Sémantique et calcul syntaxique pour les formules booléennes quantifiées

Igor Stéphan

LERIA, Université d'Angers, 2 Boulevard Lavoisier, 49045, Angers, Cedex 01, France
igor.stephan@info.univ-angers.fr

Résumé

Nous revisitons la sémantique des formules booléennes quantifiées et étudions une relation d'équivalence qui en préserve les modèles. Nous proposons un calcul syntaxique pour les formules booléennes quantifiées basé sur le concept de relation de formules et mettons en exergue le lien avec la relation d'équivalence étudiée prouvant ainsi la correction et la complétude.

1 Introduction

Le formalisme des formules booléennes quantifiées a été introduit initialement dans [18] puis largement approfondi dans [27]. A l'origine, ce formalisme qui décrit une « hiérarchie » de langages était un outil théorique pour explorer des classes de complexité au-delà de la célèbre classe NP mais il est devenu depuis [9, 10] un domaine de recherche plus appliqué qui a vu l'implantation de multiples procédures de décision et son utilisation dans de nombreux domaines de l'intelligence artificielle (par exemple en planification [22, 1] et en implantation de procédures de décision [5]) et dans la vérification formelle de circuit (voir [4] pour un florilège). La plus grande part des procédures de décision récentes pour la validité des QBF [10, 28, 17, 16] sont des extensions de l'algorithme de recherche de Davis, Logemann et Loveland [12] pour le problème de la satisfiabilité booléenne ; d'autres sont basées sur le principe de résolution [23] telle que la Q-resolution [7] ou Quantor [6] (qui combine cette dernière avec l'expansion) ; d'autres sont basées sur l'élimination des quantificateurs à la Fourier-Motzkin [20, 19] ; d'autres enfin, sans être exhaustif, sur la skolémisation [2]. La sémantique des QBF est généralement présentée soit dans sa forme décisionnelle, soit dans sa forme fonctionnelle grâce essentiellement aux fonctions de Skolem [8, 3] (des fonctions booléennes associées aux symboles existentiellement quantifiés de la formule dépendant des symboles universellement quantifiés qui les précèdent) qui peuvent être revisitées par exemple en des politiques [11]. La sémantique présentée sous sa forme décisionnelle, si elle est bien adaptée au problème théorique du test d'appartenance à un langage, ne permet pas d'extraire les solutions de la QBF et n'est donc pas suffisante lorsque l'on désire aider le « joueur existentiel » à gagner si l'on considère la QBF comme étant un jeu à deux joueurs (i.e. quels que soient les coups du « joueur universel », le « joueur existentiel » a un coup qui le mène à la victoire). Nous nous proposons de revisiter la définition de la sémantique des formules booléennes quantifiées pour en jeter des bases définies par induction permettant de traiter les symboles propositionnels libres, les symboles propositionnels existentiellement quantifiés definis par une solution et les symboles propositionnels existentiellement quantifiés qui ne sont pas définis dans une solution et qui sont éliminés suivant la sémantique habituelle basée sur la disjonction. Cette nouvelle définition de la sémantique nous permet d'explorer une relation d'équivalence basée non pas sur la préservation de la validité mais sur celle des solutions. Cette relation nous permet de définir un calcul syntaxique pour les formules booléennes quantifiées basé sur la notion de relation de formules [24].

2 Préliminaires

Les valeurs booléennes sont notées **vrai** et **faux**. L'ensemble des valeurs booléennes est noté **BOOL**. L'ensemble des symboles propositionnels est noté $\mathcal{SP}$. Le symbole $\wedge$ est utilisé pour la conjonction, $\vee$ pour la disjonction, $\neg$ pour la négation, $\rightarrow$ pour l'implication et $\leftrightarrow$ pour la bi-implication. L'ensemble des formules propositionnelles est dénoté **PROP**. Un littéral est

un symbole propositionnel ou la négation de celui-ci. Le complémentaire d'une formule propositionnelle F, noté $\overline{F}$, est G si $F = \neg G$ et $\neg F$ sinon. L'ensemble des sous-formules et leurs complémentaires d'une formule propositionelle F, incluant $\top$ et $\overline{\top}$, est dénoté $sub(F)$. Une formule propositionnelle est sous forme normale conjonctive (FNC) si c'est une conjonction de disjonctions de littéraux. Une substitution est une fonction de l'ensemble des symboles propositionnels dans l'ensemble **PROP**. Nous définissons la substitution d'un symbole propositionnel x par F dans G, notée $[x \leftarrow F](G)$, comme étant la formule obtenue de G en remplaçant toutes les occurrences du symbole propositionnel x par la formule F. Une valuation v est une fonction de $\mathcal{SP}$ dans **BOOL** et l'interprétation, notée v^* est son extension dans **PROP**. Le symbole $\exists$ est utilisé pour la quantification existentielle et $\forall$ pour la quantification universelle. Toute formule propositionnelle est aussi une formule booléenne quantifiée (QBF). Si F est une QBF et x est un symbole propositionnel alors $(\exists x\ F)$ et $(\forall x\ F)$ sont des QBF. Un lieur est une chaîne de caractères $q_1 x_1 \dots q_n x_n$ avec $x_1, \dots, x_n$ des symboles propositionnels distincts et $q_1 \dots q_n$ des quantificateurs ; le lieur vide est noté ε ; par convention, des quantificateurs différents lient des symboles propositionnels différents. Une QBF constituée d'un lieur et d'une formule booléenne appelée matrice est une QBF prénexe ; si tout symbole propositionnel apparaissant dans une QBF possède une occurrence dans le lieur elle est dite close. Nous nous restreignons par la suite aux QBF prénexes. Le lieur induit une relation d'ordre sur les symboles propositionnels qui est notée $<$ (plus un symbole est à gauche dans la lieur plus il est petit). Une QBF est en FNC si sa matrice l'est. La sémantique des symboles booléens est définie de manière habituelle ; en particulier, à chaque connecteur (resp. $\top$, $\bot$, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$) est associée une fonction booléenne (resp. $i_\top, i_\bot :\rightarrow$ **BOOL** $i_\neg$: **BOOL** $\rightarrow$ **BOOL**, $i_\wedge, i_\vee, i_\rightarrow, i_\leftrightarrow$: **BOOL**$\times$**BOOL** $\rightarrow$ **BOOL**) qui en définit sa sémantique. A une fonction booléenne f d'arité n (i.e. une fonction de $\mathbf{BOOL}^n$ dans **BOOL**) est associée une formule propositionnelle ψ_f sur les symboles propositionnels $\{x_1, \dots, x_n\}$ telle que $v^*(\psi_f) =$ **vrai** si et seulement si $f(v(x_1), \dots, v(x_n)) =$ **vrai** pour toute valuation v.

3 Sémantique et relations d'équivalences

Nous revisitons la sémantique des QBF puis nous explorons les propriétés d'une relation d'équivalence non pas basée sur la préservation de la validité comme pour l'équivalence classique mais sur la préservation des modèles QBF. La sémantique d'une QBF prénexe en définit la valeur de vérité selon une *valuation QBF* composée d'une valuation propositionnelle et d'une *valuation fonctionnelle.*

Définition 1 (valuation QBF) *Une fonction partielle sk de l'ensemble des symboles propositionnels dans l'ensemble des fonctions booléennes est une* valuation fonctionnelle *pour une QBF prénexe si pour tout symbole propositionnel existentiellement quantifié x il existe un (unique) couple $(x \mapsto \hat{x}) \in sk$ tel que la fonction booléenne $\hat{x}$ a pour arité le nombre de symboles propositionnels universellement quantifiés qui précèdent x dans le lieur. L'ensemble des valuations fonctionnelles est noté* **VAL_FONC**. *Une valuation QBF est un couple constitué d'une valuation propositionnelle et d'une valuation fonctionnelle. L'ensemble des valuations QBF est noté* **VAL_QBF** $=$ **VAL_PROP** $\times$ **VAL_FONC**. *Une valuation QBF est* partielle *si tous les symboles propositionnels existentiellement quantifiés de la QBF prénexe ne sont pas présents dans la valuation fonctionnelle.*

Une valuation QBF qui n'est pas partielle peut être qualifiée, pour insister, de « valuation QBF totale ».

