La "Model Elimination" de D.W.Loveland expliquée

Michel Lévy

22 mars 2016

Table des matières

La méthode "Model Elimination" est une méthode de preuve très simple à programmer, ce qui a fait son succès. Nous utilisons pour la présenter les références suivantes [OD97], [Don78] et [Sut12]. Le dernier document présente de façon claire et concise la production des lemmes, sans cette aide, je ne serais pas parvenu à rédiger cette explication de la méthode de D.W.Loveland.

1 Bases de la méthode

L'opposé du littéral L est $\neg L$ si L est un atome, et M si $L = \neg M$. Dans la suite, on note par $\overline{L}$, l'opposé du littéral L.

Une chaine est une liste de B-littéraux et de A-littéraux (appelés aussi littéraux ancêtres). Un A-littéral est représenté par un littéral entre crochets. Un B-littéral est un littéral au sens usuel. La liste vide est notée $\square$.

Une chaine élémentaire est une liste de B-littéraux.

Une chaine est acceptable si elle commence (à sa gauche) par un B-littéral.

Sur les chaines, on définit trois opérations, la réduction, l'expansion et l'enlèvement.

Afin de faciliter la compréhension de la méthode appelée "Model Elimination" (en abrégé ME), nous en donnerons la version pour la logique propositionnelle et la version pour la logique du premier ordre.

1.1 La ME pour la logique propositionnelle

Expansion : Soit Γ un ensemble de chaînes élémentaires.

Soit LU une chaine *acceptable* où L est le B-littéral à gauche de la chaine.

Soit $V\overline{L}W$ une chaine élément de Γ. Alors la chaine $VW[L]U$ est obtenue par *expansion* de la chaîne LU à partir de Γ.

Réduction : Soit $LU[\overline{L}]V$ une chaine acceptable, où L est un B-littéral. La chaine $U[\overline{L}]V$ est obtenue par réduction de la chaine $LU[\overline{L}]V$.

Enlèvement : Soit $[L]U$ une chaine commençant par le A-littéral $[L]$. La chaine U est obtenue par enlèvement sur la chaine $[L]U$

Définition 1 (Dérivation) *Soit Γ un ensemble de chaines élémentaires, une dérivation à partir de Γ est une suite de chaines C_i où $1 \leq i \leq n$ telle que $C_1 \in \Gamma$ et pour i de 1 à $n-1$, la chaine C_{i+1} est obtenue par une expansion de la chaine C_i à partir de Γ, par une réduction de la chaine C_i ou par un enlèvement sur la chaine C_i.*
Une chaine est dérivable à partir de Γ s'il y a une dérivation à partir de Γ terminée par cette chaine.

Soit K une chaine. On lui associe une formule normale $fn(K)$, qui donne le *sens* de la chaine.

Définition 2 (Forme normale d'une chaine)

- $fn(\Box) = \bot$ *où* $\bot$ *est la formule toujours fausse.*
- $fn(UL) = fn(U) + L$ *où* $+$ *est la disjonction, L est un B-littéral et U une chaine.*
- $fn(U[L]) = fn(U) * L$ *où* $*$ *est la conjonction, $[L]$ est un A-littéral et U une chaine.*

Notons que, d'après cette définition, une chaine élémentaire est une disjonction de ses B-littéraux.

Quand il n'y a pas d'ambiguïté, on identifie une chaine et la formule normale qui lui est associée. Prenons un exemple. Soit L un littéral, $fn([L]) = fn(\Box) * L = \bot * L$. Par suite, la formule $fn([L])$ est équivalente à $\bot$, qui est le sens de la chaine vide. Quand cela ne crée pas d'ambuïguité, l'équivalence et l'égalité entre formules et chaines sont confondues, donc on se permet d'écrire $[L] = \Box$.

Nous montrons ci-dessous que les chaines dérivées de Γ en sont des conséquences (dans le sens de la conséquence logique). Cette propriété est appelée la cohérence de la méthode.

Au cours d'une dérivation, on peut créer des lemmes, qui sont des chaines élémentaires conséquences de Γ. Il est clair que pour obtenir des conséquences de Γ, on peut utiliser des expansions à partir de Γ et à partir des lemmes créés au cours des dérivations à partir de Γ.

Dans les ouvrages [OD97] et [Don78], l'enlèvement est incorporé aux deux autres opérations. À la fin d'une expansion ou d'une réduction, on effectue tous les enlèvements nécessaires pour obtenir à nouveau une chaine acceptable. Mais il m'a paru utile, en suivant l'exemple de [Sut12], de distinguer cette opération pour faciliter la compréhension de la création et de l'utilisation des lemmes.

