République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université M'hamed Bouguerra - Boumerdès

Faculté des Sciences
Département d'Informatique

Mémoire

Pour l'obtention du diplôme de

MAGISTER EN INFORMATIQUE

***Option* : « *INFORMATIQUE FONDAMENTALE* »**

Présenté et soutenu publiquement par

HAMIMED Lyazid

***Thème* :**

Un Système de Preuve d'Ordre Supérieur Basé sur le E_Lambda calcul

JURY

M[r] AHMED-NACER M.	Pr. USTHB	Président
M[r] ZEGOUR D.E	Pr I.N.I	Examinateur
M[r] KHALIFAT M.	Cc. UMBB	Examinateur
M[r] MEZEGHICHE M.	Pr. UMBB	Rapporteur

2006

Résumé

La majorité des systèmes de preuve existants sont basés sur le paradigme « type as formula », due au typage du lambda calcul et plus précisément inspiré de l'interprétation de la relation des termes avec leurs types. Cette interprétation, connue souvent l'isomorphisme de Curry Howard, consiste à considérer les types comme étant des propositions et les termes comme étant des preuves.

Le Eλ-calcul est une extension du lambda calcul pur, où une nouvelle procédure du processus de calcul est définie (la Eλβ-réduction) et deux constantes sont introduites : une de ces constantes est destinée à représenter l'implication et l'autre pour représenter la quantification universelle. Le système obtenu est assez puissant (le processus de calcul, la Eλβ-réduction, vérifie la propriété de Church-Rosser et offre un moyen pour éviter le paradoxe de Curry) et peut être utilisé pour interpréter les logiques d'ordre supérieur [MC02].

Le but de ce mémoire est d'étudier et de définir une procédure de preuve automatique dans le système E-lambda.

Mots clés : λ-calcul, systèmes de preuve, logique d'ordre supérieur, déduction naturelle, calcul des séquents. Paradoxe de Curry.

Abstract.

The existing proof systems are all based on the paradigm " type-as-formula", induced from the typed lambda calculus and more precisely inspired from the interpretation of the relation between terms and their types. This interpretation, known often as the Curry Howard isomorphism, consists of considering types as formulas and terms as proofs. The E_lambda calculus is an extension to the pure λ-calculus, where a new procedure of the calculation process is defined (the Eλβ-Reduction) and two constants are introduced: one to represent the logic implication and the other for the universal quantification. The obtained system is consistent (it verifies the property of Church-Rosser and avoids the Curry paradox) and can be used to interpret higher order logics [MC 02].

The aim of this work is to study and to define an automatic proof procedure for the Eλ calculus.

Key words: λ-calculus, Proof assistants, Higher order logic, Natural deduction, Sequent calculus, Curry paradox.

Table des Matières

INTRODUCTION 3

1 LE LAMBDA CALCUL 8

1.1 LAMBDA CALCUL PUR 8
1.1.1 Syntaxe du langage 8
1.1.2 Variables Libres et Variables Liées 9
1.1.3 Processus de substitution 10
1.1.4 Processus de réduction 11
1.1.5 Terminaison et confluence 11
1.2 LE LAMBDA CALCUL SIMPLEMENT TYPE 11
1.2.1 Syntaxe 12
1.2.2 Système de types 12
1.2.3 Normalisation forte 14
1.3 LOGIQUE CONSTRUCTIVE 14
1.3.1 La logique minimale 14
1.3.2 Le Calcul des Prédicats 15
1.3.3 Sémantique de Heyting 17
1.3.4 L'isomorphisme de Curry Howard 18
1.4 EXTENSIONS DU LAMBDA CALCUL TYPE 19
1.4.1 Système polymorphique du second ordre λ2 19
1.4.2 Calcul des constructions 20
1.5 LOGIQUE ET CONCEPTS MATHEMATIQUES DANS LE LANGAGE DES TYPES 21
1.5.1 Connecteurs et Quantificateurs 21
1.5.2 Représentation de l'arithmétique 23
1.5.3 Représentation des ensembles 24

2 SYSTEMES DE PREUVE 25

2.1 DEDUCTION NATURELLE 25
2.1.1 Contextes et jugements : 26
2.1.2 Règles de la déduction naturelle 26
2.1.3 Formalisation du processus de dérivation 28
2.2 LE CALCUL DES SEQUENTS 29
2.2.1 Jugements du calcul des séquents 29
2.2.2 Les règles du calcul des séquents 30
2.3 QUELQUES SYSTEMES DE PREUVE 33
2.3.1 Coq 33
2.3.2 Agda et Alfa 35
2.3.3 Isabelle/HOL 36
2.3.4 Phox 37

2.3.5 PVS (Prototype Verification System) ... 38
2.3.6 ACL2 ... 40
2.4 FOLDROL ... 41
2.4.1 Principe de base ... 41
2.4.2 Des preuves à la main ... 42
2.4.3 Règles d'inférences ... 42
2.4.4 L'inférence ... 46
2.4.5 Limites du Système FOLDROL ... 49
2.4.6 Tactiques et Méthodes Automatiques ... 49

3 LE SYSTEME E_LAMBDA ... 51

3.1 LES TERMES DU SYSTEME EΛ ... 51
Définition 3.1 Les termes de l'ensemble C_0 ... 52
Définition 3.2 Les termes d'un ensemble C_i ... 52
Définition 3.3 les termes du système Eλ « C_w » ... 52
Définition 3.4 (niveau d'un Eλ-terme) ... 52
Définition 3.5 (la congruence) ... 53
Définition 3.6 (Eλβ-réduction) ... 53
3.2 PROCESSUS D'INFERENCE ... 53
3.3 LES CONNECTEURS & LES QUANTIFICATEURS LOGIQUES ... 54
Proposition 3.1 ... 55
Proposition 3.2 ... 56
3.4 LA CONSISTANCE DU SYSTEME EΛ ... 56
3.4.1 Le paradoxe de Curry ... 56

4 LE DEMONSTRATEUR EΛ-PROVER ... 57

4.1 PROCEDURE DE DEMONSTRATION ... 57
4.1.1 Transformation de la formule à prouver ... 58
4.1.2 Construction des buts élémentaires ... 60
Définition 4.1 (le processus d'unification) ... 61
Propriété 4.1 ... 61
Propriété 4.2 ... 61
Définition 4.2 (sous formule) ... 61
Définition 4.3 (ensemble de variables) ... 61
Définition 4.4 (paramètres d'un habitant) ... 61
Définition 4.5 (les règles de substitutions σ) ... 62
Définition 4.6 (ordre d'une relation) ... 62
Définition 4.7 (ordre d'un habitant) ... 62
Définition 4.8 (l'univers HABIT associée à un type) ... 62
Propriété 4.3 ... 63
4.2 EXEMPLES : ... 64

CONCLUSION ... 71

BIBLIOGRAPHIE ... 73

ANNEXE ... 75