Exemple 1 *Soit la QBF $\xi = \forall a \exists b \forall c \exists d \mu$ avec $\mu = \neg((c \rightarrow b) \rightarrow \neg(d \rightarrow a))$. La fonction partielle $\{(b \mapsto \hat{b}), (d \mapsto \hat{d})\}$, $\hat{b}$ d'arité 1 et $\hat{d}$ d'arité 2, est une valuation fonctionnelle qui forme avec toute valuation propositionnelle une valuation QBF (totale) pour la QBF ξ ; les valuations fonctionnelles $\emptyset$, $\{(b \mapsto \hat{b})\}$ et $\{(d \mapsto \hat{d})\}$ en forment avec toute valuation propositionnelle des valuations QBF partielles.*

Une valuation fonctionnelle est un ensemble de fonctions booléennes qui sont très souvent appelées «fonctions de Skolem». Dans la littérature, la valuation propositionnelle est une fonction qui associe à tout symbole propositionnel une valeur de vérité ; pour la valuation fonctionnelle, une fonction partielle est préférée à une fonction totale.

La sémantique d'une QBF prénexe est définie pour des QBF prénexes telles que des quantificateurs différents sont associés à des symboles propositionnels différents. À chaque connecteur logique est associée une fonction à valeurs dans **BOOL** qui en définit sa sémantique au niveau propositionnel. Les définitions suivantes reprennent l'organisation de la définition de la sémantique de la logique des prédicats proposée dans [14] : une définition de la sémantique des connecteurs et constantes logiques au niveau propositionnel identique à celle de la sémantique de la logique propositionnelle, une définition de la sémantique des connecteurs, constantes et quantificateurs au niveau QBF comme une restriction de celle de la sémantique de la logique des prédicats, une définition de la sémantique des QBF comme extension aux formules de la

sémantique des connecteurs, constantes et quantificateurs. Nous définissons la sémantique au niveau QBF des connecteurs et constantes logiques ainsi que des quantificateurs.

Définition 2 (sémantique des connecteurs et quantificateurs) *La sémantique des connecteurs et quantificateurs est définie par (v une valuation propositionnelle et sk une valuation fonctionnelle) :*

$$I_\top, I_\bot : \mathbf{VAL\_QBF} \to \mathbf{BOOL}$$

$$I_\bot(v, sk) = i_\bot \quad I_\top(v, sk) = i_\top$$

$$I_\neg : (\mathbf{VAL\_QBF} \to \mathbf{BOOL}) \times \mathbf{VAL\_QBF} \to \mathbf{BOOL}$$

$$I_\neg(f)(v, sk) = i_\neg(f(v, sk))$$

$$I_\circ : (\mathbf{VAL\_QBF} \to \mathbf{BOOL})^2 \times \mathbf{VAL\_QBF} \to \mathbf{BOOL}$$

$$I_\circ(f, g)(v, sk) = i_\circ(f(v, sk), g(v, sk))$$
pour tout connecteur $\circ \in \{\wedge, \vee, \to, \leftrightarrow\}$

$$I^x_\exists, I^x_\forall : (\mathbf{VAL\_QBF} \to \mathbf{BOOL}) \times \mathbf{VAL\_QBF} \to \mathbf{BOOL}$$

$$I^x_\exists(f)(v, sk) = i_\vee(f(v[x := \mathbf{vrai}], sk), f(v[x := \mathbf{faux}], sk))$$
$$I^x_\forall(f)(v, sk) = i_\wedge(\ f(v[x := \mathbf{vrai}], sk(\mathbf{vrai})), f(v[x := \mathbf{faux}], sk(\mathbf{faux})))$$

Nous sommes en mesure de définir la sémantique des QBF comme une extension de la sémantique des connecteurs, constantes et quantificateurs.

Définition 3 (sémantique des QBF prénexes) *La sémantique d'une QBF prénexe F est une fonction*

$$I^*(F) : \mathbf{VAL\_QBF} \to \mathbf{BOOL}$$

définie inductivement par :
- $I^*(\bot)(v, sk) = I_\bot(v, sk)$;
- $I^*(\top)(v, sk) = I_\top(v, sk)$;
- $I^*(x)(v, sk) = v(x)$ *si* $x \in \mathcal{SP}$;
- $I^*((G \circ H))(v, sk) = I_\circ(I^*(G), I^*(H))(v, sk)$ *si* G, H *sont des QBF et* $\circ \in \{\wedge, \vee, \to, \leftrightarrow\}$;
- $I^*(\neg G)(v, sk) = I_\neg(I^*(G))(v, sk)$ *si* G *est une QBF.*
- $I^*((\exists x\ G))(v, sk) = I^*(G)(v[x := \hat{x}], sk \setminus \{(x \mapsto \hat{x})\})$ *si* G *est une QBF,* $x \in \mathcal{SP}$ *et* $(x \mapsto \hat{x}) \in sk$;
- $I^*((\exists x\ G))(v, sk) = I^x_\exists(I^*(G))(v, sk)$ *si* G *est une QBF,* $x \in \mathcal{SP}$ *et il n'existe pas de couple* $(x \mapsto \hat{x}) \in sk$ *(*$\hat{x}$ *fonction booléenne) ;*
- $I^*((\forall x\ G))(v, sk) = I^x_\forall(I^*(G))(v, sk)$ *si* G *est une QBF et* $x \in \mathcal{SP}$.

Cette sémantique est particulièrement souple puisqu'elle fait cohabiter le symbole propositionnel libre dont la valeur de vérité est déterminée par la valuation propositionnelle, le symbole propositionnel existentiellement quantifié associé à une fonction booléenne dont la valeur de vérité est déterminée lorsque, dans le processus de calcul inductif de la sémantique, le symbole propositionnel devient libre et enfin le symbole propositionnel existentiellement quantifié qui n'est pas associé à une fonction booléenne et qui s'élimine comme une disjonction sur les deux valeurs de vérité, retrouvant ainsi la sémantique du problème de décision. A notre connaissance, il n'existe pas de définition inductive de la sémantique des QBF prénexes qui permette une telle souplesse (la définition de [8] porte sur les QBF CNF et ne propose pas l'équivalent des valuations QBF partielles ; la définition de [11], si elle est inductive, ne manipule ni les symboles propositionnels libres, ni les valuations QBF partielles sauf pour décrire des solutions partielles à des QBF non valides). Cette sémantique met particulièrement aussi en lumière que restreinte à des formules sans quantificateur, elle n'est autre que la sémantique de la logique propositionnelle. Cette sémantique permet de retrouver aussi un résultat du premier ordre qui exprime que si la formule est close alors la valuation propositionnelle est sans importance.