Lemme 3 (monotonie des chaines) *Soient U, U', V trois chaines. Soit Γ un ensemble de formules. Supposons que $\Gamma \models U \Rightarrow U'$. Alors $\Gamma \models UV \Rightarrow U'V$.*

Preuve : Supposons que $\Gamma \models U \Rightarrow U'$.
Montrons la conclusion par récurrence sur la longueur de V.
Si V est la chaine vide, c'est évident.
Supposons que $V = WL$ où L est un littéral.
Par hypothèse de récurrence, $\Gamma \models UW \Rightarrow U'W$.
Par définition du sens des chaines, $UWL = (UW) + L$ et $U'WL = (U'W) + L$.
À cause de la monotonie de la disjonction, $\Gamma \models (UW) + L \Rightarrow (U'W) + L$,
donc $\Gamma \models UWL \Rightarrow U'WL$.
Le cas où $V = W[L]$ est analogue, car la conjonction est aussi monotone. □

Corollaire 4 (monotonie des chaines) *Soient U, U', V trois chaines. Soit Γ un ensemble de formules. Supposons que $\Gamma \models U = U'$. Alors $\Gamma \models UV = U'V$.*

Ce corollaire est une conséquence immédiate du lemme précédent, car l'équivalence $U = U'$ est la conjonction de $U \Rightarrow U'$ et $U' \Rightarrow U$.

Lemme 5 (cohérence de l'enlèvement) *Soit L un littéral et U une chaine. On a : $[L]U = U$*

Preuve : On a vu ci-dessus que $[L] = \square$. D'après le corollaire 4, $[L]U = U$ □

Lemme 6 (cohérence de la réduction) *Soit L un littéral et U, V deux chaines. On a $\models LU[\bar{L}]V \Rightarrow U[\bar{L}]V$.*

Preuve : D'après le sens des chaines, $LU[\bar{L}] = (LU) * \bar{L}$.
D'après le sens de la négation, $\bar{L} \models L \Rightarrow \square$.
D'après le lemme 3 de monotonie, $\bar{L} \models LU \Rightarrow U$.
Par suite $LU[\bar{L}] \models U$ et $LU[\bar{L}] \models \bar{L}$, donc $LU[\bar{L}] \models U * \bar{L}$.
Puisque $U * \bar{L} = U[\bar{L}]$, et d'après les propriétés de la conséquence, $\models LU[\bar{L}] \Rightarrow U[\bar{L}]$.
D'après le lemme 3,$\models LU[\bar{L}]V \Rightarrow U[\bar{L}]V$. □

Lemme 7 (cohérence de l'expansion) *Soit Γ un ensemble de chaines élémentaires. Soit K une chaine donnant par expansion avec Γ la chaine K'.*
On a : $\Gamma \models K \Rightarrow K'$.

Preuve : Par définition de l'expansion, il y un littéral L et une chaine U telle que $K = LU$. Il y a une chaine de Γ qui s'écrit $V\bar{L}W$ et $K' = VW[L]U$.
La chaine élémentaire $V\bar{L}W$ est équivalente à $L \Rightarrow VW$.
Par suite $\Gamma \models L \Rightarrow VW$, donc $\Gamma \models L \Rightarrow VW * L$.
D'après le sens des chaines, $(VW) * L = VW[L]$, donc $\Gamma \models L \Rightarrow VW[L]$.
Par le lemme 3, on en déduit $\Gamma \models K \Rightarrow K'$. □

Théorème 8 (cohérence de la méthode) *Soit Γ un ensemble de chaines élémentaires et K une chaine dérivable de Γ. On a : $\Gamma \models K$.*

Preuve : Soit K_i où $1 \leq i \leq n$ une dérivation (voir 1) de K à partir de Γ.
Puisque $K_1 \in \Gamma$, on a $\Gamma \models K_1$.
Des lemmes 7, 6, 5, il résulte que : pour tout i entre 1 et $n-1$, $\Gamma \models K_i \Rightarrow K_{i+1}$.
Donc par récurrence sur la longueur des dérivations :
pour tout i où $1 \leq i \leq n$, $\Gamma \models K_i$.
Puisque K est la dernière chaine de la dérivation, $\Gamma \models K$. $\square$

Corollaire 9 (preuve d'insatisfaisabilité) *Soit* Γ *un ensemble de chaines élémentaires. Si* $\square$ *est dérivable de* Γ *alors* Γ *est insatisfaisable.*

Preuve : Supposons $\square$ dérivable de Γ. Alors d'après le théorème ci-dessus, $\Gamma \models \square$. Puisque $\square$ est la formule fausse (n'ayant aucun modèle), Γ n'a aucun modèle. $\square$

1.2 La ME pour la logique du premier ordre

Expansion : Soit Γ un ensemble de chaînes élémentaires.

Soit LU une chaine *acceptable* où L est le B-littéral à gauche de la chaine.

Soit VMW une *copie* d'une chaine élément de Γ, dont les variables *ne figurent pas* dans LU.

Supposons qu'il existe σ un unificateur *principal* de L et de l'opposé du littéral M. Alors la chaine $(VW[L]U)\sigma$ est obtenue par *expansion* de la chaîne LU à partir de Γ.

