Extending a first order predicate calculus with partially defined iota terms

Geert Vernaeve* Albert Hoogewijs

Abstract

Partial functions and “undefinedness” have been around in mathematics for a long time, without causing any trouble. It was only when mathematics and computer science met in projects on “automatization” of formal reasoning that some problems came up [Hoogewijs 1987]. Where humans are able to avoid the application of a partial function on an argument outside “the domain” of the function, formalizing the rules for this activity seems to be less trivial. In [Farmer 1996] Farmer states that there does not exist a consensus on how partial functions should be mechanized and the developer of a mechanized mathematics system must choose among many different possible ways of representing and reasoning about partial functions. We want to add one more possibility by introducing “partially defined iota terms” of the form $\iota x_\psi(\varphi)$ which represents the unique x satisfying φ whenever the condition ψ is fulfilled. We present an extension of a two-valued first order sequent calculus for predicate logic with identity [Hermes 1973], where we are able to reason correctly about partially defined iota terms.

1 Introduction

Our motivation is to extend the classical first order predicate calculus with identity (as formalised in e.g. [Hermes 1973]), in a form which is more in line with ‘common mathematical practice’, so it could be used as a foundation for a computer-based mathematical package.

*Supported by Wuytack Fonds UGent

1991 *Mathematics Subject Classification :* 03B35.

Key words and phrases : Mechanisation of proofs, sequent calculus, partial functions, undefinedness.

More specifically, we add so-called ι-terms to the calculus, in a way which is analogous to [Hilbert and Bernays 1968]: the term '$\iota x(\varphi)$' is to be interpreted as 'the (unique) x for which φ is true'. Such ι-terms are only allowed to be used if one can show that the **uniqueness condition** $\exists! x(\varphi)$ holds. For example, in a theory describing real numbers, we can introduce the operation of subtraction given addition: '$x - y$' is just $\iota z(z + y = x)$; we can indeed show $\vdash \exists! z(z + y = x)$.

However, we extend this "classical" notion of ι-term to situations where there is not always a unique x satisfying φ but only when a certain condition ψ (the **domain formula**) holds. For example, if we want to introduce division in the example given above, we'd like to proceed analogously and define $\frac{x}{y}$ as $\iota z(z \cdot y = x)$; however we can only show that $y \neq 0 \vdash \exists! z(z \cdot y = x)$; if $y = 0$ then every z satisfies $z \cdot y = x$. We will show that allowing such ι-terms to be added to the calculus introduces no contradictions, providing one considers the obtained ι-term as undefined when the uniqueness condition is not met (i.e., we consider $\iota z(z \cdot y = x)$ as undefined if $y \neq 0$). We will denote this partially defined ι-term as $\iota z_{y \neq 0}(z \cdot y = x)$: in the subscript, we note when the ι-term is defined (i.e., its domain formula). The interpretation of this ι-term is still 'the unique z for which $z \cdot y = x$' when $y \neq 0$, but when $y = 0$, this ι-term will be interpreted as 'undefined'.

The introduction of terms to denote the unique element for which a certain formula is true seems to date back to Peano, who used the notations ιx to refer to the set with x as its only element (i.e., what we would nowadays denote as $\{x\}$) and $\rotatebox[origin=c]{180}{ι} y$ to denote the element of the sole member of a set y (which corresponds to our ι-terms). Also Frege had a notation for the same purpose earlier [Whitehead and Russell 1910]. Whitehead and Russell elaborate further on this theme [Whitehead and Russell 1964], investigating the cases in which the term $\iota x(\varphi)$ can be introduced even when there exists no unique x such that φ is true. We follow the approach of Hilbert [Hilbert and Bernays 1968]: when there is no such unique x, $\iota x(\varphi)$ is still allowed as a term but one cannot derive any meaningful properties about it.

Hilbert also developed a related **epsilon calculus** which uses terms of the form $\epsilon x(\varphi)$. These are interpreted as 'an x for which φ is true' when there exist one or more such x, or 'a certain element of the domain' when there is no such x. In case there is no unique x satisfying φ, epsilon-terms hence represent a form of the axiom of choice. Note that these terms are always defined, even in the cases there is no unique x satisfying φ; in that respect, they are less suitable for our purpose of treating partially defined terms.

2 Syntax

We will introduce a logic which is an extension of the logic developed in [Hermes 1973], which we will refer to as the ι-free calculus; we will call our extension the ι-calculus.

The syntax of the ι-calculus is that of the ι-free calculus, with the only modification that we allow terms of the form $\iota x_\psi(\varphi)$, where φ and ψ are formulae of the ι-calculus and x is a variable symbol. This kind of terms will be called **ι-term**s. We call ψ the **domain formula** and φ the **definiens** of the ι-term.

The **formula**e are built up following the same rules as the ι-free calculus, except that as terms we of course use terms of the ι-calculus.

We will use the metalogical symbols $\equiv$ and $\not\equiv$ to express that two sequences of symbols are equal or not equal. We will often use variable names as x where we actually mean names for a variable name (just like we did when we said 'terms of the form $\iota x_\psi(\varphi)$', where x can be any variable symbol).

If α is a formula, then informally, $\mathbf{\Delta}(\alpha)$ is defined as the formula that states when α is defined. However, $\mathbf{\Delta}(\alpha)$ may also be the symbol $\top$ in case α is always defined. The logic will be constructed in such a way that the symbol $\top$ never will occur inside sequents; it is just a syntactical device to aid in the construction of $\mathbf{\Delta}(\alpha)$. Semantically, $\top$ will behave as if its interpretation were 'true'.

For example, $\mathbf{\Delta}(\iota x_{y\neq 0}(x \cdot y = 1) > 0)$ will be the formula $y \neq 0$. Note that the symbol $\mathbf{\Delta}$ is not part of our formal language; $\mathbf{\Delta}(\alpha)$ is a metalogical operator that maps the formula α to another formula or the symbol $\top$.