Exemple 2 *En continuant l'exemple 1 et pour la valuation QBF partielle* $sk = \{(d \mapsto \hat{d})\}$ *(et une valuation propositionnelle v quelconque) avec*

$$\hat{d} = \{((\mathbf{vrai}, \mathbf{vrai}) \mapsto \mathbf{vrai}), ((\mathbf{vrai}, \mathbf{faux}) \mapsto \mathbf{vrai}), ((\mathbf{faux}, \mathbf{vrai}) \mapsto \mathbf{faux}), ((\mathbf{faux}, \mathbf{faux}) \mapsto \mathbf{faux})\}$$

$$\begin{aligned} & I^*(\forall a \exists b \forall c \exists d \mu)(v, sk) \\ = \ & I^a_\forall(I^*(\exists b \forall c \exists d \mu))(v, sk) \\ = \ & i_\wedge(\ I^*(\exists b \forall c \exists d \mu)(v[a := \mathbf{vrai}], sk(\mathbf{vrai})), \\ & \quad I^*(\exists b \forall c \exists d \mu)(v[a := \mathbf{faux}], sk(\mathbf{faux}))) \end{aligned}$$

Détaillons, avec $v_a = v[a := \mathbf{vrai}]$

$$\begin{aligned} & I^*(\exists b \forall c \exists d \mu)(v_a, sk(\mathbf{vrai})) \\ = \ & I^b_\exists(I^*(\forall c \exists d \mu))(v_a, sk(\mathbf{vrai})) \\ = \ & i_\vee(\ I^*(\forall c \exists d \mu)(v_a[b := \mathbf{vrai}], sk(\mathbf{vrai})), \\ & \quad I^*(\forall c \exists d \mu)(v_a[b := \mathbf{faux}], sk(\mathbf{vrai}))) \end{aligned}$$

avec $v_b = v_a[b := \mathbf{vrai}]$ *et* $sk(\mathbf{vrai}) = \{(d \mapsto \{(\mathbf{vrai} \mapsto \mathbf{vrai}), (\mathbf{faux} \mapsto \mathbf{vrai})\})\}$

$$\begin{aligned} & I^*(\forall c \exists d \mu)(v_b, \{(d \mapsto \hat{d}(\mathbf{vrai}))\}) = \\ & i_\wedge(\ I^*(\exists d \mu)(v_b[c := \mathbf{vrai}], \{(d \mapsto \hat{d}(\mathbf{vrai})(\mathbf{vrai}))\}), \\ & \quad I^*(\exists d \mu)(v_b[c := \mathbf{faux}], \{(d \mapsto \hat{d}(\mathbf{vrai})(\mathbf{faux}))\})) \end{aligned}$$

enfin en posant $v_c = v_b[d := \mathbf{vrai}]$

$$\begin{array}{ll} & I^*(\exists d\mu)(v_c, \{(d \mapsto \hat{d}(\mathbf{vrai})(\mathbf{vrai}))\}) \\ = & I^*(\mu)(v_c[d := \hat{d}(\mathbf{vrai})(\mathbf{vrai})], \emptyset) \\ = & I^*(\mu)(v_c[d := \mathbf{vrai}], \emptyset) \\ = & \mathbf{vrai} \end{array}$$

Sans plus de détails,

$$I^*(\forall a \exists b \forall c \exists d \mu)(v, sk) = \mathbf{vrai}.$$

La notion de modèle (propositionnel) est étendue aux QBF prénexes.

Définition 4 (modèle QBF) *Une valuation QBF V constituée d'une valuation propositionnelle v et d'une valuation fonctionnelle (totale) sk pour une QBF prénexe F est un modèle QBF pour F si $I^*(F)(v, sk) = \mathbf{vrai}$.*

Cette définition de la notion de modèle QBF n'est autre pour notre description de la sémantique que celle pour les QBF CNF introduite dans [8]. Lorsque la QBF prénexe est close alors la valuation propositionnelle n'importe pas et, dans la définition précédente, seule la valuation fonctionnelle participe au modèle de la QBF.

Exemple 3 *En continuant l'exemple 2, la valuation fonctionnelle $sk = \{(b \mapsto \hat{b}), (d \mapsto \hat{d})\}$ avec $\hat{b} = \{(\mathbf{vrai} \mapsto \mathbf{vrai}), (\mathbf{faux} \mapsto \mathbf{vrai})\}$ permet quelle que soit la valuation propositionnelle associée d'obtenir un modèle QBF pour la QBF prénexe $\forall a \exists b \forall c \exists d \mu$.*

Les modèles d'une formule propositionnelle et les modèles d'une QBF close prénexe quantifiée uniquement existentiellement dont la matrice est précisément la formule propositionnelle sont en bijection.

La sémantique attendue des quantificateurs peut être facilement retrouvée (G une QBF prénexe dont l'unique symbole propositionnel libre est x et une valuation propositionnelle v) :

$$\begin{array}{l} I^*((\forall x\ G))(v, \emptyset) = \\ \quad i_\wedge(I^*([x \leftarrow \top](G))(v, \emptyset), I^*([x \leftarrow \bot](G))(v, \emptyset)) \end{array}$$

et

$$\begin{array}{l} I^*((\exists x\ G))(v, \emptyset) = \\ \quad i_\vee(I^*([x \leftarrow \top](G))(v, \emptyset), I^*([x \leftarrow \bot](G))(v, \emptyset)). \end{array}$$

La définition classique de la validité d'une QBF close peut alors être redéfinie dans notre reformulation de la sémantique : une QBF close F est valide si, pour toute valuation propositionnelle v, $I^*(F)(v, \emptyset) = \mathbf{vrai}$.

La question du problème de validité peut être reformulée ainsi : une QBF close est valide si et seulement si elle admet un modèle QBF.

Le lemme suivant met en exergue le lien entre les modèles d'une QBF et la formule propositionnelle tautologique née de la substitution dans la matrice des symboles existentiellement quantifiés par des formules uniquement constituées des symboles universellement quantifiés.

Lemme 1 *Soit QF une QBF prénexe dont les variables existentielles sont $\{x_1, \ldots, x_n\}$, $sk = \{(x_i \mapsto \hat{x_i})\}$ un valuation fonctionnelle pour la QBF QF, $\phi_{\hat{x_1}}, \ldots, \phi_{\hat{x_n}}$ les formules associées positivement aux fonctions $\hat{x_1}, \ldots, \hat{x_n}$ et la substitution $\sigma = [x_1 \leftarrow \phi_{\hat{x_1}}] \ldots [x_n \leftarrow \phi_{\hat{x_n}}]$ alors la valuation QBF $V = (v, sk)$, v une valuation quelconque, est un modèle de la QBF QF si et seulement si la formule propositionnelle $\sigma(F)$ est une tautologie.*

Exemple 4 *En continuant l'exemple 3 et en considérant les formules propositionnelles $\phi_b = \mathbf{vrai}$ et $\phi_d = a$, associées aux fonctions booléennes $\hat{b}$ et $\hat{d}$, la formule propositionnelle $[b \leftarrow \phi_b][d \leftarrow \phi_d](\mu)$ est une tautologie.*

La sémantique des QBF prénexes suggère deux *relations d'équivalence* : la relation d'équivalence classique ($\equiv$) sur la préservation de la validité et la relation d'équivalence ($\cong$) sur la préservation des modèles [25]. La première s'exprime simplement dans notre sémantique (F et G deux QBF prénexes) : $F \equiv G$ si, pour toute valuation propositionnelle v, $I^*(F)(v, \emptyset) = I^*(G)(v, \emptyset)$.

La relation $\equiv$ ne préserve que la validité des QBF prénexes mais n'informe pas sur la préservation des modèles, ce qui est crucial pour par exemple la compilation des QBF ; nous avons donc proposé une nouvelle relation d'équivalence (dénotée $\cong$) sur la préservation des modèles [25].