Réduction : Soit $LU[M]V$ une chaine acceptable, où L est le littéral le plus à gauche de la chaine et $[M]$ un littéral ancêtre, tel qu'il y a un unificateur principal σ entre L et l'opposé de M alors la chaine $(U[M]V)\sigma$ est obtenue par réduction de la chaine $LU[M]V$.

Enlèvement : Soit $[L]U$ une chaine commençant par le A-littéral $[L]$. La chaine U est obtenue par enlèvement sur la chaine $[L]U$

La fermeture universelle d'une formule A est notée $\forall(A)$. C'est la formule obtenue en quantifiant universellement toutes les variables libres de A.

Soit Γ un ensemble de formules. La fermeture universelle de Γ, notée $\forall(\Gamma)$ est l'ensemble des fermetures universelles des formules de Γ.

Dans la suite nous utilisons la notion de conséquence (logique) dans son sens le plus usuel. Une formule est conséquence d'un ensemble de formules, si tout modèle de l'ensemble (donnant des valeurs aux symboles de relations et de fonctions, *ainsi qu'aux variables*) est modèle de la formule.

Avec cette notion de conséquence $\forall x P(x) \models P(x)$, mais $P(x) \not\models \forall x P(x)$.

Nous verrons que les chaines dérivables d'un ensemble Γ de chaines élémentaires sont conséquences de $\forall(\Gamma)$: c'est cette propriété qui est, pour la logique du premier ordre, appelée la cohérence de la méthode. Au cours d'une dérivation, on peut créer des lemmes, qui sont des chaines élémentaires conséquences de $\forall(\Gamma)$. Il est clair que pour obtenir des conséquences de la fermeture universelle de Γ, on peut utiliser des expansions à partir de Γ et à partir des lemmes créés au cours des dérivations à partir de Γ.

Soit σ une substitution. On note $A\sigma$ la formule obtenue en remplaçant toutes les variables libres de A par leur valeur dans la substitution. Lorsque la formule A n'a pas de quantificateurs, on a $\forall(A) \models A\sigma$.

Lemme 10 (cohérence de la réduction) *Soit K une chaine et K' une chaine obtenue par réduction de K. On a : $\models \forall(K) \Rightarrow \forall(K')$.*

Preuve : Par définition de la réduction, il y a deux littéraux L et M, deux chaines U et V, une substitution σ telle que $K = LU[M]V$, les littéraux $L\sigma$ et $M\sigma$ sont opposés et $K' = (U[M]V)\sigma$.

D'après les propriétés de la fermeture universelle, $\forall(K) \models (LU[M]V)\sigma$.
D'après la cohérence de la réduction pour la logique propositionnelle 6, puisque $M\sigma = \overline{L\sigma}$, nous avons : $\models (LU[M]V)\sigma \Rightarrow (U[M]V)\sigma$.
Donc $\forall(K) \models K'$. D'après les propriétés de la conséquence $\models \forall(K) \Rightarrow \forall(K')$. □

Lemme 11 (cohérence de l'expansion) *Soit Γ un ensemble de chaines élémentaires. Soit K une chaine donnant par expansion avec Γ la chaine K'.*
On a : $\forall(\Gamma) \models \forall(K) \Rightarrow \forall(K')$.

Preuve : Par définition de l'expansion, il y un littéral L et une chaine U telle que $K = LU$. Il y a une chaine de Γ qui s'écrit VMW et une substitution σ telle que $L\sigma$ et $M\sigma$ sont deux littéraux opposés et $K' = (VW[M]U)\sigma$.
Puisque les littéraux $L\sigma$ et $M\sigma$ sont opposés, la chaine élémentaire $(VMW)\sigma$ est équivalente à $L\sigma \Rightarrow (VW)\sigma$.
Par suite $\forall(\Gamma) \models L\sigma \Rightarrow (VW)\sigma$, donc $\forall(\Gamma) \models L\sigma \Rightarrow (VW)\sigma * L\sigma$.
D'après le sens des chaines, $(VW)\sigma * L\sigma = ((VW)[L])\sigma$, donc $\forall(\Gamma) \models L\sigma \Rightarrow ((VW)[L])\sigma$.
Par le lemme de monotonie 3, on en déduit $\forall(\Gamma) \models K\sigma \Rightarrow K'$.
D'après la propriété des fermetures universelles, $\forall(K) \models K\sigma$.
D'après les propriétés de la conséquence, $\forall(\Gamma), \forall(K) \models K'$.
Puisque les hypothèses sont sans variables libres, $\forall(\Gamma), \forall(K) \models \forall(K')$.
Et par suite $\forall(\Gamma) \models \forall(K) \Rightarrow \forall(K')$. □

Théorème 12 (cohérence de la méthode) *Soit Γ un ensemble de chaines élémentaires et K une chaine dérivable de Γ. On a : $\forall(\Gamma) \models \forall(K)$.*

