

Система доведення теорем з однією аксіомою

Максим Сохацький

¹ Національний технічний університет України
ім. Ігоря Сікорського
9 грудня 2019 р.

Анотація

Ця стаття презентує диалект мови програмування \mathbf{PTS}^∞ , імплементації її типового верифікатора, а також екстрактор байткоду для віртуальної машини Erlang від Ericsson. \mathbf{PTS}^∞ — це мова проміжного рівня заснована на так званій чистій системі типів, або системі типів з однією аксіомою та зліченною кількістю всесвітів (консистента теорія залежних типів). Ця мова програмування дає зручну мову проміжного рівня для застосунку у додадках з підвищеними вимогами до математичної верифікації. Типовий верифікатор побудований за базі MLTT принципів та конфігурується правилами для предикативної та імпредикативної ієрархії всесвітів. Синтаксис цієї мови програмування сумісний з базовим синтаксистом мови Morte, та підтримує її базову бібліотеку, а також додає поняття нескінченної кількості всесвітів. Дуже базова бібліотека прилюдії з рекурсивним та корекурсивним вводом-виводом додаються як частина цієї роботи. Це дає змогу застосовувати основи математичної верифікації до нескінченних або довгоживучих процесів.

Ми коротко опишемо мову верхнього рівня, та мову проміжного ядра для описаного в статті типового верифікатора, та покажемо місце цієї мови у концептуальній системі доведення теорем, яка передбачає поєднання: 1) оптимального лямбда обчислювача; 2) мову з однією аксіомою; 3) MLTT мову; 4) мову з гомотопічними типами та інтервалом.

Зміст

1	Вступ	3
1.1	Екстракція математично-доведених програм	3
1.2	Системна архітектура	3
1.3	Місце серед інших мов	4
2	Консистентна мова проміжного рівня	5
2.1	БНФ та Синтаксичне Дерево	6
2.2	Всесвіти	6
2.3	Предикативні всесвіти	6
2.4	Impredicative Universes	7
2.5	Переключення ієрархій	7
2.6	Contexts	7
2.7	Система з однією аксіомою	7
2.8	Верифікатор	8
2.9	Зсув індексів де Брейна	10
2.10	Підстановка	10
2.11	Нормалізація	10
2.12	Рівність	11
3	Використання мови	11
3.1	Сігма тип	12
3.2	Тип рівності	13
3.3	Система ефектів	13
3.3.1	Нескінченний ввід-вивід	14
3.3.2	Скінченний ввід-вивід	15
4	Вища мова з індуктивними типами	17
4.1	БНФ	17
4.2	Синтаксичне дерево	18
4.3	Кодування індуктивних типів	18
4.4	Поліноміальні функтори	19
4.5	Приклад кодування модуля List	19
4.6	Базова бібліотека	21
4.7	Вимірювання та порівняння з іншими системами	21
5	Висновки	22
6	Подяки	23

1 Вступ

IEEE¹ стандарт та регуляторні документи ESA² визначають набір інструментів та підходів для процесу валідації та верифікації програмного забезпечення. Найбільш розширені техніки передбачають застосування математичної логіки та теорії доведення теорем для формулювання виробничих задач у математичній формі для формальної перевірки коректності таких програм на всій області визначення функції з доведення властивостей цих функцій.

Ера верифікованих теорем, типових верифікатори та систем доведення теорем бере свій початок з доводжувача теорем AUTOMATH та теорії типів Мартіна-Льофа. Станом на сьогодні ми маємо такі потужні системи як Coq, Agda, Lean, F* які базуються на CoC (Calculus of Constructions, Coquand) та CiC (Calculus of Inductive Constructions, Paulin-Mohring). Подальший розвиток систематизації призвів до лямбда кубу та чистим системам з однією аксіомою, як узагальнюючому визначенню ситсем типу CoC, AUT-68, ECC, Henk, Morte, PTS[∞]. Головна мотивація систем з однією аксіомою — це простота імплементації та простота формальної імплементації нормалізатора термів, як термінального обчислення. За допомогою формальної мови та типового верифікатора ми можемо передавати програми по відкритих каналах які задовільняють формальним типовим специфікаціям та складним теоремам як властивостями цих об'єктів. У якості областей застосування тут можна виділити наступні сфери: 1) мови смарт-контрактів; 2) сертифіковані DSL; 3) платіжні системи, тощо.

1.1 Екстракція математично-доведених програм

Завдяки ізоморфізму Каррі-Ламбека-Ховарда — відповідності всередині теорії типів Мартіна-Льофа [13] між доведеннями, моделями та програмами, де типи, сигнатури та категорії є просторами (мовами) які містять у собі точки (програми), можемо трактувати терми як програми для обчислення певного результату, і природа цього обчислення може буде повністю позбавлена типізації, що дає змогу виконувати такі доведення на практично довільному інтерпретаторі, так як майже всі так чи інакше реалізують модель лямбда-числення, тут маються на увазі мови JavaScript, Erlang, PyPy, LuaJIT, K. Також можна будувати екстрактори з інтераналізацією в C++, Rust. Ця робота головним чином презентує екстрактор в байт-код віртуальної машини Erlang, як модель простого нетипизованого лямбда числення, на кшталт LISP або Smalltalk.

1.2 Системна архітектура

PTS[∞] як мова програмування реалізує чисту систему типів, але зі зліченою кількістю всесвітів. Ця система типів формує основне мовне ядро си-

¹IEEE Std 1012-2016 — V&V Software verification and validation

²ESA PSS-05-10 1-1 1995 — Guide to software verification and validation

стеми доведення теорем, усі інші системи типів містять чисту систему типів як підкатегорію у своєму спектрі, та є її нащадками. З точки зору наслідкових зв'язків чиста система типів є основою усіх системах типів побудованих на розшаруваннях, П-типах, а також систем здатних до доведення теорем.