Définition 5 (relation $\cong$) *Soient F et G deux QBF prénexes de lieurs identiques jusqu'à la dernière existentielle. $F \cong G$ si, pour toute valuation propositionnelle v et pour toute valuation fonctionnelle sk pour F et G, $I^*(F)(v, sk) = I^*(G)(v, sk)$.*

La définition proposée ici est différente de celle présentée initialement dans [25] car elle autorise à réunir dans une même classe d'équivalence des QBF prénexes ayant des lieurs qui diffèrent sur les universelles les plus internes, prenant ainsi en compte le fait qu'un modèle QBF est constitué de fonctions booléennes dépendant des symboles propositionnels universellement quantifiés qui précèdent le symbole propositionnel existentiellement quantifié associé à la fonction. Ainsi, bien que les lieurs soient différents $\exists x x \cong \exists x \forall y((x \vee y) \wedge (y \rightarrow x))$ car ces deux QBF prénexes ont pour modèles QBF $\{(x \mapsto \mathbf{vrai})\}$; mais

$\exists xx \not\cong \forall y \exists x((x \vee y) \wedge (y \rightarrow x))$ car l'unique modèle QBF de cette dernière QBF prénexe est la valuation QBF $(\emptyset, \{(x \mapsto \{(\mathbf{vrai} \mapsto \mathbf{vrai}), (\mathbf{faux} \mapsto \mathbf{vrai})\})\})$. Une autre définition, plus complexe, de la relation d'équivalence préservant les modèles peut être choisie de telle manière qu'elle ne tienne pas compte de l'ordre des quantificateurs universels contigus.

La différence entre les deux relations d'équivalence est la suivante : la relation d'équivalence préservant uniquement la validité autorise les valuations QBF partielles ; ainsi $\exists xx \equiv \top$ mais $\exists xx \not\cong \top$ car l'unique modèle QBF de $\top$ est la valuation QBF vide alors que l'unique modèle QBF de $\exists xx$ est la valuation QBF $\{(x \mapsto \mathbf{vrai})\}$. De même $\exists xx \equiv \exists yy$ mais $\exists xx \not\cong \exists yy$.

Le lemme suivant établit que la relation $\cong$ est bien une relation d'équivalence.

Lemme 2 *La relation $\cong$ est une relation d'équivalence pour les QBF prénexes.*

Ce lemme est immédiat car l'égalité est une relation d'équivalence.

La relation d'équivalence préservant les modèles réalise une partition de la classe d'équivalence de représentant $\top$ de la relation d'équivalence préservant la validité : c'est ce qu'exprime le premier item du lemme suivant ; le second item exprime que les deux relations sont identiques lorsque les QBF sont sans quantificateur. La preuve du lemme est immédiate à partir de la remarque ci-dessus et des définitions.

Lemme 3 *Soient F et G deux QBF prénexes.*
- *Si $F \cong G$ alors $F \equiv G$.*
- *De plus si F et G sont deux QBF sans quantificateur alors $F \equiv G$ si et seulement si $F \cong G$.*

Le lemme suivant établit la congruence de l'équivalence de préservation des modèles par rapport aux quantifications existentielle et universelle et les corollaires pour des QBF sans quantificateur.

Lemme 4 *Soient F et G deux QBF prénexes. Si $F \cong G$ et x un symbole propositionnel lié ni dans F ni dans G alors $\exists xF \cong \exists xG$ et $\forall xF \cong \forall xG$.*

De plus, si F et G sont sans quantificateur, $F \equiv G$ et x un symbole propositionnel alors $\exists xF \cong \exists xG$ et $\forall xF \cong \forall xG$.

Les résultats classiques s'étendent partiellement à la relation d'équivalence préservant les modèles.

Lemme 5 *Soient F et G deux QBF prénexes, H une formule propositionnelle, x et y deux symboles propositionnels et Q un lieur. Alors*

($Q^{\cong}$.1) $\exists x \exists y F \cong \exists y \exists x F$

($Q^{\cong}$.2) $I^*(\forall x \forall y F)(v, sk) = I^*(\forall y \forall x F)(v, sk')$ *avec sk et sk' identiques à ceci près que les deux premières colonnes sont permutées*

($Q^{\cong}$.3) $\exists x Q(x \wedge H) \cong \exists x Q(x \wedge [x \leftarrow \top](H))$

($Q^{\cong}$.4) $\exists x Q(\neg x \wedge H) \cong \exists x Q(\neg x \wedge [x \leftarrow \bot](H))$

($Q^{\cong}$.5) $I^*(\forall x Q(x \vee H))(v, sk) = I^*(Q[x \leftarrow \bot](H))(v, sk(\mathbf{faux}))$

($Q^{\cong}$.6) $I^*(\forall x Q(\neg x \vee H))(v, sk) = I^*(Q[x \leftarrow \top](H))(v, sk(\mathbf{vrai}))$

Les équivalences $Q^{\cong}$.3, $Q^{\cong}$.4, $Q^{\cong}$.5 et $Q^{\cong}$.6 réalisent une propagation unitaire : les équivalences $Q^{\cong}$.3 et $Q^{\cong}$.4 conservent le symbole propositionnel existentiellement quantifié dans la matrice pour préserver les modèles (puisque le lieur doit être le même de part et d'autre) tandis que $Q^{\cong}$.5 et $Q^{\cong}$.6 éliminent le symbole propositionnel universellement quantifié ainsi que son quantificateur (les QBF ne pouvant alors plus être équivalentes). L'exemple suivant démontre par un exemple que $\forall x \forall y F \not\cong \forall y \forall x F$ ce qui met en exergue une disymétrie par l'équivalence $Q^{\cong}$.1 dans le comportement des deux quantificateurs.

Exemple 5 *Soient les deux QBF prénexes $\theta = \forall a \forall b \exists c((\neg a \wedge b) \rightarrow c)$ et $\theta' = \forall b \forall a \exists c((\neg a \wedge b) \rightarrow c)$ ainsi que la valuation fonctionnelle*

$$sk = \{(c \mapsto \{((\mathbf{vrai}, \mathbf{vrai}) \mapsto \mathbf{vrai}), ((\mathbf{vrai}, \mathbf{faux}) \mapsto \mathbf{vrai}), ((\mathbf{faux}, \mathbf{vrai}) \mapsto \mathbf{faux}), ((\mathbf{faux}, \mathbf{faux}) \mapsto \mathbf{faux})\})\}$$

alors

$$I^*(\theta)(v, sk) = \mathbf{faux} \neq I^*(\theta')(v, sk) = \mathbf{vrai}$$

mais avec la valuation fonctionnelle suivante qui respecte vis-à-vis de sk les conditions de $Q^{\cong}$.2

$$sk' = \{(c \mapsto \{((\mathbf{vrai}, \mathbf{vrai}) \mapsto \mathbf{vrai}), ((\mathbf{faux}, \mathbf{vrai}) \mapsto \mathbf{vrai}), ((\mathbf{vrai}, \mathbf{faux}) \mapsto \mathbf{faux}), ((\mathbf{faux}, \mathbf{faux}) \mapsto \mathbf{faux})\})\}$$

alors $I^*(\theta)(v, sk) = I^*(\theta')(v, sk')$.

4 Calcul syntaxique

Nous présentons notre calcul syntaxique comme une extension pour les QBF de la justification dans le cadre de la théorie de la preuve de l'algorithme de Stålmarck [24].

4.1 Relation de formules

Une relation de formules [24] (propositionnelle) R pour une formule F est définie comme étant une relation d'équivalence sur $sub(F)$ avec pour contrainte

que pour tout éléments $A, B \in sub(F)$, si $R(A, B)$ alors $R(\overline{A}, \overline{B})$. Une classe d'une relation de formules R contenant un élément A est notée $[A]_R$ (et plus simplement $[A]$ lorsque la relation de formules est clairement explicitée par le contexte). La sémantique attendue est que tous les éléments d'une même classe d'équivalence ont la même valeur de vérité. Nous étendons ce formalisme aux QBF QM en ajoutant un lieur à la partition P de $sub(M)$ et en écrivant la relation de formules (Q, P).