Preuve : Soit K_i où $1 \leq i \leq n$ une dérivation (voir 1) de K à partir de Γ.
Puisque $K_1 \in \Gamma$ et d'après les propriétés de la conséquence, on a $\forall(\Gamma) \models \forall(K_1)$.
Des lemmes 11, 10, 5, il résulte que :
pour tout i entre 1 et $n-1$, $\forall(\Gamma) \models \forall(K_i) \Rightarrow \forall(K_{i+1})$.
Donc par récurrence sur la longueur des dérivations :
pour tout i où $1 \leq i \leq n$, $\forall(\Gamma) \models \forall(K_i)$.
Puisque K est la dernière chaine de la dérivation, $\forall(\Gamma) \models \forall(K)$. □

Corollaire 13 (preuve d'insatisfaisabilité) *Soit Γ un ensemble de chaines élémentaires. Si $\square$ est dérivable de Γ alors $\forall(\Gamma)$ est insatisfaisable.*

Preuve : Supposons $\square$ dérivable de Γ. Alors d'après le théorème ci-dessus, $\forall(\Gamma) \models \square$.
Puisque $\square$ est la formule fausse (n'ayant aucun modèle), $\forall(\Gamma)$ n'a aucun modèle. □

2 Production des lemmes dans le cas propositionnel

À chaque A-littéral d'une chaine, on associe un entier appelé la portée du littéral.

Lors d'une expansion, la portée du nouvel A-littéral est nulle.

Lors d'une réduction, la portée du A-littéral qui sert à effectuer la réduction *peut être modifiée*. Si le nombre de A-littéraux à gauche de ce A-littéral est plus grande que sa portée actuelle, sa portée *devient* ce nombre.

Lors de l'enlèvement d'un A-littéral, *un lemme* consistant en la négation tous les A-littéraux dont la portée est égale au nombre de A-littéraux à leur gauche est engendrée. Les portées non nulles de ces A-littéraux sont diminuées de 1.

Remarquons que, au cours d'une dérivation, la portée d'un A-littéral est au plus égale au nombre de A-littéraux à sa gauche. C'est vrai pour la première chaine d'une dérivation, car cette chaine n'a pas de A-littéral. Cette propriété est conservée lors de la création d'un A-littéral par expansion, car sa portée initiale est 0. Cette propriété est aussi conservée par réduction, puisque la portée du A-liitéral utilisée dans la réduction devient égale au nombre de A-littéraux à sa gauche et elle est aussi conservée par l'enlèvement d'un A-littéral.

De cette remarque, il résulte que lorsqu'on enlève le A-littéral $[L]$, sa portée est nulle, donc sa négation fait partie du lemme produit.

Pour faciliter la compréhension de la création des lemmes et la preuve de leur correction, on répète ce qui vient d'être dit, en redéfinissant les trois opérations expansion, réduction et enlèvement, en y ajoutant le calcul des portées nécessaire pour la création des lemmes.

Expansion : Soit Γ un ensemble de chaînes élémentaires.
Soit LU une chaine où L est le B-littéral à gauche de la chaine.
Soit $V\overline{L}W$ une chaine élément de Γ. La chaine $VW[L]U$ est obtenue par *expansion* de la chaîne LU à partir de Γ.
La portée du nouveau littéral ancêtre $[L]$ est nulle.

Réduction : Soit $LU[\overline{L}]V$ une chaine acceptable, où L est le B-littéral le plus à gauche de la chaine et $[\overline{L}]$ un littéral ancêtre. La chaine $U[\overline{L}]V$ est obtenue par réduction de la chaine $LU[\overline{L}]V$.
Si le nombre de A-littéraux strictement à gauche de ce littéral ancêtre est supérieur à sa portée avant réduction, cette portée devient égale à ce nombre.

Enlèvement : Soit $[L]U$ une chaine commençant par le A-littéral $[L]$. La chaine U est obtenue par enlèvement de la chaine $[L]U$.
Un lemme consistant en la négation de ce A-littéral et de tous les autres A-littéraux dont la portée est égale au nombre de A-littéraux à leur gauche est engendré. Les portées non nulles de ces A-littéraux sont diminuées de 1.

L'ajout des lemmes peut *faciliter ou compliquer* les dérivations. Elle peut les faciliter, parce l'usage d'un lemme évite de refaire la dérivation qui a produit ce lemme. Elle peut les compliquer, parce qu'on ajoute des lemmes trop nombreux et inutiles.

Il y a plusieurs politiques d'utilisation des lemmes. On peut les ajouter au cours d'une dérivation, ou lors de la construction d'un arbre des dérivations (une dérivation pouvant ajouter des lemmes utilisés dans une autre dérivation). On peut sélectionner les "meilleurs" lemmes, par exemple les plus courts. On peut remplacer des chaines d'entrées par des lemmes qui les subsument.