Likewise, if t is a term, $\mathbf{\Delta}(t)$ will be the formula that states when t is defined, so $\mathbf{\Delta}(\iota x_{y\neq 0}(x \cdot y = 1)) \equiv y \neq 0$.

Formally, $\mathbf{\Delta}(t)$ is defined as follows:

- If t is a variable symbol, then $\mathbf{\Delta}(t)$ is $\top$.
- $\mathbf{\Delta}(f(t_1, t_2, \ldots)) \equiv \mathbf{\Delta}(t_1) \,\&\mathbf{\Delta}(t_2) \,\& \ldots$ and for 0-ary function symbols $\mathbf{\Delta}(f()) \equiv \top$.
- $\mathbf{\Delta}(\iota x_\psi(\varphi)) \equiv \psi$.

One could also express these rules less formally as $\mathbf{\Delta}(t) \equiv \psi_1 \& \psi_2 \& \ldots$ where $\psi_1, \psi_2, \ldots$ are the domain formulae of the top-level ι-terms of t (i.e., those ι-terms that are themselves not contained into another ι-term), in their order of appearance from left to right in the term t.

As indicated above, we don't want the symbol $\top$ to occur in sequents. To achieve this, we will assume that formulae containing $\top$ are automatically simplified with the rules

$$\begin{array}{rcl} \alpha\&\top & \rightarrow & \alpha \\ \top\&\alpha & \rightarrow & \alpha \\ \forall x(\top) & \rightarrow & \top \end{array}$$

We see that, using these rules, either the symbol $\top$ does not occur in $\mathbf{\Delta}(t)$ or $\mathbf{\Delta}(t) \equiv \top$.

For formulae, the formal definition of $\mathbf{\Delta}(\alpha)$ is

- $\mathbf{\Delta}(t_1 = t_2) \equiv \mathbf{\Delta}(t_1) \,\&\mathbf{\Delta}(t_2)$
- $\mathbf{\Delta}(p(t_1, t_2, \ldots)) \equiv \mathbf{\Delta}(t_1) \,\&\mathbf{\Delta}(t_2) \,\& \ldots$; for 0-ary predicate symbols we have again $\mathbf{\Delta}(p(t_1, t_2, \ldots)) \equiv \top$
- $\mathbf{\Delta}(\neg\alpha) \equiv \mathbf{\Delta}(\alpha)$.
- $\mathbf{\Delta}(\alpha\&\beta) \equiv \mathbf{\Delta}(\alpha) \,\&(\alpha \Rightarrow \mathbf{\Delta}(\beta))$.
- $\mathbf{\Delta}(\forall x(\alpha)) \equiv \forall x(\mathbf{\Delta}(\alpha))$.

For atomic formulae α, we see again that $\mathbf{\Delta}(\alpha) \equiv \psi_1 \& \psi_2 \& \dots$ where $\psi_1, \psi_2, \dots$ are the domain formulae of the top-level ι-terms of α in their order of appearance from left to right in α.

Finally, we define $\mathbf{\Delta}(\top) \equiv \top$.

A term $\iota x_\psi(\varphi)$ has as free variables the union of the free variables of φ except x (which we call a bound variable of the term) and the free variables of ψ. Symbolically, if we denote the set of free variables of a term t as $FV(t)$, then $FV(\iota x_\psi(\varphi)) = (FV(\varphi) \setminus \{x\}) \cup FV(\psi)$.

We denote the substitution of all free occurrences of a term t for a variable symbol x in a formula α or term T as $[t/x]\alpha$ resp. $[t/x]T$. The substitution is defined in the same way as in the ι-free calculus (in particular, the substitution cannot take place when free variables of t would become bound); substituting in ι-terms is defined as follows:

- If $x \equiv y$ or if x is not a free variable of φ, then $[t/x]\iota y_\psi(\varphi) \equiv \iota y_\psi(\varphi)$ when x is not a free variable of ψ, or $[t/x]\iota y_\psi(\varphi) \equiv \iota y_{\mathbf{\Delta}(t)\&[t/x]\psi}(\varphi)$ when x is a free variable of ψ.
- If $x \not\equiv y$ and x is a free variable of φ and y is not a free variable of t, then then $[t/x]\iota y_\psi(\varphi) \equiv \iota y_{\mathbf{\Delta}(t)\&[t/x]\psi}([t/x]\varphi)$.
- If $x \not\equiv y$ and x is a free variable of φ and y is a free variable of t, then $[t/x]\iota y_\psi(\varphi)$ is undefined; we say that the substitution would capture the free variable y of t.

A **ι-sequent** is an expression of the form

$$\sigma_1, \sigma_2, \dots ; \gamma_1, \gamma_2, \dots \vdash_\iota \alpha$$

where the σs, γs and α are formulae of the ι-calculus. If there are no σs, then the leading semicolon is to be dropped.

The finite and possibly empty list $\sigma_1, \sigma_2, \dots$ is called the **context** of the sequent; the finite and possibly empty list $\gamma_1, \gamma_2, \dots$ is called the **antecedent** and the mandatory formula α is the **consequent**.

As before, the order of the formulae of the antecedent is not important and we suppose that no double formulae occur. However, the order of the formulae in the context is significant. When the context contains double formulae, we consider the sequent identical to the same sequent in which we only keep the first copy of the double formula in the context.

Note that the derivability relation of the ι-calculus is noted as $\vdash_\iota$ whereas we denote the derivability relation of the ι-free calculus with $\vdash$.

3 Semantics

We start from a **domain** D, which must be a non-empty set. An **interpretation** is a function $\mathcal{I}$ defined on the variable, function and predicate symbols, such that

- for each variable symbol x we have $\mathcal{I}(x) \in D$

- for each n-ary function symbol f, $\mathcal{I}(f)$ is a n-place function over D
- for each n-ary predicate symbol p, $\mathcal{I}(p)$ is a n-place predicate over D

Intuitively, an interpretation fixes a 'meaning' for each symbol of the formal language.

Remark that all functions and predicates above are total, i.e., defined for all n-tuples of elements of D where n is the arity of the function or predicate.