Поверх цієї базової системи типів виділяються інші системи типів які можна звести теж до одно-аксіоматичних систем з чітко-вираженим кодуваннями ізоморфізмів. До концептуальної моделі системи доведення теорем включатимемо наступні мовні ядра: 1) Мова з індуктивними типами для доведення у стилі математичної індукції; 2) Гомотопічне ядро з відкритим інтервалом для доведення у кубічному стилі; 3) Числення отоків як базис для тензорного числення (Futhark); 4) Числення процесів як базис для лінійних типів, коіндуктивного моделювання та середовища виконання. Незважаючи на те, що з усіх цих мовних рівней існують функтори в систему з однією аксіомою, ці мовні розширення програмуються як окремі плагіни функтори які погрузаються у головний цикл типового верифікатора разом зі своїми правилами. Це дозволяє пришвидшити виконання нормалізації термів у процесі типової верифікації.

Однак не всі вищі мови можуть бути розкладені в базисі PTS. Як було показано Geuvers [9] ми не можемо побудувати принцип індукції всередині чистої PTS, ми повинні послабити до залучення оператора нерухомої точки принаймні для типової специфікації самого індуктивного рекурсивного типу. Також ми не можемо побудувати елімінатор рівності та функціональну екстенціональність. Але незважаючи на це PTS це потужна система яка відразу дає змогу генерувати сертифіковані програми з доведених теорем. Властивості можуть доводитися у інших мовах концептуальної моделі системи доведення теорем. Прошарок PTS більшим чином пов'язаний з мовою цільового інтерпретатора.

Як подальший розвиток цього проекту ми бачимо долучення індуктивної системи типів та гомотопічної системи типів.

1.3 Місце серед інших мов

Продукт який представлено у статті виконаний для телекомунікаційної платформи Erlang/OTP від Ericsson, що дало змогу використовувати доведені програми на цій віртуальній машині. Цей додаток експонує наступні сервіси у середовищі Erlang: 1) типова верифікація; 2) нормалізація; 3) екстракція. Усі частини системи **PTS**[∞] написані на мові Erlang та виключно для системи Erlang.

- Рівень 0 — сертифікований векторизований інтерпретатор
- Рівень 1 — консистентна система з однією аксіомою
- Рівень 2 — вища мова для доведення теорем та перевірки властивостей

Табл. 1: Список мов, досліджених у якості цільової платформи для екстракції

Target	Class	Intermediate	Theory
C++	компілятор/native	HNC	System F
Rust	компілятор/native	HNC	System F
JVM	інтерпретатор/native	Java	F-sub ³
JVM	інтерпретатор/native	Scala	System F-omega
GHC Core	компілятор/native	Haskell	System D
GHC Core	компілятор/native	Morte	CoC
Haskell	компілятор/native	Coq	CiC
OCaml	компілятор/native	Coq	CiC
BEAM	інтерпретатор	Om	PTS[∞]
O	інтерпретатор	Om	PTS [∞]
K	інтерпретатор	Q	Applicative
PyPy	інтерпретатор/native	N/A	ULC
LuaJIT	інтерпретатор/native	N/A	ULC
JavaScript	інтерпретатор/native	PureScript	System F

2 Консистентна мова проміжного рівня

The **Om** language is a dependently typed lambda calculus **PTS[∞]**, an extension of Coquand' Calculus of Constructions [6] with the predicative hierarchy of indexed universes. There is no fixpoint axiom, so there is no infinite term dependence, the theory is fully consistent and has strong normalization property.

All terms respect ranking **Axioms** inside the sequence of universes **Sorts** and complexity of the dependent term is equal to the maximum complexity of term and its dependency **Rules**. The universe system is completely described by the following PTS notation due to Barendregt [2]:

$$\begin{cases} \text{Sorts} = \text{Type}.\{i\}, i : \text{Nat} \\ \text{Axioms} = \text{Type}.\{i\} : \text{Type}.\{\text{inc } i\} \\ \text{Rules} = \text{Type}.\{i\} \rightsquigarrow \text{Type}.\{j\} : \text{Type}.\{\text{max } i \ j\} \end{cases}$$

The **Om** language is based on Henk languages described first by Erik Meijer and Simon Peyton Jones in 1997 [12]. Later on in 2015 Morte implementation of Henk design appeared in Haskell, using the Boem-Berrarducci encoding of non-recursive lambda terms. It is based only on one type constructor Π , its intro λ and apply eliminator, infinite number of universes, and β -reduction. The design of Om language resemble Henk and Morte both in design and in implementation. This language intended to be small, concise, easy provable and able to produce the verifiable piece of code that can be distributed over the networks, compiled at the target platform with a safe linkage.

2.1 БНФ та Синтаксичне Дерево

Om syntax is compatible with CoC presented in Morte and Henk languages. However, it has extension in a part of specifying universe index as a **Nat** number. Traditionally we present the language in Backus-Naur form. Equivalent AST tree encoding from the right side.