Nous n'entrerons pas dans cette politique d'usage des lemmes, qui a fait l'objet de beaucoup d'articles. Nous nous contenterons de prouver que les lemmes engendrés dans une dérivation sont bien des conséquences des chaines d'entrées de la dérivation.

Nous présentons une propriété des chaines, vérifiée par une chaine sans A-littéraux, et conservée par chaque étape expansion, réduction, enlèvement. Cette propriété est donc vérifiée par toute chaine dérivée et nous permet de prouver la correction des lemmes.

Définition 14 (Propriété des chaines dérivées) *Soit* Γ *un ensemble de chaines élémentaires et soit K une chaine. Il existe n, où* $n \geq 0$*, des littéraux* L_i *où* $1 \leq i \leq n$*, des entiers* k_i *où* $1 \leq i \leq n$*, où* k_i *est la portée du littéral* L_i*, et des chaines élémentaires* U_i *où* $1 \leq i \leq n+1$ *tels que* $K = U_1[L_1^{k_1}]...U_n[L_n^{k_n}]U_{n+1}$.

Soit C_i *l'ensemble de littéraux défini par* $C_i = \{L_j \mid i \leq j, j-i \leq k_j \leq j-1\}$. *On identifie cet ensemble avec la* conjonction *de ses éléments.*

K vérifie la propriété des chaines dérivées relativement à Γ *si pour i où* $1 \leq i \leq n$*,* $L_i \in C_i$ *et* $\Gamma \models C_i \Rightarrow U_1..U_i$.

Le A-literal $L_j^{k_j}$ est utilisé dans la réduction des descendants de L_{j-k_j}. Donc pour $k_j = j-1$ il est utilisé pour réduire des descendants de L_1 et pour $k_j = j-i$, il sert à réduire des descendants de L_i.

Ainsi C_i est l'ensemble des A-littéraux utilisés pour réduire un B-littéral descendant des A-littéraux $L_1, ...L_i$.

Je dois reconnaitre que j'étais incapable de comprendre la preuve de la correction des lemmes à la seule lecture du livre de D.W.Loveland [Don78]. C'est ce qui m'a poussé à rédiger cette *explication* de méthode ME. Le plus difficile fut de trouver la propriété des chaines qui est invariante au cours des dérivations et qui permet d'expliquer la correction des lemmes.

Lemme 15 (Invariance de la propriété des chaines dérivées) *Soit* Γ *un ensemble de chaines élémentaires et soit K une chaine vérifiant la propriété des chaines dérivées relativement à* Γ. *Alors cette même propriété est vérifiée par la chaine* K' *obtenue par expansion avec* Γ*, réduction ou enlèvement sur K.*

Le lemme produit lors de l'enlèvement est conséquence de Γ.

Preuve : Pour la chaine K, nous reprenons les notations de la propriété ci-dessus 14.

Puisque K' est une chaine, il existe p, où $p \geq 0$, des littéraux L'_i où $1 \leq i \leq p$, des entiers k'_i où $1 \leq i \leq p$, et des chaines élémentaires U'_i où $1 \leq i \leq p+1$ tels que $K' = U'_1[L'^{k'_1}_1]...U'_p[L'^{k'_p}_p]U'_{p+1}$.

Soit C'_i l'ensemble de littéraux défini par $C'_i = \{L'_j \mid i \leq j, j-i \leq k'_j \leq j-1\}$.

- Supposons que la chaine K' a été produite par expansion de K avec Γ.

  Supposons que K commence par le B-littéral L et que l'expansion a été produite avec la chaine $V\overline{L}W$ élément de Γ.

  Notons que $p = n+1$. Puisqu'un nouveau A-littéral $L'_1 = L$ a été ajouté, on a pour i où $2 \leq i \leq n+1$, $L'_i = L_{i-1}, U'_{i+1} = U_i$.