An interpretation depends on the domain chosen, so actually we should write $\mathcal{I}_D$, but in the sequel we suppose the domain to be a fixed set and just write $\mathcal{I}$ to ease the notation.

Given an interpretation $\mathcal{I}$, a variable symbol x and an element $a \in D$, we define a new interpretation $\mathcal{I}_x^a$ as follows:

- $\mathcal{I}_x^a(x) = a$
- $\mathcal{I}_x^a(y) = \mathcal{I}(y)$ if $x \not\equiv y$.

We write $\mathcal{I}_{xy}^{ab}$ as an abbreviation of $(\mathcal{I}_x^a)_y^b$.

Starting from $\mathcal{I}$, we can associate to each term t an element of D or the status '**undefined**'. As not to burden the notation, we will note this element (or the status 'undefined') too as $\mathcal{I}(t)$. It is defined as follows:

- $\mathcal{I}(\iota x_\psi(\varphi))$ is undefined if ψ is invalid or undefined in $\mathcal{I}$. If ψ is valid in $\mathcal{I}$, then $\mathcal{I}(\iota x_\psi(\varphi))$ is the $a \in D$ such that φ is valid in $\mathcal{I}_x^a$. If there is no such a, or there are multiple such a, then $\mathcal{I}(\iota x_\psi(\varphi))$ is undefined. (Note that the notions 'valid' and 'invalid' will be defined shortly.)
- $\mathcal{I}(f(t_1, \ldots, t_n)) = \mathcal{I}(f)(\mathcal{I}(t_1), \ldots, \mathcal{I}(t_n))$, provided all $\mathcal{I}(t_i)$ are defined; else $\mathcal{I}(f(t_1, \ldots, t_n))$ is undefined.

Note that again, for function symbols f and predicate symbols p, $\mathcal{I}(f)$ and $\mathcal{I}(p)$ are supposed to be total functions resp. predicates. Also, the interpretation of a variable symbol is always an element of D; it can never be undefined. Support for partially defined functions and predicates will be given in §8. Hence, for now, the only "source of undefinedness" are the ι-terms.

We attach to a formula α and an interpretation $\mathcal{I}$ the status valid, invalid or **undefined** as follows:

- If α is atomic, then we say that $t_1 = t_2$ is valid in $\mathcal{I}$ if both t_i are defined and $\mathcal{I}(t_1) = \mathcal{I}(t_2)$. We say that $p(t_1, \ldots, t_n)$ is valid in $\mathcal{I}$ if all t_i are defined and $\mathcal{I}(p)(\mathcal{I}(t_1), \ldots, \mathcal{I}(t_n))$ holds. However, if not all $\mathcal{I}(t_i)$ are defined, we say that α is undefined. In all other cases, α is invalid.
- $\neg\alpha$ is valid in $\mathcal{I}$ if α is invalid in $\mathcal{I}$; $\neg\alpha$ is invalid in $\mathcal{I}$ if α is valid in $\mathcal{I}$; $\neg\alpha$ is undefined if α is undefined.
- $\alpha\&\beta$ is valid in $\mathcal{I}$ if both α and β are valid in $\mathcal{I}$; $\alpha\&\beta$ is invalid when α is invalid, or when α is valid and β is invalid; else $\alpha\&\beta$ is undefined. (This is the McCarthy conjunction.)

- $\forall x(\alpha)$ is valid in $\mathcal{I}$ if for each $a \in D$, α is valid in $\mathcal{I}^a_x$. If there exist one or more $a \in D$ such that α is undefined in $\mathcal{I}^a_x$, then we say that $\forall x(\alpha)$ is undefined. In all other cases, α is invalid.

When a formula is valid or invalid, we will call it **defined**.

Note that we use the term 'undefined' in two contexts: a substitution can be undefined in the sense that the *substitution* $[t/x]\alpha$ cannot take place, hence this is a syntactical notion; on the other hand, a term or a formula of the ι-calculus can be undefined in an *interpretation* $\mathcal{I}$, so this is a semantical notion. It will be clear from the context which kind of 'undefined' we mean in the sequel.

Let $\Sigma \equiv \sigma_1, \sigma_2, \ldots$ If for an interpretation $\mathcal{I}$, the following three conditions hold, then we say that α is a **consequence in $\mathcal{I}$** of $\Sigma; \Gamma$:

- whenever all formulae of Γ and Σ are valid in $\mathcal{I}$, then also α is valid in $\mathcal{I}$.
- whenever all formulae of Σ are valid in $\mathcal{I}$, then all formulae of Γ are defined in $\mathcal{I}$.
- σ_1 is defined in $\mathcal{I}$; when σ_1 is valid in $\mathcal{I}$, σ_2 is defined in $\mathcal{I}$; when σ_1 and σ_2 are valid in $\mathcal{I}$, σ_3 is defined in $\mathcal{I}$, and so on. This is equivalent to requiring that the formula $\sigma_1 \& \sigma_2 \& \ldots$ is defined in $\mathcal{I}$.

We denote this as $\Sigma; \Gamma \models^{\mathcal{I}}_{\iota} \alpha$.

If these conditions hold for any interpretation $\mathcal{I}$, then we say that α is a **consequence** of $\Sigma; \Gamma$. We denote this as $\Sigma; \Gamma \models_{\iota} \alpha$.

3.1 Motivation

Equivalently, we can determine whether $\Sigma; \Gamma \models^{\mathcal{I}}_{\iota} \alpha$ using the following procedure. First, examine σ_1. If it is undefined, then α is not a consequence of $\Sigma; \Gamma$, which we will denote as $\Sigma; \Gamma \not\models_{\iota} \alpha$. If σ_1 is invalid, then $\Sigma; \Gamma \models^{\mathcal{I}}_{\iota} \alpha$. If it is valid, then examine σ_2. We then proceed similarly as with σ_1 and continue until we have processed Σ completely. If all σ_i are valid, we consider Γ: if at least one γ_i is undefined then $\Sigma; \Gamma \not\models_{\iota} \alpha$; else if at least one is invalid then $\Sigma; \Gamma \models^{\mathcal{I}}_{\iota} \alpha$; if they are all valid then finally we also have to examine α. If α is undefined or invalid then $\Sigma; \Gamma \not\models_{\iota} \alpha$; if it is valid then $\Sigma; \Gamma \models^{\mathcal{I}}_{\iota} \alpha$.