La relation de formules la plus fine pour une QBF prénexe QM est la relation identité Id_{QM} qui est la partition des singletons de $sub(M)$ associée au lieur Q. La relation de formules $R([A]_R = [B]_R)$ (notée plus simplement par la suite $R([A] = [B])$) pour une QBF prénexe QM est la relation de formules la plus fine pour QM telle qu'elle est un raffinement de R et $([A]_R = [B]_R)$. La relation de formules $Id_{QM}([M] = [\top])$ nous servira de racine à l'arbre de déduction de notre calcul syntaxique. Dans ce qui suit seule une des deux classes symétriques $[A]$ et $[\overline{A}]$ sera explicitée.

Exemple 6 *Soit la QBF*

$$\xi = \forall a \exists b \forall c \exists d \neg((c \rightarrow b) \rightarrow \neg(d \rightarrow a))$$

alors

$$Id_\xi([\overline{F}] = [\top]) = (\forall a \exists b \forall c \exists d, [\top, \overline{F}], [a], [b], [c], [d], [F_0], [F_1])$$

avec $F = (F_0 \rightarrow \overline{F_1})$, $F_0 = (c \rightarrow b)$ *et* $F_1 = (d \rightarrow a)$.

4.2 Système syntaxique

Nous présentons notre système syntaxique S_{QBF} pour les QBF comme un ensemble de règles $\frac{conclusion}{prémisse}$ qui opèrent sur des relations de formules formant un arbre de déduction dont la racine est la relation de formules $Id_{QM}([M] = [\top])$. Mais avant de présenter le système nous définissons un ensemble de relations de formules qui correspondent à des relations de formules à partir desquelles aucune déduction ne sera plus possible.

Définition 6 (explicitement contradictoire) *Une relation de formules est* explicitement contradictoire *si une des conditions suivantes est vérifiée :*

1. *il existe une formule F dans la relation de formules telle que $[F] = [\overline{F}]$;*
2. *il existe une classe qui contient au moins deux symboles propositionnels universellement quantifiés du lieur ;*
3. *il existe une classe qui contient un symbole propositionnel universellement quantifié u du lieur et un symbole propositionnel existentiellement quantifié e tel que $e < u$.*

La condition 1 maintient intuitivement qu'une formule et son complémentaire ne peuvent avoir la même valeur de vérité. La condition 2 exprime que deux symboles universellement quantifiés ne sont jamais liés fonctionnellement. La condition 3 correspond dans le cadre de l'unification de termes du premier ordre au classique test d'occurrence. Une relation de fomules peut n'être pas explicitement contradictoire et contenir des classes qui le sont.

Nous ne présentons les règles du système S_{QBF} que pour le fragment $\{\rightarrow, \top\}$. Pour simplifier, dans la description de la prémisse et de la conclusion de la règle, seuls le lieur et les classes pertinentes sont notées, les classes invariantes ne sont pas décrites (la classe $[\top]$ est implicitement toujours présente).

Définition 7 (système S_{QBF} pour $\{\rightarrow, \top\}$) *Le système S_{QBF} est constitué de deux règles d'élimination du quantificateur existentiel :*

$$\exists\top : \frac{(Q,[x]=[\top])}{(\exists x Q,[x])} \qquad \exists\bot : \frac{(Q,[\overline{x}]=[\top])}{(\exists x Q,[x])}$$

d'une règle d'élimination du quantificateur universel :

$$\forall : \frac{(Q,[x]=[\top]) \quad (Q,[\overline{x}]=[\top])}{(\forall x Q,[x])}$$

et neuf règles de fusion des classes :

$$1 : \frac{(Q,[\overline{F_X}]=[\top],[\overline{F_Y}]=[\top])}{(Q,[(F_X \rightarrow F_Y)]=[\overline{F_Y}])} \qquad 2 : \frac{(Q,[F_X]=[\top],[F_Y]=[\top])}{(Q,[(F_X \rightarrow F_Y)]=[F_X])}$$

$$3 : \frac{(Q,[F_X]=[\top],[\overline{F_Y}]=[\top])}{(Q,[\overline{(F_X \rightarrow F_Y)}]=[\top])} \qquad 4 : \frac{(Q,[(F_X \rightarrow F_Y)]=[\overline{F_X}])}{(Q,[(F_X \rightarrow F_Y)],[\overline{F_Y}]=[\top])}$$

$$5 : \frac{(Q,[(F_X \rightarrow F_Y)]=[\overline{F_X}])}{(Q,[(F_X \rightarrow F_Y)],[F_X]=[\overline{F_Y}])} \qquad 6 : \frac{(Q,[(F_X \rightarrow F_Y)]=[\top])}{(Q,[(F_X \rightarrow F_Y)],[\overline{F_X}]=[\top])}$$

$$7 : \frac{(Q,[(F_X \rightarrow F_Y)]=[\top])}{(Q,[(F_X \rightarrow F_Y)],[F_Y]=[\top])} \qquad 8 : \frac{(Q,[(F_X \rightarrow F_Y)]=[\top])}{(Q,[(F_X \rightarrow F_Y)],[F_X]=[F_Y])}$$

$$9 : \frac{(Q,[(F_X \rightarrow F_Y)]=[F_Y])}{(Q,[(F_X \rightarrow F_Y)],[F_X]=[\top])}$$

Le lien sémantique entre la prémisse et la conclusion des règles de fusion est un lien d'équivalence de préservation des modèles qui sera explicité dans la section suivante.

Exemple 7 *La règle 9 de la définition précédente exprime que si la relation de formules R est telle que son lieur est Q et la partition est telle qu'une classe contienne une formule $(F_X \rightarrow F_Y)$ et que les formules F_X et $\top$ appartiennent à la même classe alors est inférée par la règle 9 une relation de formules $R([(F_X \rightarrow F_Y)] = [F_Y])$ (en particulier, cette nouvelle relation de formules est toujours telle que $[F_X] = [\top]$).*

Nous sommes à même de décrire ce qu'est un arbre de déduction et une preuve pour le système S_{QBF}.

Définition 8 (arbre de déduction) *Un* arbre de déduction *est défini inductivement ainsi :*

- *toute relation de formules qui est non explicitement contradictoire est un arbre de déduction pour le système S_{QBF} ;*
- *si R est une relation de formules, r une règle du S_{QBF} telle que la premisse soit satisfaite par R et que le résultat R', unique conclusion de l'application de la règle à la prémisse soit non explicitement contradictoire et si ∇' est un arbre de déduction de racine R' alors $\frac{\nabla'}{R}r$ est un arbre de déduction de racine R ;*
- *si R est une relation de formules, r une règle du S_{QBF} telle que la premisse soit satisfaite par R et que les résultats R' et R'', conclusions de l'application de la règle r à la prémisse soient non explicitement contradictoires et si ∇' et ∇'' sont des arbres de déduction de racine respectivement R' et R'' alors $\frac{\nabla' \quad \nabla''}{R}r$ est un arbre de déduction de racine R.*

Dans les exemples qui suivent, seule l'application des règles de fusion est indicée par le numéro de la règle.