Puisque le marquage des portées ne change pas (sauf pour le nouvel A-littéral), nous avons pour i où $2 \leq i \leq n+1$, ${L'}_i^{k'_i} = L_{i-1}^{k_{i-1}}$. En clair la portée du i-ème A-littéral de K' est la même que la portée du $i-1$-ème littéral de K. Donc pour $2 \leq i \leq n+1$, on a : $C'_i = C_{i-1}$.
Puisque le nouveau A-littéral est introduit comme L'_1 avec la portée 0, par définition de C'_1, nous avons :
(a) : $L'_1 \in C'_1$
D'après les hypothèses sur K, pour i où $1 \leq i \leq n$, $L_i \in C_i$, nous avons :
pour i où $1 \leq i \leq n$, $L'_{i+1} \in C'_{i+1}$, donc, en remplaçant $i+1$ par j et $n+1$ par p, on a :
pour j où $2 \leq j \leq p$, $L'_j \in C'_j$. En y ajoutant la condition **(a)**, on obtient :
(b) : pour i où $1 \leq i \leq p$, $L'_i \in C'_i$
Ce qui est la première partie de la propriété que doit verifier K'. Il reste à vérifier que pour j où $1 \leq j \leq p$, $\Gamma \models C'_j \Rightarrow U'_1...U'_j$.
Vu les notations de K et K', on a $U_1 = LX$, $U'_1 = VW$, $U'_2 = X$. Rappelons que l'expansion a été réalisée sur le littéral L avec la chaine $V\overline{L}W$, qui est élément de Γ.
Puisque cette chaine est équivalente à $L \Rightarrow VW$, il en résulte que $\Gamma \models L \Rightarrow U'_1$ et par le lemme 3, que $\Gamma \models U_1 \Rightarrow U'_1U'_2$.
D'après la propriété des chaines dérivées de K, nous avons pour i où $1 \leq i \leq n$, $\Gamma \models C_i \Rightarrow U_1...U_i$.
D'après les correspondances déjà citées entre K et K', nous avons
(c) : pour i où $1 \leq i \leq n$, $\Gamma \models C'_{i+1} \Rightarrow U_1U'_3...U'_{i+1}$
Puisque $V\overline{L}W \in \Gamma$ et que cette chaine est équivalente à $L \Rightarrow VW$, nous avons $\Gamma \models L \Rightarrow VW$. Rappelons que $U_1 = LX, VW = U'_1, X = U'_2$. D'après le lemme de monotonie 3 :
(d) : $\Gamma \models U_1 \Rightarrow U'_1U'_2$.
De **(c)** et **(d)**, on déduit que pour i où $1 \leq i \leq n$, $\Gamma \models C'_{i+1} \Rightarrow U'_1U'_2U'_3...U'_{i+1}$
En remplaçant $i+1$ par j, on obtient : **(e) :** pour j où $2 \leq j \leq p$, $\Gamma \models C'_j \Rightarrow U'_1...U'_j$
Nous savons déjà que L'_1 est élément de la conjonction C'_1, donc $\Gamma \models C'_1 \Rightarrow U'_1$. Par suite pour j où $1 \leq j \leq p$, $\Gamma \models C'_j \Rightarrow U'_1...U'_j$ ce qui termine la preuve que K', obtenue par expansion de K, conserve la propriété des chaines dérivées.

- Supposons que K' ait été obtenue par réduction de K.

  Dans ce cas $p = n$, et les A-littéraux n'ont pas changé. Seule la partie U_1 de la chaine K a été modifiée. En résumé, pour i de 1 à n, $L'_i = L_i$ et pour i de 2 à $n+1$, $U'_i = U_i$.

  La chaine U_1 s'écrit LX et il y a un A-littéral L_i où $i \geq 1$ et $L_i = \overline{L}$ et $U'_1 = X$.

  Par définition de la réduction, la portée du littéral L'_i est égale à $i-1$ (le nombre de A-littéraux à gauche de L'_i) dans K'. Dans la suite nous réservons i comme l'indice du littéral ayant causé la réduction.

  Puisque pour tout j tel que $1 \leq j \leq n$ et $j \neq i$, $k_j = k'_j$ et que $k'_i = i-1$, nous avons pour tout j tel que $1 \leq j \leq n$, $C'_j = C_j \cup \{L_i\}$.

Puisque K verifie pour tout j tel que $1 \leq j \leq n$, $L_j \in C_j$, et que pour tout j tel que $1 \leq j \leq n$, $L'_j = L_j$ et $C'_j = C_j \cup \{L_i\}$, nous avons :
pour j tel que $1 \leq j \leq n$, $L'_j \in C'_j$ est une propriété vérifiée par K'.

Ainsi K' verifie la première partie de la propriété des chaines dérivées. Il reste à prouver que pour j de 1 à $n-1$, $\Gamma \models C'_j \Rightarrow U'_1...U'_j$.

Puisque $L_i = \overline{L}$ et que pour tout j tel que $1 \leq j \leq n$, $C'_j = C_j \cup \{L_i\}$, nous avons :
(a) : pour tout j où $1 \leq j \leq n$, $\models C'_j \Rightarrow \overline{L}$.

D'après le lemme 3, nous avons :
(b) :$\models \overline{L} \Rightarrow U_1 \Rightarrow U'_1$

Des propositions **(a)** et **(b)**, on déduit :
(c) : pour tout j où $1 \leq j \leq n$, $\models C'_j \Rightarrow U_1 \Rightarrow U'_1$.

Puisque, pour tout j, $C'_j = C_j \cup \{L_i\}$ et que ces ensembles sont considérés comme la conjonction de leurs éléments, nous avons, pour tout $1 \leq i \leq n$, $\models C'_i \Rightarrow C_i$.

Vu la propriété des chaines dérivées vérifiée par K, nous avons :
$\Gamma \models C_i \Rightarrow U_1...U_i$.

Puisque C'_i *implique* C_i, nous avons :
(d) :$\Gamma \models C'_i \Rightarrow U_1...U_i$.