$ \begin{aligned} \diamond &::= \#option \\ V &::= \#identifier \\ S &::= * < \#number > \\ O &::= S \mid V \mid (O) \\ &\quad \mid O O \mid O \rightarrow O \\ &\quad \mid \lambda (I : O) \rightarrow O \\ &\quad \mid \forall (I : O) \rightarrow O \end{aligned} $	<pre> data pts = star (n: nat) var (n: name) app (f a: pts) lambda (x: name) (d c: pts) pi (x: name) (d c: pts) </pre>
--	--

2.2 Всесвіти

As **Om** has infinite number of universes it should include metatheoretical **Nat** inductive type in its core. **Om** supports predicative and impredicative hierarchies.

$$U_0 : U_1 : U_2 : U_3 : \dots$$

Where U_0 — propositions, U_1 — sets, U_2 — types and U_3 — kinds, etc.

$$\frac{}{Nat} \quad (I)$$

$$\frac{o : Nat}{Type_o} \quad (S)$$

You may check if a term is a universe with the star function. If an argument is not a universe it returns $\{error, _ \}$.

```

star (: star , N) → N
_ → (: error , "*" )

```

2.3 Предикативні всесвіти

All terms obey the **Axioms** ranking inside the sequence of **Sorts** universes, and the complexity **Rules** of the dependent term is equal to a maximum of the term's complexity and its dependency. Note that predicative universes are incompatible with Church lambda term encoding. You choose either predicative or impredicative universes with a type checker parameter.

$$\frac{i : Nat, j : Nat, i < j}{Type_i : Type_j} \quad (A_1)$$

$$\frac{i : Nat, j : Nat}{Type_i \rightarrow Type_j : Type_{max(i,j)}} \quad (R_1)$$

2.4 Impredicative Universes

Propositional contractible bottom space is the only available extension to the predicative hierarchy which doesn't lead to inconsistency. However, there is another option to have the infinite impredicative hierarchy.

$$\frac{i : \text{Nat}}{\text{Type}_i : \text{Type}_{i+1}} \quad (A_2)$$

$$\frac{i : \text{Nat}, \quad j : \text{Nat}}{\text{Type}_i \rightarrow \text{Type}_j : \text{Type}_j} \quad (R_2)$$

2.5 Переключення ієрархій

Function **h** returns the target Universe of B term dependence on A. There are two dependence rules known as the predicative one and the impredicative one which returns max universe or universe of the last term respectively.

```
dep A B : impredicative → B
      A B : predicative   → max A B
```

```
h A B → dep A B : impredicative
```

2.6 Contexts

The contexts model a dictionary with variables for type checker. It can be typed as the list of pairs or **List Sigma**. The elimination rule is not given here as in our implementation the whole dictionary is destroyed after type checking.

$$\frac{}{\Gamma : \text{Context}} \quad (\text{Ctx-formation})$$

$$\frac{\Gamma : \text{Context}}{\text{Empty} : \Gamma} \quad (\text{Ctx-intro}_1)$$

$$\frac{A : \text{Type}_i, \quad x : A, \quad \Gamma : \text{Context}}{(x : A) \vdash \Gamma : \text{Context}} \quad (\text{Ctx-intro}_2)$$

2.7 Система з однією аксіомою

This language is called one axiom language (or pure) as eliminator and introduction rules inferred from type formation rule. The only computation rule of Pi type is called beta-reduction. Computational rules of language are called operational semantics and establish equality of substitution and lambda application. Operational semantics in that way defines the rewrite rules of computations.

$$\frac{x : A \vdash B : \text{Type}}{\Pi (x : A) \rightarrow B : \text{Type}} \quad (\Pi\text{-formation})$$

$$\begin{array}{c}
\frac{x : A \vdash b : B}{\lambda (x : A) \rightarrow b : \Pi (x : A) \rightarrow B} \quad (\lambda\text{-intro}) \\
\\
\frac{f : (\Pi (x : A) \rightarrow B) \quad a : A}{f a : B [a/x]} \quad (App\text{-elimination}) \\
\\
\frac{x : A \vdash b : B \quad a : A}{(\lambda (x : A) \rightarrow b) a = b [a/x] : B [a/x]} \quad (\beta\text{-computation}) \\
\\
\frac{\pi_1 : A \quad u : A \vdash \pi_2 : B}{[\pi_1/u] \pi_2 : B} \quad (\text{subst})
\end{array}$$

The theorems (specification) of PTS could be embedded in itself and used as Logical Framework for the Pi type. Here is the example in the higher language.

```

record Pi (A: Type) :=
  (intro: (A → Type) → Type)
  (lambda: (B: A → Type) → pi A B → intro B)
  (app: (B: A → Type) → intro B → pi A B)
  (applam: (B: A → Type) (f: pi A B) → (a: A) →
    Path (B a) ((app B (lambda B f)) a) (f a))
  (lamapp: (B: A → Type) (p: intro B) →
    Path (intro B) (lambda B (λ (a:A) → app B p a)) p)

```

The proofs intentionally left blank, as it proofs could be taken from various sources [2]. The equalities of computational semantics presented here as **Path** types in the higher language.

The **Om** language is the extention of the **PTS**[∞] with the remote AST node which means remote file loading from trusted storage, anyway this will be checked by the type checker. We deny recursion over the remote node. We also add an index to var for simplified de Bruijn indexes, we allow overlapped names with tags, incremented on each new occurrence.

```

data om = star (n: nat)
  | var (n: name) (n: nat)
  | remote (n: name) (n: nat)
  | pi (x: name) (n: nat) (d c: om)
  | fn (x: name) (n: nat) (d c: om)
  | app (f a: om)

```

Our typechecker differs from canonical example of Coquand [5]. We based our typechecker on variable **Substitution**, variable **Shifting**, term **Normalization**, definitional **Equality** and **Type Checker** itself.