Exemple 8 (suite de l'exemple 6) *L'arbre ci-dessous est un arbre de déduction pour le système S_{QBF} ($F = (F_0 \to \overline{F_1})$, $F_0 = (c \to b)$ et $F_1 = (d \to a)$).*

$$\dfrac{\dfrac{\nabla \quad \nabla'}{(\forall a \exists b \forall c \exists d, [\top, \overline{F}, F_0, F_1], [a], [b], [c], [d])}\,3}{Id_\xi([\overline{F}] = [\top])}$$

avec ∇ tel que

$$\dfrac{\dfrac{\dfrac{(\varepsilon, [\top, \overline{F}, F_0, F_1, a, b, c, d])}{(\exists d, [\top, \overline{F}, F_0, F_1, a, b, c], [d])} \quad \dfrac{(\varepsilon, [\top, \overline{F}, F_0, F_1, a, b, \overline{c}, d])}{(\exists d, [\top, \overline{F}, F_0, F_1, a, b, \overline{c}], [d])}}{(\forall c \exists d, [\top, \overline{F}, F_0, F_1, a, b], [c], [d])}}{(\exists b \forall c \exists d, [\top, \overline{F}, F_0, F_1, a], [b], [c], [d])}$$

avec ∇' tel que

$$\dfrac{\dfrac{\dfrac{(\exists d, [\top, \overline{F}, F_0, F_1, \overline{a}, \overline{d}, b, c]) \quad (\exists d, [\top, \overline{F}, F_0, F_1, \overline{a}, \overline{d}, b, \overline{c}])}{(\forall c \exists d, [\top, \overline{F}, F_0, F_1, \overline{a}, \overline{d}, b], [c])}}{(\exists b \forall c \exists d, [\top, \overline{F}, F_0, F_1, \overline{a}, \overline{d}], [b], [c])}}{(\exists b \forall c \exists d, [\top, \overline{F}, F_0, F_1, \overline{a}], [b], [c], [d])}\,4$$

La relation de formules $(\exists d, [\top, \overline{F}, F_0, F_1, \overline{a}, \overline{d}, b, c])$ n'est pas explicitement contradictoire bien que a et c soient des symboles propositionnels universellement quantifés car ils n'appartiennent plus au lieur qui est présentement $\exists d$.

Nous sommes en mesure de définir ce qu'est une preuve pour une QBF dans le système S_{QBF}.

Définition 9 (axiome et preuve) *Un* axiome *est une relation de formules non explicitement contradictoire ne contenant que deux classes et qui est telle que l'on ne puisse construire un arbre de déduction avec l'axiome pour racine et contenant une relation de formules explicitement contradictoire. Une* preuve *pour une QBF QM dans le système S_{QBF} est un arbre de déduction de racine $Id_{QM}([M] = [\top])$ tel que toute feuille soit un axiome.*

Exemple 9 *L'arbre de déduction de l'exemple 8 est une preuve dans le système S_{QBF} de la QBF*

$$\forall a \exists b \forall c \exists d \neg((c \to b) \to \neg(d \to a)).$$

La définition de l'axiome prévient la contradiction dans une classe. Cette définition se réduit uniquement à la première condition si l'utilisation de la règle d'élimination du quantificateur n'est utilisée que lorsque aucune autre règle ne peut plus l'être (car alors nécessairement des règles aurait été déduite la contradiction).

Exemple 10 *La relation de formules*

$$(\varepsilon, [(a \to b), a, \overline{b}, \top], [\overline{(a \to b)}, \overline{a}, b, \overline{\top}])$$

(dont exceptionnellement toutes les classes ont été explicitées) n'est pas explicitement contradictoire mais n'est pas un axiome car :

$$\dfrac{(\varepsilon, [(a \to b), a, \overline{b}, \top, \overline{(a \to b)}, \overline{a}, b, \overline{\top}])}{(\varepsilon, [(a \to b), a, \overline{b}, \top], [\overline{(a \to b)}, \overline{a}, b, \overline{\top}])}\,1$$

Ceci interdit une preuve n'utilisant que la règle d'élimination du quantificateur existentiel telle que :

$$\dfrac{\dfrac{(\varepsilon, [(a \to b), a, \overline{b}, \top], [\overline{(a \to b)}, \overline{a}, b, \overline{\top}])}{(\exists b, [(a \to b), a, \top], [\overline{(a \to b)}, \overline{a}, \overline{\top}], [b], [\overline{b}])}}{(\exists a \exists b, [(a \to b), \top], [\overline{(a \to b)}, \overline{\top}], [a], [\overline{a}], [b], [\overline{b}])}$$

4.3 Sémantique

Nous introduisons une fonction d'interprétation qui explicite la sémantique d'une relation de fonctions en une QBF.

Définition 10 (fonction d'interprétation) *La fonction d'interprétation d'une relation de formules $(\cdot, \cdot)^*$ est une fonction de l'ensemble des relations de formules dans les QBF définie par*

$$(Q, P)^* = Q \bigwedge_{C \in P} \Big(\bigwedge_{F, F' \in C} (F \leftrightarrow F') \Big).$$

Clairement, $(Q, Id_{QM}([M] = [\top]))^* \cong QM$.

Exemple 11

$$(\exists b \forall c \exists d, [\top, \overline{F}, F_0, F_1, \overline{a}, \overline{d}], [b], [c])^* \\ = \quad \exists b \forall c \exists d (\overline{F} \wedge F_0 \wedge F_1 \wedge \neg a \wedge \neg d)$$

La correction du système S_{QBF} par rapport à la sémantique des QBF est une conséquence du lemme suivant.

Lemme 6 (Correction des règles de fusion) *Soit la relation de formules R' le résultat de l'application d'une règle de fusion sur une relation de formules R alors $R'^* \cong R^*$.*

Il est immédiat qu'à partir du calcul de la validité directement par la définition de la sémantique des quantificateurs il est possible de construire une preuve dans le système S_{QBF} : la preuve, de bas en haut élimine tous les quantifcateurs puis fusionne les classes grâce aux règles 4, 5 et 7, d'où la complétude.

Théorème 1 (Correction et complétude du système S_{QBF} par rapport à la sémantique des QBF) *Une QBF QM est valide si et seulement si la relation de formules $Id_{QM}([M] = [\top])$ admet une preuve dans le système S_{QBF}.*

4.4 Extensions au système S_{QBF}

Le système S_{QBF} présenté jusqu'ici est assez pauvre : il n'élimine les quantificateurs qu'en employant explicitement leur sémantique et il ne tire aucun avantage des propriétés algébriques du connecteur logique. Les extensions proposées ci-dessous préservent la correction (la complétude étant préservée si nous ne faisons qu'étendre le système de règles).

Nouvelles règles d'élimination triviale des quantificateurs. Nous introduisons deux règles d'élimination des quantificateurs pour les symboles propositionnels qui n'interviennent pas dans la matrice d'une QBF :

$$\not\exists : \ \frac{(QQ', P)}{(Q \exists x Q', P)} \qquad \not\forall : \ \frac{(QQ', P)}{(Q \forall x Q', P)}$$

sachant que le symbole propositionnel x n'apparait pas dans la partition P.

Nouvelles règles pour l'élimination des quantificateurs. Nous introduisons deux nouvelles règles d'élimination du quantificateur existentiel basées sur l'équivalence : $Q \exists x Q'(x \wedge H) \equiv QQ'[x \leftarrow \top](H)$.

$$\exists + : \ \frac{(QQ', [x]=[\top])}{(Q \exists x Q', [x]=[\top])} \qquad \exists - : \ \frac{(QQ', [\overline{x}]=[\top])}{(Q \exists x Q', [\overline{x}]=[\top])}$$

Elles expriment que si le symbole propositionnel existentiellement quantifié a été déduit comme ne pouvant valoir qu'une valeur de vérité particulière alors le quantificateur peut être supprimé.