D'après **(c)**, **(d)** et puisque pour $1 < i$, $U_i = U'_i$, nous avons :
pour tout i où $1 \leq i \leq n, \Gamma \models C'_i \Rightarrow U'_1...U'_i$.

Par suite la chaine K' dérivée par réduction de K, vérifie aussi la propriété des chaines dérivées.

- Supposons que la chaine K' ait été obtenue par enlèvement sur la chaine K.

  Nous montrons tout d'abord que lemme créé lors l'enlèvement est conséquence de Γ. Lors de l'enlèvement, $U_1 = \square$.

  D'après la propriété des chaines dérivées vérifiée par K, on a pour i où $1 \leq I \leq n$, $\Gamma \models C_i \Rightarrow U_1...U_i$.

  Par suite $\Gamma \models C_1 \Rightarrow \square$. Noter que C_1 est la *conjonction* (et l'ensemble) des littéraux L_i, dont la portée est $i-1$, c'est-à-dire le nombre de A-littéraux à gauche de L_i.

  La formule $C_1 \Rightarrow \square$ est équivalente à la *disjonction* des opposés de ces littéraux,représentée par la chaine élémentaire comportant la liste des opposés de ces littéraux. Le lemme engendré, lors de l'enlèvement, est donc bien une conséquence de Γ.

  La décrémentation des portées, *après* l'enlèvement du premier A-littéral de K, fait que les autres A-littéraux de K qui avaient leur portée égale au nombre de leur A-littéraux à gauche, restent les mêmes dans K'. Formellement, cela veut dire que là où nous avions $k_j = j-1$ dans K, nous avons $k'_{j-1} = j-2$ dans K'. Cette remarque implique que pour j tel que $2 \leq j \leq n$, $C_j = C'_{j-1}$.

  Dans le cas de l'enlèvement, $p = n-1$, $U_1 = \square$ et d'après notre notation de K', pour j de 2 à n, $L_j = L'_{j-1}$, pour j de 2 à $n+1$, $U_j = U'_{j-1}$.
  La chaine K verifie : pour j tel que $1 \leq j \leq n$, $L_j \in C_j$ et $\Gamma \models C_j \Rightarrow U_1...U_j$.
  Puisque $L_j = L'_{j-1}, C_j = C'_{j-1}, U_j = U'_{j-1}$ et $U_1 = \square$, nous avons pour j tel que $2 \leq j \leq n$, $L'_{j-1} \in C'_{j-1}$ et $\Gamma \models C'_{j-1} \Rightarrow U'_1...U'_{j-1}$

En remplaçant $j-1$ par k et sachant $p = n-1$, nous concluons que : pour k tel que $1 \leq k \leq p$, $L'_k \in C'_k$ et $\Gamma \models C'_k \Rightarrow U'_1 \ldots U'_k$.

Ainsi l'enlèvement conserve bien la propriété des chaines dérivées.

□

Théorème 16 *Soit* Γ *un ensemble de chaines élémentaires. Toutes les chaines K d'une dérivation à partir de* Γ *vérifie la propriété des chaines dérivées 14 et les lemmes produits au cours de cette dérivation sont conséquences de* Γ.

Preuve : La chaine à l'origine d'une dérivation, n'ayant aucun A-littéral, vérifie la propriété des chaines dérivées. Cette propriété étant préservée par chaque étape d'une dérivation d'après 15, toutes les chaines de la dérivation la vérifient.

Lors d'un enlèvement sur une chaine vérifiant la propriété des chaines dérivées 14, le lemme produit est conséquence de Γ. Puisque toutes les chaines d'une dérivation vérifient cette propriété, lors de chaque enlèvement au cours de la dérivation, les lemmes produits sont conséquences de Γ. □

3 Production des lemmes en logique du premier ordre

Le marquage des portées est presque le même que dans le cas propositionnel. Lors d'une expansion, la portée du nouvel A-littéral est nulle. Lors d'une réduction, la portée du A-littéral qui sert à effectuer la réduction *peut être modifiée*. Si le nombre de A-littéraux à gauche de ce A-littéral est plus grande que sa portée actuelle, sa portée *devient* ce nombre. Lors de l'enlèvement d'un A-littéral, *un lemme* consistant en les opposés de tous les A-littéraux dont la portée est égale au nombre de A-littéraux à leur gauche est engendrée. Les portées non nulles de ces A-littéraux (sauf évidemment celui qui a été enlevé) sont diminuées de 1. Pour éviter toute ambiguïté on redéfinit les trois opérations expansion, réduction et enlèvement, en y ajoutant le calcul des portées nécessaire pour la création des lemmes.