Thus there are two "left-to-right evaluation" elements in our calculus: the definition of conjunction and the definition of consequence. In our view, this is the reflection of the way in which 'common mathematical practice' deals with undefined terms: one is not permitted to prove something about potentially undefined terms like $\frac{1}{x}$ unless one *first* ascertains that $x \neq 0$; the "left-to-right" way of evaluating gives us a way to assert the validity of certain formulae *before* that of others.

Hence, for example, $x = \frac{1}{0} \not\models_{\iota} x \neq 5$ but $x \neq 0 \models_{\iota} \frac{1}{0} \neq 0$. In the first case, we are not permitted to consider $\frac{1}{0}$ because it is possible that $x = 0$; in the second case, this is impossible, because when we have to evaluate $\frac{1}{0} \neq 0$, earlier, $\mathcal{I}(x \neq 0)$ must have been valid.

Note that in contrast, $\forall x(\alpha)$ is undefined as soon as $\mathcal{I}^a_x(\alpha)$ is undefined for one $a \in D$, even though there might be $b \in D$ for which $\mathcal{I}^a_x(\alpha)$ is invalid, which seems to run counter to the idea of universal quantification as a ‘generalised conjunction’. However, in general, there is no natural order in which we can enumerate the elements of D; if we were to start with a, the generalised conjunction would evaluate as undefined, whereas if we started with b, it would yield invalidity. Since as indicated, we wish to avoid to reason about potentially undefined terms, the only safe choice is to consider $\forall x(\alpha)$ as undefined.

4 Deduction rules

Double formulae are to be removed from the antecedent of the conclusion. For the context of the conclusion, the same holds, but here we cannot choose arbitrarily which copy we keep: we have to keep the first instance of a formula and remove the others. Note that a formula is allowed to occur both in the antecedent and the context of the conclusion; we do not remove those double formulae. For example, we will assume that the sequent

$$\alpha, \alpha, \beta, \alpha, \gamma, \beta; \gamma, \gamma, \alpha \vdash_\iota \delta$$

is automatically rewritten into $\alpha, \beta, \gamma; \gamma, \alpha \vdash_\iota \delta$ or $\alpha, \beta, \gamma; \alpha, \gamma \vdash_\iota \delta$; these are the only two valid forms of that sequent.

Also note that the order of the premises is significant; e.g., when we interchange both premises of the &-introduction rule, we get a different sequent, $\Sigma_2, \Sigma_1; \Gamma, \Delta \vdash_\iota \beta \& \alpha$ as a result:

$$\frac{\begin{array}{rcl} \Sigma_2; \Gamma & \vdash_\iota & \beta \\ \Sigma_1; \Delta & \vdash_\iota & \alpha \end{array}}{\begin{array}{rcl} \Sigma_2, \Sigma_1; \Gamma, \Delta & \vdash_\iota & \beta \& \alpha \end{array}}$$

The **uniqueness condition** corresponding to a ι-term $\iota x_\psi(\varphi)$ is the sequent

$$\psi \vdash_\iota \exists! x(\varphi)$$

where $\exists! x(\varphi)$ is an abbreviation for $\exists x(\varphi) \& \forall x \forall y((\varphi \& [y/x]\varphi) \Rightarrow x = y)$ where y is a variable symbol not occuring in φ and $\alpha \Rightarrow \beta$ is shorthand for $\neg(\alpha \& \neg\beta)$.

Given a formula α, we denote the list containing the uniqueness conditions corresponding to all its ι-terms as $UC(\alpha)$.

Concerning the $\top$ symbol, we introduce the following conventions which will ascertain that the $\top$ symbol never will occur inside sequents, as we already announced:

- If $\top$ would occur inside the context or antecedent of a sequent, it is removed from the context or antecedent. For example, the sequent $\top, \alpha; \beta, \top \vdash_\iota \gamma$ is to be rewritten as $\alpha; \beta \vdash_\iota \gamma$.

- If $\top$ would occur as consequent, the whole sequent is simply dropped. For example, if a proof rule would require $\Sigma; \Gamma \vdash_\iota \top$ as premise, that premise doesn't need to be supplied.

Assumption introduction:
$$\frac{\begin{array}{rcl} & UC(\alpha) & \\ \Sigma; & \vdash_\iota & \mathbf{\Delta}(\alpha) \end{array}}{\begin{array}{rcl} \Sigma; \alpha & \vdash_\iota & \alpha \end{array}}$$

According to the convention given above, if $\mathbf{\Delta}(\alpha)$ is $\top$, then the $\Sigma; \vdash_\iota \mathbf{\Delta}(\alpha)$ premise is to be dropped (note that in this case, it is easy to see that $UC(\alpha)$ is empty so this rule then requires no premises at all).