2.8 Верифікатор

For sure in a pure system, we should be careful with **:remote** AST node. Remote AST nodes like **#List/Cons** or **#List/map** are remote links to files. So using trick one should desire circular dependency over **:remote**.

type (:star,N)	D → (:star,N+1)
(:var,N,I)	D → :true = proplists:is_defined N B, om:keyget N D I
(:remote,N)	D → om:cache (type N D)
(:pi,N,0,I,O)	D → (:star,h(star(type I D)),star(type O [(N,norm I) D]))
(:fn,N,0,I,O)	D → let star (type I D), NI = norm I
	in (:pi,N,0,NI,type(O,[(N,NI) D]))
(:app,F,A)	D → let T = type(F,D),
	(:pi,N,0,I,O) = T, :true = eq I (type A D)
	in norm (subst O N A)

2.9 Зсув індексів де Брейна

Shift renames var N in B. Renaming means adding 1 to the nat component of variable.

```

sh  (: star ,X)      N P → (: star ,X)
    (: var ,N,I)     N P → (: var ,N,I+1) when I >= P
                        → (: var ,N,I)
    (: remote ,X)    N P → (: remote ,X)
    (: pi ,N,0 ,I ,O) N P → (: pi ,N,0 ,sh I N P ,sh O N P+1)
    (: fn ,N,0 ,I ,O) N P → (: fn ,N,0 ,sh I N P ,sh O N P+1)
    (: app ,L,R)     N P → (: app ,L,R)

```

2.10 Підстановка

Substitution replaces variable occurrence in terms.

```

sub  (: star ,X)      N V L → (: star ,X)
    (: var ,N,L)      N V L → V
    (: var ,N,I)      N V L → (: var ,N,I-1) when I > L
    (: remote ,X)     N V L → (: remote ,X)
    (: pi ,N,0 ,I ,O) N V L → (: pi ,N,0 ,sub I N V L ,sub O N (sh V N 0) L+1)
    (: pi ,F,X,I ,O)  N V L → (: pi ,F,X ,sub I N V L ,sub O N (sh V F 0) L)
    (: fn ,N,0 ,I ,O) N V L → (: fn ,N,0 ,sub I N V L ,sub O N (sh V N 0) L+1)
    (: fn ,F,X,I ,O)  N V L → (: fn ,F,X ,sub I N V L ,sub O N (sh V F 0) L)
    (: app ,F,A)      N V L → (: app , sub F N V L ,sub A N V L)

```

2.11 Нормалізація

Normalization performs substitutions on applications to functions (beta-reduction) by recursive entrance over the lambda and pi nodes.

```

norm  (: star ,X)      → (: star ,X)
    (: var ,X)         → (: var ,X)
    (: remote ,N)      → cache (norm N [])
    (: pi ,N,0 ,I ,O)  → (: pi ,N,0 ,norm I ,norm O)
    (: fn ,N,0 ,I ,O)  → (: fn ,N,0 ,norm I ,norm O)
    (: app ,F,A)       → case norm F of
                        (: fn ,N,0 ,I ,O) → norm (subst O N A)
                        NF → (: app ,NF ,norm A) end

```

2.12 Рівність

Definitional Equality simply checks the equality of Erlang terms.

```

eq  (: star ,N)          (: star ,N)          → true
    (: var ,N,I)         (: var ,(N,I))        → true
    (: remote ,N)        (: remote ,N)         → true
    (: pi ,N1,0 ,I1 ,O1) (: pi ,N2,0 ,I2 ,O2) →
      let :true = eq I1 I2
      in eq O1 (subst (shift O2 N1 0) N2 (:var ,N1,0) 0)
    (: fn ,N1,0 ,I1 ,O1) (: fn ,N2,0 ,I2 ,O2) →
      let :true = eq I1 I2
      in eq O1 (subst (shift O2 N1 0) N2 (:var ,N1,0) 0)
    (: app ,F1,A1)        (: app ,F2,A2)        → let :true = eq F1 F2 in eq A1 A2
    (A,B)                 → (: error ,( : eq ,A,B))

```

3 Використання мови

Here we will show some examples of **Om** language usage. In this section, we will show two examples. One is lifting PTS system to MLTT system by defining **Sigma** and **Equ** types using only **Pi** type. We will use Bohm inductive dependent encoding [3]. The second is to show how to write real world programs in **Om** that performs input/output operations within Erlang environment. We show both recursive (finite, routine) and corecursive (infinite, coroutine, process) effects.

```

$ ./om help me
[{a,[expr],"to parse. Returns {_,_} or {error,_}.",
 {type,[term],"typechecks and returns type."},
 {erase,[term],"to untyped term. Returns {_,_}.",
 {norm,[term],"normalize term. Returns term's normal form."},
 {file,[name],"load file as binary."},
 {str,[binary],"lexical tokenizer."},
 {parse,[tokens],"parse given tokens into {_,_} term."},
 {fst,[{x,y}],"returns first element of a pair."},
 {snd,[{x,y}],"returns second element of a pair."},
 {debug,[bool],"enable/disable debug output."},
 {mode,[name],"select metaverse folder."},
 {modes,[],"list all metaverses."}]

$ ./om print fst erase norm a "#List/Cons"
  \ Head
-> \ Tail
-> \ Cons
-> \ Nil
-> Cons Head (Tail Cons Nil)
ok

```

3.1 Сірма тип

The PTS system is extremely powerful even without **Sigma** type. But we can encode **Sigma** type similar how we encode **Prod** tuple pair in Bohm encoding. Let's formulate **Sigma** type as an inductive type in higher language.

```
data Sigma (A: Type) (P: A -> Type) (x: A): Type =
  (intro: P x -> Sigma A P)
```

The **Sigma-type** with its eliminators appears as example in Aaron Stump [15]. Here we will show desugaring to **PTS**[∞].

```
— Sigma/@
  \ (A: *)
-> \ (P: A -> *)
-> \ (n: A)
-> \/ (Exists: *)
-> \/ (Intro: A -> P n -> Exists)
-> Exists

— Sigma/Intro
  \ (A: *)
-> \ (P: A -> *)
-> \ (x: A)
-> \ (y: P x)
-> \ (Exists: *)
-> \ (Intro: \/ (x:A) -> P x -> Exists)
-> Intro x y

— Sigma/fst
  \ (A: *)
-> \ (B: A -> *)
-> \ (n: A)
-> \ (S: #Sigma/@ A B n)
-> S A ( \ (x: A) -> \ (y: B n) -> x)

— Sigma/snd
  \ (A: *)
-> \ (B: A -> *)
-> \ (n: A)
-> \ (S: #Sigma/@ A B n)
-> S (B n) ( \ (_: A) -> \ (y: B n) -> y )

> om: fst (om: erase (om: norm (om: a("#Sigma/test.fst")))).
{{λ,{ 'Succ',0}},
 {any,{λ,{ 'Zero',0}},{any,{var,{ 'Zero',0}}}}}}
```