Expansion : Soit Γ un ensemble de chaînes élémentaires.
Soit LU une chaine *acceptable* où L est le B-littéral à gauche de la chaine.
Soit VMW une *copie* d'une chaine élément de Γ, dont les variables *ne figurent pas* dans LU.
Supposons qu'il existe σ un unificateur *principal* de L et de l'opposé du littéral M. Alors la chaine $(VW[L]U)\sigma$ est obtenue par *expansion* de la chaîne LU à partir de Γ.
La portée du nouveau littéral ancêtre $[L\sigma]$ est nulle.
Notons aussi que les portées définies dans U et dans $U\sigma$ sont conservées, plus précisement la portée du i-ème littéral de la chaine U et la chaine $U\sigma$ sont identiques, en bref les portées sont préservées par substitution.

Réduction : Soit $LU[M]V$ une chaine acceptable, où L est le B-littéral le plus à gauche de la chaine et $[M]$ un littéral ancêtre, tel qu'il y a un unificateur principal σ entre L et l'opposé de M alors la chaine $(U[M]V)\sigma$ est obtenue par réduction de la chaine $LU[M]V$.

Si le nombre de A-littéraux strictement à gauche de ce littéral ancêtre est supérieur à sa portée avant réduction, cette portée devient égale à ce nombre.

Comme pour l'expansion, les portées des autres A-littéraux sont préservées par substitution.

Enlèvement : Soit $[L]U$ une chaine commençant par le A-littéral $[L]$. La chaine U est obtenue par enlèvement de la chaine $[L]U$.

Un lemme consistant en la négation de ce A-littéral et de tous les autres A-littéraux dont la portée est égale au nombre de A-littéraux à leur gauche est engendré. Les portées non nulles de ces A-littéraux sont diminuées de 1.

Nous ne faisons pas dans le cas du premier ordre, toutes les preuves nécessaires pour assurer la correction des lemmes. Nous donnons seulement la propriété des chaines dérivées, invariante au cours des dérivations et nous admettons cette invariance. Dans la propriété de la chaine dérivée, on constate que la seule différence avec le cas propositionnel est le remplacement de Γ par sa fermeture universelle $\forall(\Gamma)$.

La preuve de l'invariance de la propriéte ci-dessous, à chaque étape d'une dérivation, est analogue au cas propositionnel, compliquée par les substitutions. Nous laissons cette preuve au lecteur courageux.

Définition 17 (Propriété des chaines dérivées) *Soit Γ un ensemble de chaines élémentaires et soit K une chaine.*

Il existe n, où $n \geq 0$, des littéraux L_i où $1 \leq i \leq n$, des entiers k_i où $1 \leq i \leq n$, où k_i est la portée du littéral L_i, et des chaines élémentaires U_i où $1 \leq i \leq n+1$ telles que $K = U_1[L_1^{k_1}]...U_n[L_n^{k_n}]U_{n+1}$.

Soit C_i l'ensemble de littéraux défini par $C_i = \{L_j \mid i \leq j, j-i \leq k_j \leq j-1\}$. On identifie l'ensemble C_i avec la conjonction *de ses éléments.*

K vérifie la propriété des chaines dérivées relativement à Γ si pour i où $1 \leq i \leq n$, $L_i \in C_i$ et $\forall(\Gamma) \models C_i \Rightarrow U_1..U_i$.

Théorème 18 *Soit Γ un ensemble de chaines élémentaires. Tout lemme produit durant une dérivation à partir de Γ est une conséquence of $\forall(\Gamma)$.*

Preuve : Soit K une chaine dérivée de Γ, commençant par un A-littéral. Le lemme produit par l'enlèvement de cet A-littéral est la chaine élémentaire composée par les opposés des A-littéraux de la chaine dont la portée est égale au nombre de A-littéraux à leur gauche.

D'après l'invariance de la propriété des chaines dérivées, nous savons que K vérifie cette propriété. Donc $\forall(\Gamma) \models C_1 \Rightarrow \Box$, où C_1 est la conjonction des A-littéraux de la chaine, dont la portée est égale au nombre de littéraux à leur gauche. Le lemme engendré est équivalent à la formule $C_1 \Rightarrow \Box$, donc il est conséquence de $\forall(\Gamma)$.

$\Box$

Conclusion : Ce qui rend la lecture du livre de Loveland [OD97] si difficile, est qu'il n'a pas séparé le cas propositionnel et le cas du premier ordre. En effectuant cette séparation, j'espère avoir *expliqué* brièvement et clairement la méthode Model Elimination notamment en montrant pourquoi les lemmes engendrés par cette méthode sont corrects.

Références

[Don78] Donald.W.Loveland. *Automated Theorem Proving : A Logical Basis*. North-Holland, 1978.

[OD97] O.L.Astrachan and D.W.Loveland. The use of lemmas in the model elimination procedure. *Journal of Automated Reasoning*, 19 :117–141, 1997.

[Sut12] Geoff Sutcliffe. Chain format linear refinements. `http://www.cs.miami.edu/home/geoff/Courses/CSC648-12S/Content/ChainFormat.shtml`, 2012.