Nouvelles règles pour les symboles propositionnels universellement quantifiés. L'ensemble des règles de fusion sont purement propositionnelles et ne tiennent pas compte des contraintes qui s'imposent pour les symboles propositionnels universellement quantifiés. Nous introduisons un nouvel ensemble de règles de fusion qui se déduisent aisément de la sémantique associée à une relation de formules via la fonction d'interprétation.

$$10 : \ \frac{(QQ' \forall x Q'', [y]=[\top])}{(Q \exists y Q' \forall x Q'', [(x \rightarrow y)]=[\top])}$$

$$11 : \ \frac{(QQ' \forall x Q'', [y]=[\top])}{(Q \exists y Q' \forall x Q'', [(x \rightarrow y)]=[y])}$$

$$12 : \ \frac{(QQ' \forall y Q'', [x]=[\top])}{(Q \exists x Q' \forall y Q'', [(x \rightarrow y)]=[y])}$$

$$13 : \ \frac{(QQ' \forall x Q'', [\overline{y}]=[\top])}{(Q \exists y Q' \forall x Q'', [(x \rightarrow y)]=[\overline{x}])}$$

$$14 : \ \frac{(QQ' \forall y Q'', [\overline{x}]=[\top])}{(Q \exists x Q' \forall y Q'', [(x \rightarrow y)]=[\top])}$$

$$15 : \ \frac{(QQ' \forall y Q'', [\overline{x}]=[\top])}{(Q \exists x Q' \forall y Q'', [(x \rightarrow y)]=[\overline{x}])}$$

Le nouveau système peut être considéré comme l'abstraction d'une restriction du système de propagation de contraintes pour les QBF [26] en voyant la propagation de contraintes comme un système de fusion des classes d'équivalences.

Exemple 12 *En continuant l'exemple 1. Extrait de la preuve pour le système S_{QBF} enrichi (avec $F_0 = (c \rightarrow b)$) :*

$$\dfrac{\dfrac{(\forall a \forall c \exists d, [\top, \overline{F}, F_0, F_1, b], [a], [c], [d])}{(\forall a \exists b \forall c \exists d, [\top, \overline{F}, F_0, F_1], [a], [b], [c], [d])}\,{}_{10}}{Id_\xi([\overline{F}] = [\top])}\,{}_{3}$$

4.5 Calcul du modèle

Nous annotons notre système S_{QBF} pour les QBF prénexes en y ajoutant la construction d'un modèle QBF : nos règles opérent maintenant sur un couple $V \vdash (Q, P)$ avec P une partition pour $sub(M)$, (Q, P) une relation de formules et V une valuation QBF de QM. Nous étendons les notions d'axiome, de dérivation et de preuve pour un nouveau système S^a_{QBF}, extension annotée du système S_{QBF}.

Le système S^a_{QBF} est constitué de deux règles d'élimination du quantificateur existentiel :

$$\exists \top^a : \ \frac{(v[x{:=}\mathbf{vrai}], sk) \vdash (Q, [x]=[\top])}{(v, \{\hat{x}{=}\mathbf{vrai}\} \cup sk) \vdash (\exists x Q, [x])}$$

$$\exists \bot^a : \ \frac{(v[x{:=}\mathbf{faux}], sk) \vdash (Q, [\overline{x}]=[\top])}{(v, \{\hat{x}{=}\mathbf{faux}\} \cup sk) \vdash (\exists x Q, [x])}$$

d'une règle d'élimination du quantificateur universel (en notant $V_{\mathbf{vrai}} = (v[x := \mathbf{vrai}], sk(\mathbf{vrai}))$ et $V_{\mathbf{faux}} = (v[x := \mathbf{faux}], sk(\mathbf{faux}))$) :

$$\forall^a : \quad \frac{V_{\mathbf{vrai}} \vdash (Q,[x]=[\top]) \quad V_{\mathbf{faux}} \vdash (Q,[\overline{x}]=[\top])}{(v,sk) \vdash (\forall x Q,[x])}$$

et chaque règle de fusion des classes de 1 à 9 de la définition 7 de structure $\frac{R'}{R}$ est augmentée en une règle $\frac{V \vdash R'}{V \vdash R}$.

Nous annotons aussi les règles de fusion 10 à 15 de l'extension du système S_{QBF} :

$$10 : \quad \frac{(v[y:=\mathbf{vrai}],sk) \vdash (QQ'\forall xQ'',[y]=[\top])}{(v,\{\hat{y}=\mathbf{vrai}\}\cup sk) \vdash (Q\exists yQ'\forall xQ'',[(x\rightarrow y)]=[\top])}$$

$$11 : \quad \frac{(v[y:=\mathbf{vrai}],sk) \vdash (QQ'\forall xQ'',[y]=[\top])}{(v,\{\hat{y}=\mathbf{vrai}\}\cup sk) \vdash (Q\exists yQ'\forall xQ'',[(x\rightarrow y)]=[y])}$$

$$12 : \quad \frac{(v[x:=\mathbf{vrai}],sk) \vdash (QQ'\forall yQ'',[x]=[\top])}{(v,\{\hat{x}=\mathbf{vrai}\}\cup sk) \vdash (Q\exists xQ'\forall yQ'',[(x\rightarrow y)]=[y])}$$

$$13 : \quad \frac{(v[y:=\mathbf{faux}],sk) \vdash (Q\exists yQ'\forall xQ'',[\overline{y}]=[\top])}{(v,\{\hat{y}=\mathbf{faux}\}\cup sk) \vdash (Q\exists yQ'\forall xQ'',[(x\rightarrow y)]=[\overline{x}])}$$

$$14 : \quad \frac{(v[x:=\mathbf{faux}],sk) \vdash (QQ'\forall yQ'',[\overline{x}]=[\top])}{(v,\{\hat{x}=\mathbf{faux}\}\cup sk) \vdash (Q\exists xQ'\forall yQ'',[(x\rightarrow y)]=[\top])}$$

$$15 : \quad \frac{(v[x:=\mathbf{faux}],sk) \vdash (QQ'\forall yQ'',[\overline{x}]=[\top])}{(v,\{\hat{x}=\mathbf{faux}\}\cup sk) \vdash (Q\exists xQ'\forall yQ'',[(x\rightarrow y)]=[\overline{x}])}$$

Si la preuve se construit de bas en haut pour la recherche des axiomes, la construction du modèle QBF se réalise de haut en bas.

Exemple 13 *En continuant l'exemple 1 et pour la valuation QBF* $sk = \{(b \mapsto \hat{b}), (d \mapsto \hat{d})\}$ *(et une valuation propositionnelle* v *quelconque) avec*

$\hat{b} = \{(\mathbf{vrai} \mapsto \mathbf{vrai}), (\mathbf{faux} \mapsto \mathbf{vrai})\} = \mathbf{vrai}$ *et*
$\hat{d} = \{((\mathbf{vrai}, \mathbf{vrai}) \mapsto \mathbf{vrai}), ((\mathbf{vrai}, \mathbf{faux}) \mapsto \mathbf{vrai}),$
$((\mathbf{faux}, \mathbf{vrai}) \mapsto \mathbf{faux}), ((\mathbf{faux}, \mathbf{faux}) \mapsto \mathbf{faux})\}$

Extrait de la preuve pour le système S^a_{QBF} *avec calcul du modèle :*

$$\dfrac{\dfrac{\dfrac{\nabla_{\mathbf{vrai}} \quad \nabla_{\mathbf{faux}}}{(v[b := \mathbf{vrai}], \{(d \mapsto \hat{d})\}) \vdash (\forall a \forall c \exists d, [\top, \overline{F}, F_0, F_1, b], [a], [c], [d])}}{(v, sk) \vdash (\forall a \exists b \forall c \exists d, [\top, \overline{F}, F_0, F_1], [a], [b], [c], [d])}\,{}_{3}}{(v, sk) \vdash Id_\xi([\overline{F}] = [\top])}\,{}_{10}$$

avec $\nabla_{\mathbf{vrai}}$ *tel que*

$$(v[b := \mathbf{vrai}][a := \mathbf{vrai}], \{(d \mapsto \hat{d}(\mathbf{vrai}))\}) \vdash (\forall c \exists d, [\top, \overline{F}, F_0, F_1, b, a], [c], [d])$$

et $\nabla_{\mathbf{faux}}$ *tel que*

$$(v[b := \mathbf{vrai}][a := \mathbf{faux}], \{(d \mapsto \hat{d}(\mathbf{faux}))\}) \vdash (\forall c \exists d, [\top, \overline{F}, F_0, F_1, b, \overline{a}], [c], [d])$$