For using **Sigma** type for Logic purposes one should change the home Universe of the type to **Prop**. Here it is:

```
data Sigma (A: Prop) (P: A -> Prop): Prop =
  (intro: (x:A) (y:P x) -> Sigma A P)
```

3.2 Тип рівності

Another example of expressiveness is Equality type a la Martin-Löf.

```
data Equ (A: Type): A -> A -> Type :=
  (refl (a: A): Equ A a a)
```

```
— Equ/@
  \ (A: *)
-> \ (x: A)
-> \ (y: A)
-> \/ (Equ: A -> A -> *)
-> \/ (Refl: \/ (z: A) -> Equ z z)
-> Equ x y

— Equ/Refl
  \ (A: *)
-> \ (x: A)
-> \ (Equ: A -> A -> *)
-> \ (Refl: \/ (z: A) -> Equ z z)
-> Refl x
```

You cannot construct a lambda that will check different values of A type is they are equal, however, you may want to use built-in definitional equality and normalization feature of type checker to actually compare two values:

```
> om: print (om: type (
  om: a ("(\ \ (z: #Equ/@ #Nat/@ #Nat/One #Nat/One) -> #Prop/True)" ++
    " (#Equ/Refl #Nat/@ (#Nat/Succ #Nat/Zero))" ))) .
  \/ (True: *0)
-> \/ (Intro: True)
-> True
ok

> om: print (om: type (
  om: a ("(\ \ (z: #Equ/@ #Nat/@ #Nat/One #Nat/One) -> #Prop/True)" ++
    " (#Equ/Refl #Nat/@ #Nat/Zero)" ))) .
** exception error: no match of right hand side value
   {error, { "==",
               {app, { {var, { 'Succ ', 0 } }, {var, { 'Zero ', 0 } } },
                     {var, { 'Zero ', 0 } } } }
```

3.3 Система ефектів

This work is expected to compile to a limited number of target platforms. For now, Erlang, Haskell, and LLVM are awaiting. Erlang version is expected to be used both on LING and BEAM Erlang virtual machines. This language allows you to define trusted operations in System F and extract this routine to Erlang/OTP platform and plug as trusted resources. As the example, we also

provide infinite coinductive process creation and inductive shell that linked to Erlang/OTP IO functions directly.

IO protocol. We can construct in pure type system the state machine based on (co)free monads driven by **IO/IOI** protocols. Assume that **String** is a **List Nat** (as it is in Erlang natively), and three external constructors: `getLine`, `putLine` and `pure`. We need to put correspondent implementations on host platform as parameters to perform the actual IO.

```
String: Type = List Nat
data IO: Type =
  (getLine: (String -> IO) -> IO)
  (putLine: String -> IO)
  (pure: () -> IO)
```

3.3.1 Нескінченний ввід-вивід

Infinity I/O Type Spec.

```
— IOI/@: (r: U) [x: U] [[s: U] -> s -> [s -> #IOI/F r s] -> x] x
  \ (r : *)
-> \ (x : *)
-> (\ (s : *)
  -> s
  -> (s -> #IOI/F r s)
  -> x)
-> x

— IOI/F
  \ (a : *)
-> \ (State : *)
-> \ (IOF : *)
-> \ (PutLine_ : #IOI/data -> State -> IOF)
-> \ (GetLine_ : (#IOI/data -> State) -> IOF)
-> \ (Pure_ : a -> IOF)
-> IOF

— IOI/MkIO
  \ (r : *)
-> \ (s : *)
-> \ (seed : s)
-> \ (step : s -> #IOI/F r s)
-> \ (x : *)
-> \ (k : forall (s : *) -> s -> (s -> #IOI/F r s) -> x)
-> k s seed step

— IOI/data
#List/@ #Nat/@
```

Infinite I/O Sample Program.

```

— Morte/corecursive
( \ (r: *1)
  -> ( (((#IOI/MkIO r) (#Maybe/@ #IOI/data)) (#Maybe/Nothing #IOI/data))
    ( \ (m: (#Maybe/@ #IOI/data))
      -> (((((#Maybe/maybe #IOI/data) m) ((#IOI/F r) (#Maybe/@ #IOI/data)))
        ( \ (str: #IOI/data)
          -> ((((#IOI/putLine r) (#Maybe/@ #IOI/data)) str)
            (#Maybe/Nothing #IOI/data))))
        (((#IOI/getLine r) (#Maybe/@ #IOI/data))
          (#Maybe/Just #IOI/data))))))

```

Erlang Coinductive Bindings.

```

copure () ->
  fun (_) -> fun (IO) -> IO end end.

cogetLine () ->
  fun (IO) -> fun (_) ->
    L = ch:list(io:get_line("> ")),
    ch:ap(IO,[L]) end end.

coputLine () ->
  fun (S) -> fun (IO) ->
    X = ch:unlist(S),
    io:put_chars(": "++X),
    case X of "0\n" -> list ([]);
    _ -> corec() end end end.

corec () ->
  ap('Morte':corecursive(),
    [copure(),cogetLine(),coputLine(),copure(),list([])]).