&-introduction: $$\frac{\begin{array}{c}\Sigma_1;\Gamma \ \vdash_\iota \ \alpha \\ \Sigma_2;\Delta \ \vdash_\iota \ \beta\end{array}}{\Sigma_1,\Sigma_2;\Gamma,\Delta \ \vdash_\iota \ \alpha\&\beta}$$

&-elimination: $$\frac{\Sigma;\Gamma \ \vdash_\iota \ \alpha\&\beta}{\Sigma;\Gamma \ \vdash_\iota \ \alpha} \qquad \frac{\Sigma;\Gamma \ \vdash_\iota \ \alpha\&\beta}{\Sigma;\Gamma \ \vdash_\iota \ \beta}$$

Removal: $$\frac{\begin{array}{c}\Sigma_1;\Gamma,\alpha \ \vdash_\iota \ \beta \\ \Sigma_2;\Delta,\neg\alpha \ \vdash_\iota \ \beta\end{array}}{\Sigma_1,\Sigma_2;\Gamma,\Delta \ \vdash_\iota \ \beta}$$

Contradiction: $$\frac{\begin{array}{c}UC(\beta) \\ \Sigma_1;\Gamma \ \vdash_\iota \ \alpha \\ \Sigma_2;\Delta \ \vdash_\iota \ \neg\alpha\end{array}}{\Sigma_1,\Sigma_2;\Gamma,\Delta \ \vdash_\iota \ \beta}$$

$\forall$-introduction: $$\frac{\Sigma;\Gamma \ \vdash_\iota \ \alpha}{\Sigma;\Gamma \ \vdash_\iota \ \forall x(\alpha)} \text{ provided } x \text{ is not free in } \Gamma \text{ and } \Sigma$$

$\forall$-elimination: $$\frac{\Sigma;\Gamma \ \vdash_\iota \ \forall x(\alpha)}{\Sigma;\Gamma \ \vdash_\iota \ \alpha}$$

Substitution: $$\frac{\begin{array}{c}UC(t) \\ \Sigma;\Gamma \ \vdash_\iota \ \alpha\end{array}}{\boldsymbol{\Delta}(t)\,,[t/x]\Sigma;[t/x]\Gamma \ \vdash_\iota \ [t/x]\alpha}$$

where $[t/x]\Gamma$ is shorthand for $[t/x]\gamma_1,[t/x]\gamma_2,\ldots$ with $\Gamma \equiv \gamma_1,\gamma_2,\ldots,\gamma_n$. The notation $\alpha\&\Gamma$ stands for $\alpha\&\gamma_1,\alpha\&\gamma_2,\ldots$; when Γ is empty it is shorthand for α.

Equality rules: $$\frac{UC(t)}{\boldsymbol{\Delta}(t) \ \vdash_\iota \ t=t} \qquad \frac{\begin{array}{c}UC(t) \\ \Sigma;\Gamma \ \vdash_\iota \ \alpha\end{array}}{\Sigma,\boldsymbol{\Delta}(t)\,;\Gamma,x=t \ \vdash_\iota \ [t/x]\alpha}$$

ι-rule: $$\frac{UC(\iota x_\psi(\varphi))}{\psi \ \vdash_\iota \ [\iota x_\psi(\varphi)/x]\widetilde{\varphi}}$$

where $\widetilde{\varphi}$ is obtained from φ by changing the names of all bound variables, i.e., $\widetilde{x} \equiv x$; $\widetilde{f}(t_1,\ldots) \equiv f(\widetilde{t_1},\ldots)$; $\widetilde{\iota x_\psi(\phi)} \equiv \iota y_{\widetilde{\psi}}([y/x]\widetilde{\phi})$ where y is not a free variable of φ and $\widetilde{\phi}$; $\widetilde{p}(t_1,\ldots) \equiv p(\widetilde{t_1},\ldots)$; $\widetilde{\alpha\&\beta} \equiv \widetilde{\alpha}\&\widetilde{\beta}$; $\widetilde{\neg\alpha} \equiv \neg\widetilde{\alpha}$ and $\widetilde{\forall x(\alpha)} \equiv \forall y([y/x]\widetilde{\alpha})$ where y is not a free variable of φ and $\widetilde{\alpha}$.

$\boldsymbol{\Delta}$-rules; only applicable when the consequent of the conclusion is not $\top$:

$$\frac{UC(\alpha)}{\vdash_\iota \ \boldsymbol{\Delta}(\boldsymbol{\Delta}(\alpha))} \qquad \frac{\Sigma;\Gamma,\alpha \ \vdash_\iota \ \beta}{\Sigma; \ \vdash_\iota \ \boldsymbol{\Delta}(\alpha)} \qquad \frac{\Sigma;\Gamma \ \vdash_\iota \ \alpha}{\Sigma;\Gamma \ \vdash_\iota \ \boldsymbol{\Delta}(\alpha)}$$

Finally, we add these rules for manipulating contexts:

$$\frac{\Sigma;\sigma\&\Gamma,\Delta \ \vdash_\iota \ \alpha}{\Sigma,\sigma;\Gamma,\Delta \ \vdash_\iota \ \alpha} \qquad \frac{\Sigma,\sigma;\Gamma \ \vdash_\iota \ \alpha}{\Sigma;\sigma\&\Gamma \ \vdash_\iota \ \alpha}$$

5 Equiconsistency proof

In this section, we will give a process to transform a sequent in the ι-calculus to one or more sequents in the ι-free calculus.

We define two metalogical operations on formulae α of the ι-calculus: the reduction $\mathcal{R}(\alpha)$ and the definedness $\mathcal{D}(\alpha)$. Both produce a sequent of the ι-free calculus. Semantically, $\mathcal{R}(\alpha)$ will express that if α is defined, it is true (or equivalently, that α is undefined or true), and $\mathcal{D}(\alpha)$ will express that α is defined.

We define $\mathcal{R}$ by structural induction on the formula α:

- α is an atomic formula, i.e., $\alpha \equiv t_1 = t_2$ or $\alpha \equiv p(t_1, t_2, \ldots)$. We will only cover the latter case; the former is analogous. We enumerate all top-level ι-terms of α (i.e., those ι-terms that are themselves not contained into another ι-term) as $\iota x_{1\psi_1}(\varphi_1)$, $\iota x_{2\psi_2}(\varphi_2)$, $\ldots$ We define $\mathcal{R}(\alpha)$ as

  $$\exists u_1 \exists u_2 \ldots (\mathcal{R}([u_1/x_1]\varphi_1) \& \mathcal{R}([u_2/x_2]\varphi_2) \& \ldots \& q)$$

  where q is the formula obtained from α by replacing all top-level ι-terms $\iota x_{i\psi_i}(\varphi_i)$ by their corresponding variable symbol u_i. We choose the u_is such that they are all different from each other and such that u_i does not occur in α.
  If there are no ι-term arguments of p, then we define $\mathcal{R}(\alpha) \equiv \alpha$.