5 Conclusion

Nous avons proposé dans cet article une nouvelle présentation de la sémantique des QBF souple permettant de traiter les symboles propositionnels libres, les symboles propositionnels existentiellement quantifiés associés à une fonction booléenne dans une valuation QBF et les symboles propositionnels existentiellement quantifiés qui ne sont pas associés à une fonction booléenne dans une valuation QBF et qui sont éliminés suivant la sémantique habituelle basée sur la disjonction. Cette sémantique nous a permis d'explorer une relation d'équivalence basée sur la préservation des modèles QBF et non seulement sur la préservation de la validité. Nous avons proposé en outre un calcul syntaxique démontré correct et complet vis-à-vis de la sémantique des QBF qui tire parti de cette nouvelle relation d'équivalence en étendant la notion de relation de formules aux QBF. Le travail le plus proche de cette dernière contribution est sans doute le système de séquent GQBF [13] pour QBF CNF non prénexes sur lequel est basé la procédure `qpro`. Dans ce travail sont présentes les règles d'élimination des quantificateurs $\exists\top$, $\exists\bot$ et $\forall$ qui sont inhérentes à la sémantique des QBF. Ce travail est une extension du calcul des séquents classiques [14] orienté élimination des connecteurs et non relation de formules et son principal intérêt, de notre point de vue, est de fournir une justification dans le cadre de la théorie de preuve à la technique du «backjumping» [21, 15]. Notre proposition de calcul syntaxique non seulement étend aux QBF le système proposé pour l'algorithme de Stålmarck [24] mais l'étend aussi au niveau propositionnel dans la mesure où il permet de définir, dans le cadre de la propagation de contraintes, des propagateurs plus puissants (i.e. qui propagent plus d'information).

Références

[1] A. Ayari and D. Basin. Qubos : Deciding Quantified Boolean Logic using Propositional Satisfiability Solvers. In *Proceedings of the 4th International Conference on Formal Methods in Computer-Aided Design (FMCAD'02)*, pages 187–201, 2002.

[2] M. Benedetti. Evaluating QBFs via Symbolic Skolemization. In *Proceedings of the 11th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'05)*, number 3452 in LNCS, pages 285–300. Springer, 2005.

[3] M. Benedetti. Extracting Certificates from Quantified Boolean Formulas. In *Proceedings of 9th International Joint Conference on Artificial Intelligence (IJCAI'05)*, pages 47–53, 2005.

[4] M. Benedetti and H. Mangassarian. Experience and Perspectives in QBF-Based Formal Verification. *Journal on Satisfiability, Boolean Modeling and Computation*, 5 :133–191, 2008.

[5] P. Besnard, T. Schaub, H. Tompits, and S. Woltran. Paraconsistent reasoning via quantified Boolean formulas, i : Axiomatising signed systems. In *In Proceedings of the 8th European Conference on Logics in Artificial Intelligence (JELIA'02)*, pages 320–331, 2002.

[6] A. Biere. Resolve and Expand. In *Proceedings of the 7th International Confrerence on Theory and Applications of Satisfiability Testing (SAT'04)*, pages 59–70, 2004.

[7] H. K. Büning, M. Karpinski, and A. Flögel. Resolution for quantified Boolean formulas. *Information and Computation*, 117(1) :12–18, 1995.

[8] H. K. Büning, K. Subramani, and X. Zhao. Boolean Functions as Models for Quantified Boolean Formulas. *Journal of Automated Reasoning*, 39(1) :49–75, 2007.

[9] M. Cadoli, A. Giovanardi, and M. Schaerf. Experimental Analysis of the Computational Cost of Evaluating Quantified Boolean Formulae. In *Fifth Conference of the Italian Association for Artificial Intelligence*, pages 207–218, 1997.

[10] M. Cadoli, M. Schaerf, A. Giovanardi, and M. Giovanardi. An Algorithm to Evaluate Quantified Boolean Formulae and Its Experimental Evaluation. *Journal of Automated Reasoning*, 28(2) :101–142, 2002.

[11] S. Coste-Marquis, H. Fargier, J. Lang, D. Le Berre, and P. Marquis. Representing Policies for Quantified Boolean Formulae. In *Proceedings of the 10th International Conference on Principles of Knowledge Representation and Reasoning (KR'06)*, pages 286–296, 2006.

[12] M. Davis, G. Logemann, and D. Loveland. A machine program for theorem-proving. *Communication of the ACM*, 5, 1962.

[13] U. Egly, M. Seidl, and S. Woltran. A Solver for QBFs in Nonprenex Form. *Constraints*, 14(1) :38–79, 2009.

[14] J. H. Gallier. *Logic for computer science : foundations of automatic theorem proving*. Harper & Row Publishers, Inc., 1985.

[15] E. Giunchiglia, M. Narizzano, and A. Tacchella. Backjumping for Quantified Boolean Logic Satisfiability. In *Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI'01)*, pages 275–281, 2001.

[16] E. Giunchiglia, M. Narizzano, and A. Tacchella. Clause/Term Resolution and Learning in the Evaluation of Quantified Boolean Formulas. *Journal of Artificial Intelligence Research*, 26 :371–416, 2006.

[17] F. Bacchus H. Samulowitz. Using SAT in QBF. In *Proceedings of the 11th International Conference on Principles and Practice of Constraint Programming, Lecture Notes in Computer Science*, volume 3709, pages 578 – 592, 2005.

[18] A.R. Meyer and L.J. Stockmeyer. The equivalence problem for regular expressions with squaring requires exponential space. In *Proceedings of the 13th Annual Symposium on Switching and Automata Theory (SWAT'72)*, pages 125–129, 1972.

[19] G. Pan and M.Y. Vardi. Symbolic Decision Procedures for QBF. In *International Conference on Principles and Practice of Constraint Programming*, 2004.

[20] D.A. Plaisted, A. Biere, and Y. Zhu. A satisfiability procedure for quantified Boolean formulae. *Discrete Applied Mathematics*, 130 :291–328, 2003.

[21] Patrick Prosser. Hybrid algorithms for the constraint satisfaction problem. *Computational Intelligence*, 9 :268–299, 1993.

[22] J. Rintanen. Constructing conditional plans by a theorem-prover. *Journal of Artificial Intelligence Research*, 10 :323–352, 1999.

[23] J.A. Robinson. A machine-oriented logic based on the resolution principle. *JACM*, 12(1) :23–41, 1965.

[24] M. Sheeran and G. Stålmarck. A tutorial on Stålmarck's proof procedure for propositional logic. In G. Gopalakrishnan and P. Windley, editors, *Formal Methods in Computer-Aided Design*, volume 1522, pages 82–99. Springer-Verlag, Berlin, 1998.

[25] I. Stéphan. Algorithmes d'élimination de quantificateurs pour le calcul des politiques des formules booléennes quantifiées. In *Premières Journées Francophones de Programmation par Contraintes*, 2005.

[26] I. Stéphan. Boolean Propagation Based on Literals for Quantified Boolean Formulae. In *17th European Conference on Artificial Intelligence*, 2006.

[27] L.J. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3 :1–22, 1977.

[28] L. Zhang. Solving QBF with combined conjunctive and disjunctive normal form. In *National Conference on Artificial Intelligence (AAAI'06)*, 2006.