```

```

> om_extract:extract("priv/normal/IOI").
ok
> Active: module loaded: {reloaded,'IOI'}

```

```

> om:corec().
> 1
: 1
> 0
: 0
#Fun<List.3.113171260>

```

3.3.2 Скінченний ввід-вивід

I/O Type Spec.

```

— IO/@
  \ (a : *)
-> \ / (IO : *)

```

```

-> \ / (GetLine_ : (#IO/data -> IO) -> IO)
-> \ / (PutLine_ : #IO/data -> IO -> IO)
-> \ / (Pure_ : a -> IO)
-> IO

-- IO/replicateM
  \ (n: #Nat/@)
-> \ (io: #IO/@ #Unit/@)
-> #Nat/fold n (#IO/@ #Unit/@)
      (#IO/[>>] io)
      (#IO/pure #Unit/@ #Unit/Make)

```

Guarded Recursion I/O Sample Program.

```

-- Morte/recursive
((#IO/replicateM #Nat/Five)
 (((#IO/[>>=] #IO/data) #Unit/@) #IO/getLine) #IO/putLine))

```

Erlang Inductive Bindings.

```

pure() ->
  fun(IO) -> IO end.

getLine() ->
  fun(IO) -> fun(_) ->
    L = ch:list(io:get_line("> ")),
    ch:ap(IO,[L]) end end.

putLine() ->
  fun (S) -> fun(IO) ->
    io:put_chars(": "++ch:unlist(S)),
    ch:ap(IO,[S]) end end.

rec() ->
  ap('Morte':recursive(),
    [getLine(),putLine(),pure(),list([])]).

```

Here is example of Erlang/OTP shell running recursive example.

```

> om:rec().
> 1
: 1
> 2
: 2
> 3
: 3
> 4
: 4
> 5
: 5
#Fun<List.28.113171260>

```


4 Вища мова з індуктивними типами

As was shown by Herman Geuvers [9] the induction principle is not derivable in second-order dependent type theory. However there a lot of ways doing this. For example, we can build in induction principal into the core for every defined inductive type. We even can allow recursive type check for only terms of induction principle, which have recursion base — that approach was successfully established by Peng Fu and Aaron Stump [15]. In any case for derivable induction principle in PTS^∞ we need to have fixpoint somehow in the core.

So-called Calculus of Inductive Constructions [14] is used as a top language on top of PTS to reason about inductive types. Here we will show you a sketch of such inductive language model which intended to be a language extension to PTS system. CiC is allowing fixpoint for any terms, and base checking should be performed during type checking such terms.

Our future top language is a general-purpose functional language with Π and Σ types, recursive algebraic types, higher order functions, corecursion, and a free monad to encode effects. It compiles to a small MLTT core of dependent type system with inductive types and equality. It also has an Id-type (with its recursor) for equality reasoning, Case analysis over inductive types.

4.1 БНФ

```

< > ::= #option
[] ::= #list
| ::= #sum
1 ::= #unit
I ::= #identifier
U ::= Type < #nat >
T ::= 1 | ( I : O ) T
F ::= 1 | I : O = O , F
B ::= 1 | [ | I [ I ] → O ]
O ::= I | ( O ) |
      U | O → O | O O
          | fun ( I : O ) → O | fst O
          | snd O | id O O O
          | J O O O O O | let F in O
          | ( I : O ) * O | ( I : O ) → O
          | data I T : O := T | record I T : O := T
          | case O B

```

4.2 Синтаксичне дерево

The AST of higher language is formally defined using itself. Here you can find telescopes (context lists), split and its branches, inductive data definitions.

```
data tele (A: U) = emp | tel (n: name) (b: A) (t: tele A)
data branch (A: U) = br (n: name) (args: list name) (term: A)
data label (A: U) = lab (n: name) (t: tele A)
data ind
  = star (n: nat)
  | var (n: name) (i: nat)
  | app (f a: ind)
  | lambda (x: name) (d c: ind)
  | pi (x: name) (d c: ind)
  | sigma (n: name) (a b: ind)
  | arrow (d c: ind)
  | pair (a b: ind)
  | fst (p: ind)
  | snd (p: ind)
  | id (a b: ind)
  | idpair (a b: ind)
  | idelim (a b c d e: ind)
  | data_ (n: name) (t: tele ind) (labels: list (label ind))
  | case (n: name) (t: ind) (branches: list (branch ind))
  | ctor (n: name) (args: list ind)
```

The Erlang version of parser encoded with OTP library **yec** which implements LALR-1 grammar generator. This version resembles the model and slightly based on cubical type checker by Mortberg [4] and could be reached at Github repository⁴.

4.3 Кодування індуктивних типів

There are a number of inductive type encodings: 1) Commutative square encoding of F-algebras by Hinze, Wu [11]; 2) Inductive-recursive encoding, algebraic type of algebraic types, inductive family encoding by Dagand [7]; 3) Encoding with motives inductive-inductive definition, also with inductive families, for modeling quotient types by Altenkirch, Kaposi [1]; 4) Henry Ford encoding or encoding with Ran, Lan-extensions by Hamana, Fiore [10]; 5) Church-compatible Bohm-Berarducci encoding Bohm, Berarducci [3]. Om is shipped with base library in Church encoding and we already gave the example of IO system encoded with runtime linkage. We give here simple calculations behind this theory.

⁴<http://github.com/groupoid/infinity/tree/master/priv>

4.4 Поліноміальні функтори

Least fixed point trees are called well-founded trees. They encode polynomial functors.

Natural Numbers: $\mu X \rightarrow 1 + X$

List A: $\mu X \rightarrow 1 + A \times X$

Lambda calculus: $\mu X \rightarrow 1 + X \times X + X$

Stream: $\nu X \rightarrow A \times X$

Potentially Infinite List A: $\nu X \rightarrow 1 + A \times X$

Finite Tree: $\mu X \rightarrow \mu Y \rightarrow 1 + X \times Y = \mu X = \text{List } X$

As we know there are several ways to appear for a variable in a recursive algebraic type. Least fixpoint is known as a recursive expression that has a base of recursion. In Church-Bohm-Berarducci encoding type are store as non-recursive definitions of their right folds. A fold in this encoding is equal to id function as the type signature contains its type constructor as parameters to a pure function.