- $\mathcal{R}(\neg\alpha) \equiv \neg\mathcal{R}(\alpha)$

- $\mathcal{R}(\alpha \& \beta) \equiv \mathcal{R}(\alpha) \& \mathcal{R}(\beta)$

- $\mathcal{R}(\forall x(\alpha)) \equiv \forall x(\mathcal{R}(\alpha))$

Note that this is the same definition as in [Hilbert and Bernays 1968], except that there, $u_i \equiv x_i$ is chosen, which is incorrect when two or more x_i's are the same variable symbol.

Next, we define $\mathcal{D}$:

- $\mathcal{D}(p(t_1, t_2, \ldots)) \equiv \mathcal{R}(\psi_1) \& \mathcal{R}(\psi_2) \& \ldots$ with the same notations as in the definition of $\mathcal{R}$. If there are no ι-terms as argument of p, then $\mathcal{D}(p(\ldots)) \equiv \forall x(x = x)$. We treat $\mathcal{D}(t_1 = t_2)$ analogously. Note that it would be natural to define $\mathcal{D}(p(t_1, t_2, \ldots)) \equiv \mathcal{R}(\psi_1) \& \mathcal{D}(\psi_1) \& \ldots$ but it appears that we get $\mathcal{D}(\psi_i)$ from the uniqueness condition for $\iota x_{i\psi_i}(\varphi_i)$.

- $\mathcal{D}(\neg\alpha) \equiv \mathcal{D}(\alpha)$

- $\mathcal{D}(\alpha \& \beta) \equiv \mathcal{D}(\alpha) \& (\mathcal{R}(\alpha) \Rightarrow \mathcal{D}(\beta))$

- $\mathcal{D}(\forall x(\alpha)) \equiv \forall x(\mathcal{D}(\alpha))$

5.1 Translation of proofs

We define the **translation** of a ι-sequent $\Sigma; \Gamma \vdash_\iota \alpha$ as the three sequents

$$\begin{cases} & \vdash \mathcal{D}(\sigma_1 \& \sigma_2 \& \ldots \& \sigma_n) \\ \mathcal{R}(\sigma_1), \mathcal{R}(\sigma_2), \ldots, \mathcal{R}(\sigma_n) & \vdash \mathcal{D}(\gamma_1) \& \mathcal{D}(\gamma_2) \& \ldots \\ \mathcal{R}(\sigma_1), \mathcal{R}(\sigma_2), \ldots, \mathcal{R}(\sigma_n), \mathcal{R}(\gamma_1), \mathcal{R}(\gamma_2), \ldots & \vdash \mathcal{R}(\alpha) \& \mathcal{D}(\alpha) \end{cases}$$

where $\Sigma \equiv \sigma_1, \sigma_2, \ldots, \sigma_n$ and $\Gamma \equiv \gamma_1, \gamma_2, \ldots$ If Γ is the empty list, then we drop the second sequent of the translation.

One can now prove that given a correct ι-proof of a ι-sequent, one can obtain a proof in the ι-free calculus of its translation. One shows this by examining all deduction rules of the ι-calculus in turn and proving that one can find a proof in the ι-free calculus of the translation of the conclusion of that rule, given the translation of the premises.

Just like in [Hilbert and Bernays 1968, pp. 441–448], for most rules this is fairly easy; the rules involving substitution are more complicated. In [Hilbert and Bernays 1968],the key step is to prove that, using our notations,

$$\vdash (\forall x(\mathcal{R}(\varphi) \Rightarrow \mathcal{R}(\alpha))) \Leftrightarrow \mathcal{R}([\iota x_\psi(\varphi)/x]\alpha)$$

is derivable from the uniqueness condition $\vdash \exists! x(\mathcal{R}(\varphi))$. Analogously, the key step in our proof is to prove that

$$\mathcal{R}(\psi) \vdash_\iota (\forall x(\mathcal{R}(\varphi) \Rightarrow \mathcal{R}(\alpha))) \Leftrightarrow \mathcal{R}([\iota x_\psi(\varphi)/x]\alpha)$$

is derivable from the translation of the uniqueness condition of $\iota x_\psi(\varphi)$; Hilbert and Bernays' proof is rather easy to extend to this case.

Of course, we also need to prove some extra properties concerning $\mathcal{D}$, among which

$$\begin{array}{rcl}
\mathcal{R}(\boldsymbol{\Delta}(\alpha)) & \dashv\vdash & \mathcal{D}(\alpha) \\
\mathcal{D}(t), \forall x(\mathcal{R}(\alpha)) & \vdash & \mathcal{R}([t/x]\alpha) \\
\mathcal{D}(t), \mathcal{R}([t/x]\mathcal{D}(\alpha)) & \vdash & \mathcal{D}([t/x]\alpha) \\
\mathcal{D}(t), \forall x(\mathcal{D}(\alpha)) & \vdash & \mathcal{D}([t/x]\alpha)
\end{array}$$

are useful lemmas.

5.2 Equiconsistency

Suppose that the ι-calculus would be inconsistent, i.e., every ι-sequent is derivable in the ι-calculus. In particular, the sequent $\vdash \neg(x = x)$ would then be derivable in the ι-calculus. Translating the ι-proof of this sequent, we get a proof whose last sequent is

$$\vdash \mathcal{R}(\neg(x = x)) \& \mathcal{D}(\neg(x = x)) \quad \text{, i.e.,} \qquad \vdash \neg(x = x) \& \forall x(x = x)$$

But then we would have a proof (in the ι-free calculus) of $\vdash \neg(x = x)$, and it is easy to see that this would imply that the ι-free calculus would be inconsistent.

5.3 Conservativeness of the extension

The ι-calculus is a conservative extension of the ι-free calculus, i.e., if a given sequent $\Gamma \vdash \alpha$ is not derivable in the ι-free calculus, it remains underivable in the ι-calculus.

