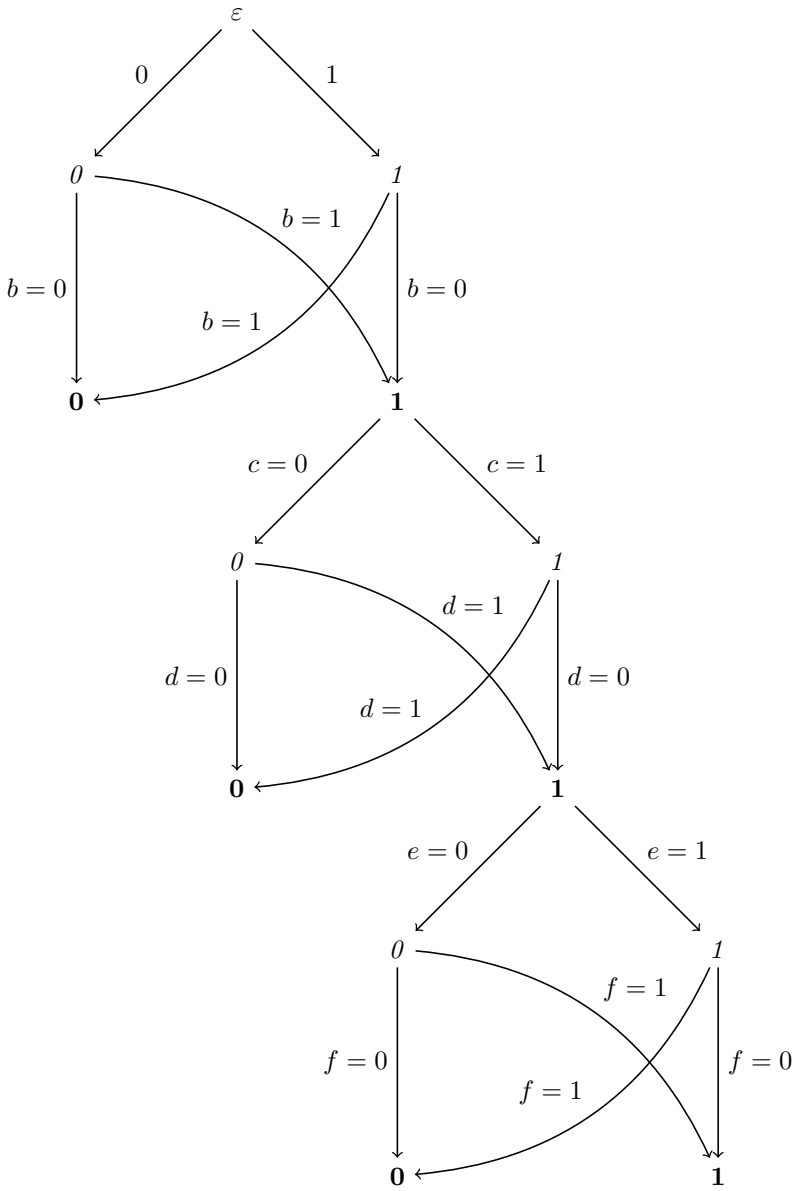
2.2 Formule en diamant

1. Un BDD réduit pour la relation $a \oplus b$ avec les variables dans l'ordre a, b est

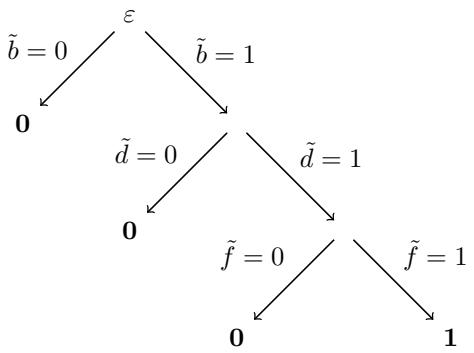


Pour construire un BDD réduit $(a \oplus b) \wedge (c \oplus d) \wedge (e \oplus f)$ avec les variables dans l'ordre (a, b, c, d, e, f), il suffit d'entasser ce BDD, une copie de ce BDD en remplaçant (a, b) par (c, d) et une copie de ce BDD en remplaçant (a, b) par (e, f), puis de remplacer les nœuds **1** par des liaisons sur le BDD suivant.

Par souci de clarté et de simplicité du tracé, le nœud **0** est représenté plusieurs fois.



2. Une fois fixées les valeurs de a, c, e, la relation $(a \oplus b) \wedge (c \oplus d) \wedge (e \oplus f)$ est équivalente à $\tilde{b} \wedge \tilde{d} \wedge \tilde{f}$ où $\tilde{b}$ est b si $a = \mathsf{false}$, $\neg b$ si $a = \mathsf{true}$, $\tilde{d}$ est d si $c = \mathsf{false}$, $\neg d$ si $c = \mathsf{true}$, $\tilde{f}$ est d si $e = \mathsf{false}$, $\neg f$ si $e = \mathsf{true}$. Cette relation $\tilde{b} \wedge \tilde{d} \wedge \tilde{f}$ se représente par le BDD réduit, pour l'ordre b, d, f :



Ce BDD comprend 3 nœuds internes plus les feuilles 0 et 1. Suivant les valeurs de a, c, e, il y a 8 BDD différents pour b, d, f. Il faut donc distinguer 8 cas pour a, c, e, ce qui nécessite 7 nœuds internes.