4.5 Приклад кодування модуля List

The data type of lists over a given set A can be represented as the initial algebra $(\mu L_A, in)$ of the functor $L_A(X) = 1 + (A \times X)$. Denote $\mu L_A = \text{List}(A)$. The constructor functions $nil : 1 \rightarrow \text{List}(A)$ and $cons : A \times \text{List}(A) \rightarrow \text{List}(A)$ are defined by $nil = in \circ inl$ and $cons = in \circ inr$, so $in = [nil, cons]$. Given any two functions $c : 1 \rightarrow C$ and $h : A \times C \rightarrow C$, the catamorphism $f = \llbracket [c, h] \rrbracket : \text{List}(A) \rightarrow C$ is the unique solution of the simultaneous equations:

$$\begin{cases} f \circ nil = c \\ f \circ cons = h \circ (id \times f) \end{cases}$$

where $f = foldr(c, h)$. Having this the initial algebra is presented with functor $\mu(1 + A \times X)$ and morphisms $sum : [1 \rightarrow \text{List}(A), A \times \text{List}(A) \rightarrow \text{List}(A)]$ as catamorphism. Using this encoding the base library of List will have following form:

$$\begin{cases} list = \lambda ctor \rightarrow \lambda cons \rightarrow \lambda nil \rightarrow ctor \\ cons = \lambda x \rightarrow \lambda xs \rightarrow \lambda list \rightarrow \lambda cons \rightarrow \lambda nil \rightarrow cons x (xs list cons nil) \\ nil = \lambda list \rightarrow \lambda cons \rightarrow \lambda nil \rightarrow nil \end{cases}$$

Here traditionally we show the **List** definition in higher language and its desugared version in **Om** language.

```
data List: (A: *) → * :=
  (Cons: A → list A → list A)
  (Nil: list A)
```

```

— List/@
  \ (A : *)
-> \ (List: *)
-> \ (Cons: \ (Head: A) -> \ (Tail: List) -> List)
-> \ (Nil: List)
-> List

— List/Cons
  \ (A: *)
-> \ (Head: A)
-> \ (Tail:
  \ (List: *)
  -> \ (Cons: \ (Head: A) -> \ (Tail: List) -> List)
  -> \ (Nil: List)
  -> List)
-> \ (List: *)
-> \ (Cons:
  \ (Head: A)
  -> \ (Tail: List)
  -> List)
-> \ (Nil: List)
-> Cons Head (Tail List Cons Nil)

— List/Nil
  \ (A: *)
-> \ (List: *)
-> \ (Cons:
  \ (Head: A)
  -> \ (Tail: List)
  -> List)
-> \ (Nil: List)
-> Nil

```

```

record lists : (A B: *) :=
  (len: list A → integer)
  ((++): list A → list A → list A)
  (map: (A → B) → (list A → list B))
  (filter: (A → bool) → (list A → list A))

```

$$\begin{cases}
foldr = \llbracket [f \circ nil, h] \rrbracket, f \circ cons = h \circ (id \times f) \\
len = \llbracket [zero, \lambda a \ n \rightarrow succ \ n] \rrbracket \\
(++) = \lambda xs \ ys \rightarrow \llbracket [\lambda(x) \rightarrow ys, cons] \rrbracket(xs) \\
map = \lambda f \rightarrow \llbracket [nil, cons \circ (f \times id)] \rrbracket
\end{cases}$$

$$\left\{ \begin{array}{l} len = foldr (\lambda x n \rightarrow succ n) 0 \\ (++) = \lambda ys \rightarrow foldr cons ys \\ map = \lambda f \rightarrow foldr (\lambda x xs \rightarrow cons (f x) xs) nil \\ filter = \lambda p \rightarrow foldr (\lambda x xs \rightarrow if p x then cons x xs else xs) nil \\ foldl = \lambda f v xs = foldr (\lambda xg \rightarrow (\lambda \rightarrow g (f a x))) id xs v \end{array} \right.$$

4.6 Базова бібліотека

The base library includes basic type-theoretical building blocks starting from **Unit**, **Bool**, **Either**, **Maybe**, **Nat**, **List** and **IO**. Here some examples how it looks like. The full listing of Base Library folder is available at **Om** GitHub repository⁵.

```
data Nat: Type :=
  (Zero: Unit → Nat)
  (Succ: Nat → Nat)

data List (A: Type) : Type :=
  (Nil: Unit → List A)
  (Cons: A → List A → List A)

record String: List Nat := List.Nil

data IO: Type :=
  (getLine: (String → IO) → IO)
  (putLine: String → IO)
  (pure: () → IO)

record IO: Type :=
  (data: String)
  ([>=>]: ...)

record Morte: Type :=
  (recursive: IO.replicateM
    Nat.Five (IO.[>=>] IO.data Unit
              IO.getLine IO.putLine))
```

4.7 Вимірювання та порівняння з іншими системами

The underlying **Om** type checker and compiler is a target language for higher level languages. The overall size of **Om** language with extractor to Erlang is 265 lines of code.

⁵<http://github.com/groupoid/om>

Табл. 2: Compiler Passes

Module	LOC	Description
om_tok	54 LOC	Токенайзер
om_parse	81 LOC	Синтаксичний парсер
om_type	60 LOC	Нормалізатор та верифікатор
om_erase	36 LOC	Стирання типів
om_extract	34 LOC	Екстракція Erlang байткоду

5 Висновки

В роботі запропонована модифікована версія CoC, також відома як чиста система або система з однією аксіомою, разом з предикативною або імпредикативною ієрархією зліченної кількості всесвітів. Ця система відома як консистентна, підтримує сильну нормалізацію термів, та відтворює базове ядро усіх сучасних систем доведення теорем, таких як Coq, Lean, Agda, тощо.