Indeed, suppose that we would have a ι-proof of $\Gamma \vdash_\iota \alpha$. As shown above, we can translate this into a proof of its translation, and hence we get a proof of $\mathcal{R}(\gamma_1), \cdots \vdash \mathcal{R}(\alpha)$, i.e., of $\Gamma \vdash \alpha$, a contradiction.

6 Soundness

We first prove a connection between the semantics and the operations $\mathcal{R}$ and $\mathcal{D}$.

Lemma 1. *Given a formula α of the ι-calculus and an interpretation $\mathcal{I}$. Suppose that the uniqueness conditions of all ι-terms in α are valid in $\mathcal{I}$. Then*

$$\begin{array}{rcl} \alpha \textit{ is valid in } \mathcal{I} & \Leftrightarrow & \mathcal{R}(\alpha)\&\mathcal{D}(\alpha) \textit{ is valid in } \mathcal{I} \textit{ (in the } \iota\textit{-free calculus)} \\ \alpha \textit{ is invalid in } \mathcal{I} & \Leftrightarrow & \neg\mathcal{R}(\alpha)\&\mathcal{D}(\alpha) \textit{ is valid in } \mathcal{I} \textit{ (in the } \iota\textit{-free calculus)} \\ \alpha \textit{ is undefined in } \mathcal{I} & \Leftrightarrow & \neg\mathcal{D}(\alpha) \textit{ is valid in } \mathcal{I} \textit{ (in the } \iota\textit{-free calculus)} \end{array}$$

One proves this by structural induction on α.

Theorem 2 (Soundness of the ι-calculus). *If $\Gamma \vdash_\iota \alpha$, then also $\Gamma \models_\iota \alpha$.*

Proof. We know that if we hava a ι-proof of $\Gamma \vdash_\iota \alpha$, we can translate this into a proof in the ι-free calculus, i.e., we obtain a proof of the sequents

$$\left\{ \begin{array}{rcl} & \vdash & \mathcal{D}(\gamma_1)\&\mathcal{D}(\gamma_2)\&\ldots\&\mathcal{D}(\gamma_n) \\ \mathcal{R}(\gamma_1), \mathcal{R}(\gamma_2), \ldots, \mathcal{R}(\gamma_n) & \vdash & \mathcal{R}(\alpha)\&\mathcal{D}(\alpha) \end{array} \right.$$

We have to prove $\Gamma \models_\iota \alpha$, which means that

- For any interpretation $\mathcal{I}$, if γ_1, γ_2, ... are valid in $\mathcal{I}$, then α is valid too in $\mathcal{I}$. Using the previous lemma, this is equivalent with proving in the ι-free calculus that if $\mathcal{R}(\gamma_1)\&\mathcal{D}(\gamma_1)\&\mathcal{R}(\gamma_2)\&\mathcal{D}(\gamma_2)\&\ldots$ is valid, then $\mathcal{R}(\alpha)\&\mathcal{D}(\alpha)$ is valid, i.e.,

  $$\mathcal{R}(\gamma_1), \mathcal{D}(\gamma_1), \mathcal{R}(\gamma_2), \mathcal{D}(\gamma_2), \ldots \models \mathcal{R}(\alpha)\&\mathcal{D}(\alpha)$$

  Because of the soundness of the ι-free calculus, this amounts to

  $$\mathcal{R}(\gamma_1), \mathcal{D}(\gamma_1), \mathcal{R}(\gamma_2), \mathcal{D}(\gamma_2), \ldots \vdash \mathcal{R}(\alpha)\&\mathcal{D}(\alpha)$$

  which follows easily from the second sequent of the translation given.

- There exist no interpretations in which a γ_i is undefined. Hence, in each interpretation, γ_i must be valid or invalid, which we can express using the previous lemma as $\models (\mathcal{R}(\gamma_i)\&\mathcal{D}(\gamma_i)) \vee (\neg\mathcal{R}(\gamma_i)\&\mathcal{D}(\gamma_i))$ which is equivalent with $\models \mathcal{D}(\gamma_i)$. Again, because of the completeness of the ι-free calculus, we have to prove that $\vdash \mathcal{D}(\gamma_i)$, which follows easily from the first sequent of the translation.

■

Note that this is a *relative* soudness proof: the ι-calculus is proved sound if we assume the ι-free calculus to be sound.

7 Completeness

In this section we will prove the competeness of the ι-calculus, i.e.,

$$\text{if } \Gamma \models_\iota \alpha \text{ then also } \Gamma \vdash_\iota \alpha$$

Denote $\Gamma \equiv \gamma_1, \gamma_2, \ldots$ By definition, $\Gamma \models_\iota \alpha$ means that for any interpretation $\mathcal{I}$,

- whenever all γ_i are valid in $\mathcal{I}$, then so is α. Using lemma 1, this is equivalent with
$$\mathcal{R}(\gamma_1)\&\mathcal{D}(\gamma_1), \mathcal{R}(\gamma_2)\&\mathcal{D}(\gamma_2), \ldots \models \mathcal{R}(\alpha)\&\mathcal{D}(\alpha)$$
- all γ_i are defined in $\mathcal{I}$, which is by the same lemma equivalent with
$$\begin{cases} \models \mathcal{D}(\gamma_1) \\ \models \mathcal{D}(\gamma_2) \\ \models \ldots \end{cases}$$

Using the completeness of the ι-free calculus, what we have to prove is reduced to a syntactical problem:

$$\text{if} \begin{cases} \mathcal{R}(\gamma_1)\&\mathcal{D}(\gamma_1), \mathcal{R}(\gamma_2)\&\mathcal{D}(\gamma_2), \ldots & \vdash \; \mathcal{R}(\alpha)\&\mathcal{D}(\alpha) \\ & \vdash \; \mathcal{D}(\gamma_1) \\ & \vdash \; \mathcal{D}(\gamma_2) \\ & \vdash \; \ldots \end{cases}$$

then also $\Gamma \vdash_\iota \alpha$.