3. Pour représenter $(x_1 \oplus y_1) \wedge \cdots \wedge (x_n \oplus y_n)$ pour l'ordre $(x_1, y_1, \ldots, x_n, y_n)$, nous avons juste besoin d'empiler n BDD représentant $x_i \oplus y_i$, d'où une *complexité linéaire* en n.

   Pour représenter cette même fonction pour l'ordre $(x_1, \ldots, x_n, y_1, \ldots, y_n)$, chaque choix de $x_1, \ldots, x_n$ donne une fonction partielle en $y_1, \ldots, y_n$ différente, donc un BDD différent ; il faut donc distinguer 2^n choix. Le BDD a donc une *complexité exponentielle* en n.

   NB : Les bibliothèques de BDD, telles que CUDD, sélectionnent généralement elles-mêmes l'ordre des variables, à l'aide d'heuristiques. La détermination de l'ordre optimal est un problème NP-complet.

3 Points fixes

1. Soit Z_n l'ensemble des états accessibles en au maximum n pas, autrement dit l'ensemble des états σ_n tels qu'il existe un chemin $\sigma_0 \to \cdots \to \sigma_N$ avec $N \leq n$, $\sigma_0 \in \Sigma_0$ et $(\sigma_i, \sigma_{i+1}) \in \tau$ pour tout i.

   Montrons que $Z_n \subseteq Y_n$ par récurrence sur n. Le cas $n = 0$ est trivial. Supposons l'hypothèse valide au rang n. Soit $\sigma_0 \to \cdots \to \sigma_{N+1}$ avec $N \leq n$, $\sigma_0 \in \Sigma_0$ et $(\sigma_i, \sigma_{i+1}) \in \tau$ pour tout i. Alors $\sigma_N \in Z_n$ par définition de Z_n, donc $\sigma_N \in Y_n$ par l'hypothèse de récurrence, et donc $\sigma_{N+1} \in R(Y_n)$ par définition de R. Au final, $\sigma_{N+1} \in Z_{n+1}$.

   Montrons que $Y_n \subseteq Z_n$ par récurrence sur n. Le cas $n = 0$ est trivial. Supposons l'hypothèse valide au rang n. Soit $\sigma \in Y_{n+1} = \Sigma_0 \cup R(Y_n)$. Premier cas : $\sigma \in \Sigma_0$, trivial. Deuxième cas : $\sigma \in R(Y_n)$, il existe donc $\sigma' \in Y_n$ tel que $(\sigma', \sigma) \in \tau$. Par hypothèse de récurrence, il existe $\sigma_0 \to \cdots \to \sigma_N = \sigma'$ avec $\sigma_0 \in \Sigma_0$, $N \leq n$ et $(\sigma_i, \sigma_{i+1}) \in \tau$ pour tout $i < N$. Le résultat s'ensuit.

2. La preuve $Z_n \subseteq Y_n$ par récurrence sur n est identique à celle du point précédent.

   Montrons que $Y_n \subseteq Z_n$ par récurrence sur n. Le cas $n = 0$ est trivial. Supposons l'hypothèse valide au rang n. Soit $\sigma \in Y_{n+1} = Y_n \cup R(Y_n)$. Deux cas : $\sigma \in Y_n$ et $\sigma \in R(Y_n)$. Dans le premier cas, on conclut immédiatement à l'aide de l'hypothèse de récurrence. Le second cas se traite comme au point précédent.

3. L'ensemble des points fixes de f, $\{X \mid f(X) \leq X\}$, est inclus dans $\{X \mid f(X) \leq X\}$, donc la borne inférieure L de ce dernier ensemble minore tout point fixe de f.

   Montrons maintenant que L est un point fixe de f. Soit X tel que $f(X) \leq X$; alors $L \leq X$. Par monotonie, $f(L) \leq f(X)$, donc $f(L) \leq X$. $f(L)$ minore donc $\{X \mid f(X) \leq X\}$, donc $f(L) \leq L$ car L est le plus grand des minorants. Par monotonie, $f(f(L)) \leq f(L)$, donc $f(L)$ appartient à $\{X \mid f(X) \leq X\}$ dont L est un minorant, donc $L \leq f(L)$. On a donc $L = f(L)$.

4. Si $f \leq g$, alors $\{X \mid f(X) \leq X\} \supseteq \{X \mid g(X) \leq X\}$. On conclut en utilisant le fait que si $A \supseteq B$, alors $\inf A \mathit{leq} \inf B$.