Результати дослідження В результаті цього дослідження встановлені наступні відкриття: 1) Відсутність рекурсії робить неможливим кодування принципу індукції, необхідне послаблення хоча б для сигнатур рекурсивних типів, так звані Self-типи, запропоновані у мові Cedile, авторами Peng Fu та Aaron Stump [8]. 2) Однак для забезпечення виконання програм System F цілком достатньо для забезпечення бібліотеки часу виконання; 2) Теореми які можуть бути вираженими без конструктора нерухомої точки, більше відповідають категорній семантиці; 3) Ця система може бути природнім чином транспортована у нетипизовані лямбда числення та їх евалуатори, що розширює область застосування майже на усі інтерпретатори. 4) Якщо обмежити розмір інтерпретатор та його програм розміром кеша першого рівня, то швидкість інтерпретації лямбда контекстів буде на рівні JIT або native.

Переваги над існуючими аналогічними рішеннями. 1) рафінована версія типового верифікатора на 300 рядків; Мінімальність ядра дає змогу швидко перекоонатися в коректності та здійснити ревью; 2) підтримка предикативної та імпредикативної ієрархій, як елемент конфігурації \mathbf{PTS}^∞ ; 3) евалуатор Erlang більш ефективний ніж вбудовування в Haskell; 4) мова \mathbf{PTS}^∞ використовується для специфікації нескінченних процесів.

Наукове та виробниче використання. 1) Ця мова може використовуватися як сертифікована ядро для додатків з підвищеними вимогами до якості, такі як фінансові додатки, математичні, або інші теми, які потребують перевірки тотальності функцій; 2) Ця мова може використовуватися як вбудовувана бібліотека; 3) В академії \mathbf{PTS}^∞ може використовуватися як дидактичний інструмент з логіки, систем типів, лямбда численню, функціональним мовам програмування.

Перспективи подальших досліджень. 1) Розширення спектру цільових мов та доведення семантики у cubicaltt; 2) Побудова екстрактор в оптиміальний лямбда евалуатор з \mathbf{PTS}^∞ ; 3) Побудова сертифікованого інтерпретатора на Rust як заміна Erlang; 4) Залучення принципу індукції в \mathbf{PTS}^∞ в майбутньому.

6 Подяки

Висловлюється подяка усім дописувичам Групоїд Інфініті, хто допоміг уникнути помилок в TeX та Erlang файлах. Також подяка всім рідним, хто підтримує нас.

Література

- [1] Thorsten Altenkirch and Ambrus Kaposi. Type theory in type theory using quotient inductive types. In *Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '16, pages 18–29, New York, NY, USA, 2016. ACM.
- [2] H. P. Barendregt. In S. Abramsky, Dov M. Gabbay, and S. E. Maibaum, editors, *Handbook of Logic in Computer Science (Vol. 2)*, pages 117–309, New York, NY, USA, 1992. Oxford University Press, Inc.
- [3] Corrado Böhm and Alessandro Berarducci. Automatic synthesis of typed lambda-programs on term algebras. In *Theoretical Computer Science*, volume 39, pages 135–154, 1985.
- [4] Cyril Cohen, Thierry Coquand, Simon Huber, and Anders Mörtberg. In *Cubical Type Theory: a constructive interpretation of the univalence axiom*, volume abs/1611.02108, 2017.
- [5] Thierry Coquand. An algorithm for type-checking dependent types. In *Sci. Comput. Program.*, volume 26, pages 167–177, 1996.
- [6] Thierry Coquand and Gerard Huet. The calculus of constructions. In *Information and Computation*, pages 95–120, Duluth, MN, USA, 1988. Academic Press, Inc.
- [7] P.É. Dagand, University of Strathclyde. Department of Computer, and PhD thesis Information Sciences. *A Cosmology of Datatypes: Reusability and Dependent Types*. 2013.
- [8] Peng Fu and Aaron Stump. Self types for dependently typed lambda encodings. In *Rewriting and Typed Lambda Calculi - Joint International Conference, RTA-TLCA 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14-17, 2014. Proceedings*, pages 224–239, 2014.

- [9] Herman Geuvers. *Induction Is Not Derivable in Second Order Dependent Type Theory*, pages 166–181. Springer Berlin Heidelberg, Berlin, Heidelberg, 2001.
- [10] Makoto Hamana and Marcelo P. Fiore. A foundation for gadts and inductive families: dependent polynomial functor approach. In *Proceedings of the seventh ACM SIGPLAN workshop on Generic programming, WGP@ICFP 2011, Tokyo, Japan, September 19-21, 2011*, pages 59–70, 2011.
- [11] Ralf Hinze and Nicolas Wu. Histo- and dynamorphisms revisited. In *Proceedings of the 9th ACM SIGPLAN Workshop on Generic Programming, WGP ’13*, pages 1–12, New York, NY, USA, 2013. ACM.
- [12] Simon Peyton Jones and Erik Meijer. Henk: A typed intermediate language. In *In Proc. First Int’l Workshop on Types in Compilation*, 1997.
- [13] P. Martin-Löf and G. Sambin. *Intuitionistic type theory*. Studies in proof theory. Bibliopolis, 1984.
- [14] Christine Paulin-Mohring. Introduction to the Calculus of Inductive Constructions. In Bruno Woltzenlogel Paleo and David Delahaye, editors, *All about Proofs, Proofs for All*, volume 55 of *Studies in Logic (Mathematical logic and foundations)*. College Publications, January 2015.
- [15] Aaron Stump. The calculus of dependent lambda eliminations. In *Journal of Functional Programming*, volume 27. Cambridge University Press, 2017.