One can show that for each formula α of the ι-calculus, one can derive

$$\begin{cases} \mathbf{\Delta}(\alpha)\,\&\alpha & \dashv\vdash_\iota \; \mathcal{D}(\alpha)\&\mathcal{R}(\alpha) \\ \mathbf{\Delta}(\alpha) & \dashv\vdash_\iota \; \mathcal{D}(\alpha) \end{cases}$$

The proof is by structural induction on α and uses a number of technical lemmas.

Using this result, it is easy to show the completeness of the ι-calculus.

Note that this is a *relative* completeness proof, since we assumed the completeness of the ι-free calculus.

8 Defined symbols

8.1 Simultaneous extended substitution

As in [Hermes 1973], given a formula α, terms $t_1, \ldots, t_n$ and variable symbols $x_1, \ldots, x_n$, where all x_i are different, we define the **simultaneous extended substitution** of α as follows:

$$\left[\tfrac{t_1}{x_1} \cdots \tfrac{t_n}{x_n}\right] \alpha \;:=\; \forall y_1 \ldots \forall y_n((y_1 = t_1 \& \ldots \& y_n = t_n) \Rightarrow \\ \forall x_1 \ldots \forall x_n \left((x_1 = y_1 \& \ldots \& x_n = y_n) \Rightarrow \alpha\right))$$

where the variable symbols $y_1, \ldots, y_n$ are different from each other and from $x_1, \ldots, x_n$ and do not occur in $t_1, \ldots, t_n$ or α.

8.2 Definitional axioms

We will show that informally, without affecting the consistency of the logic, one can admit the definition of a new function symbol g using an axiom of the form

$$\mathbf{\Delta}(t) \vdash_\iota g(x_1, \ldots, x_n) = t$$

where g is a new function symbol (i.e., it has not been defined in another axiom), where the set of free variables of the term t is a subset of $\{x_1, \ldots, x_n\}$ and t does not contain g. We call t the **definiens** of g, which we will also denote as g^*, and $\mathbf{\Delta}(t)$ its **domain formula**. Analogously, one can define a new predicate symbol q using an axiom of the form

$$\mathbf{\Delta}(\alpha) \vdash_\iota q(x_1, \ldots, x_n) \Leftrightarrow \alpha$$

where again the set of free variables of α is a subset of $\{x_1, \ldots, x_n\}$ and α does not contain q. We call α the **definiens** of q, which we also denote as q^*, and $\mathbf{\Delta}(\alpha)$ its **domain formula**.

We call the axioms above **definitional axiom**s and the symbols g resp. q **defined symbol**s.

Formally, we will again define a new calculus, which is a conservative extension of the ι-calculus. We will call this calculus the ι'-calculus, and note its sequents as $\Sigma; \Gamma \vdash_{\iota'} \alpha$, so the definitional axioms above should actually have read

$$\begin{array}{rcl} \mathbf{\Delta}'(t) & \vdash_{\iota'} & g(x_1, \ldots, x_n) = t \\ \mathbf{\Delta}'(\alpha) & \vdash_{\iota'} & q(x_1, \ldots, x_n) \Leftrightarrow \alpha \end{array}$$

where $\mathbf{\Delta}'$ is identical to $\mathbf{\Delta}$, except for the treatment of the freshly defined symbols:

$$\begin{array}{rcl} \mathbf{\Delta}'(g(t_1, \ldots, t_n)) & \equiv & \mathbf{\Delta}'(t_1) \& \ldots \& \mathbf{\Delta}'(t_n) \& \left[\frac{t_1}{x_1} \cdots \frac{t_n}{x_n}\right] \mathbf{\Delta}'(g^*) \\ \mathbf{\Delta}'(q(t_1, \ldots, t_n)) & \equiv & \mathbf{\Delta}'(t_1) \& \ldots \& \mathbf{\Delta}'(t_n) \& \left[\frac{t_1}{x_1} \cdots \frac{t_n}{x_n}\right] \mathbf{\Delta}'(q^*) \end{array}$$

The deduction rules of the ι'-calculus are the same as those of the ι-calculus, where $\mathbf{\Delta}'$ is used instead of $\mathbf{\Delta}$.

One can show that the addition of defined symbols does not render the calculus inconsistent, essentially by considering $q(t_1, \ldots, t_n)$ as an abbreviation for $\left[\frac{t_1}{x_1} \frac{t_2}{x_2} \cdots\right] q^*$ and analogously $g(t_1, \ldots, t_n)$ as an abbreviation for $\iota y_{\mathbf{\Delta}\left(\left[\frac{t_1}{x_1} \frac{t_2}{x_2} \cdots\right] (y = g^*)\right)} (\left[\frac{t_1}{x_1} \frac{t_2}{x_2} \cdots\right] (y = g^*))$.

References

[Farmer 1996] W. Farmer, Mechanizing the traditional approach to partial functions. In: W. Farmer, M. Kerber, and M. Kohlhase, eds., *Proceedings of the Workshop on the Mechanization of Partial Functions*, pp. 27–32, CADE-13, Rutgers University, New Brunswick, New Jersey, July 30, 1996.

[Hermes 1973] H. Hermes, Introduction to Mathematical Logic, Springer (1973).

[Hilbert and Bernays 1968] D. Hilbert, P. Bernays, Grundlagen der Mathematik I, 2nd ed., Springer (1968).

[Hoogewijs 1987] A. Hoogewijs, Partial Predicate Logic in Computer Science, Acta Informatica 24, pp 381–393, Springer Verlag, 1987.

[Whitehead and Russell 1910] A. Whitehead, B. Russell, Incomplete symbols: Descriptions, in J. van Heijenoort, From Frege to Gödel, pp 216–223, Harvard University Press, 1967.

[Whitehead and Russell 1964] A. Whitehead, B. Russell, Principia Mathematica, Cambridge University Press, 1964.

Department of Pure Mathematics and Computer Algebra
Gent University, Belgium
gvernaev@cage.UGent.be, bh@cage.UGent.be