8- dLPA$^\omega$: a sequent calculus with dependent types for classical arithmetic

Drawing on the calculi we studied in the last chapters, we shall now present dLPA$^\omega$, a sequent calculus version of Herbelin’s dPA$^\omega$. This calculus provides us with dependent types restricted to the NEF fragment, for which dLPA$^\omega$ is an extension of dL$^\omega$. Indeed, in addition to the language of dL$^\omega$, dLPA$^\omega$ has terms for classical arithmetic in finite types (PA$^\omega$). More importantly, it includes a lazily evaluated co-fixpoint operator. To this end, the calculus uses a shared store, as in the $\lambda[lvt\tau\star]$-calculus.

We first present the language of dLPA$^\omega$ with its type system and its reduction rules. We prove that the calculus verifies the property of subject reduction and that it is as expressive as dPA$^\omega$. In particular, the proof terms for AC and DC of dPA$^\omega$ can be directly defined in dLPA$^\omega$. We then apply once again the methodology of Danvy’s semantic artifacts to derive a small-step calculus, from which we deduce a continuation-passing-style translation and a realizability interpretation. Both artifacts are somehow a combination of the corresponding ones that we developed for the $\lambda[lvt\tau\star]$-calculus and dL$^\omega$.

In some sense, there will not be any real novelties in this chapter. In particular, most of the proofs resemble a lot to the corresponding ones in the previous chapters. Yet, as dLPA$^\omega$ gathers all the expressive power and features of the $\lambda[lvt\tau\star]$-calculus and dL$^\omega$, the different proofs also combined all the tools and tricks used in each case. They are therefore very technical and long, in particular proofs by induction require the tedious verification of multiple cases which are very similar to cases of proofs we already did. We will hence sketch them most of the time, trying to highlight the most interesting parts.

Normalization of dLPA$^\omega$

The main result of this chapter consists in the normalization of dLPA$^\omega$, from which it is easy to convince oneself that dPA$^\omega$ normalizes to $\mathbb{P}$. We sketch a proof of normalization through a continuation-passing-style translation, which would rely on the normalization of System $F_L$. We then give a detailed proof through the realizability interpretation.

Nonetheless, we should say before starting this chapter that we already have a guardrail for the normalization. Indeed, we already proved the normalization of a simply-typed classical call-by-need calculus and we explained that the proof was scalable to the same calculus with a second-order type system. Yet, co-fixpoints are definable in a second-order calculus, for instance a stream for the infinite conjunction $A(0) \land A(1) \land \ldots$ can be obtained through the formula $\exists X. [X(0) \land \forall x \in \mathbb{N}. (X(x) \rightarrow A(x) \land X(S(x)))]$. Besides, the presence of dependent types does not bring any risk of losing the normalization, since erasing the dependencies in types yield a system with the exact same computational behavior. Hence the normalization of dL$^\omega$ and the one of the second-order $\lambda[lvt\tau\star]$-calculus should be enough, a priori, to guarantee the normalization of dLPA$^\omega$.

---

1As explained in Chapter 5, we will not bother with a formal proof of this statement, neither will we prove any properties on the preservation of dPA$^\omega$ reduction rules through the embedding in dLPA$^\omega$. Indeed, we are already satisfied with the normalization of dLPA$^\omega$, which is as expressive as dPA$^\omega$ and which allows for the same proof terms for dependent and countable choice.

2A definition in the framework of dPA$^\omega$ is given in 70.
Another handwavy explanation could consist in arguing that we could authorize infinite stores in the \( \tilde{\lambda}_{[\text{UT}}{\text{●\text{●}}}] \)-calculus without altering its normalization. Indeed, from the point of view of existing programs (which are finite and typed in finite contexts), they are computing with a finite knowledge of the memory (and we proved that all the terms were suitable for a store extension\(^3\)). Note that in the store, we could theoretically replace any co-fixpoint that produces a stream by the (fully developed) stream in question. Due to the presence of backtracks in co-fixpoints, the store would contain all the possible streams (possibly an infinite number of it) produced when reducing co-fixpoints. In this setting, if a term were to perform an infinite number of reductions steps, it would necessarily have to explore an infinite number of cells in the pre-computed memory, independently from its production. This should not be possible either.

The latter argument is actually quite close from Herbelin’s original proof sketch, which this thesis is precisely trying to replace with a more formal proof. So that these unprecise explanations should be taken more as spoilers of the final result than as proof sketches. We shall now present formally dLPA\(\omega\) and prove its normalization, which will then not come as a surprise.

8.1 dLPA\(\omega\): a sequent calculus with dependent types for classical arithmetic

8.1.1 Syntax

The language of dLPA\(\omega\) should not be a surprise either. It is based on the syntax of dL\(\tilde{\varphi}\), extended with the expressive power of dPA\(\omega\) and with explicit stores as in the \( \tilde{\lambda}_{[\text{UT}}{\text{●\text{●}}}] \)-calculus. We stick to a stratified presentation of dependent types, which we find very convenient to separate terms and proof terms which are handled differently.

The syntax of terms is extended as in dPA\(\omega\) to include functions \( \lambda x.t \) and applications \( tu \), as well as a recursion operator \( \text{rec}_y^\infty[l_0 | t_S] \), so that terms represent objects in arithmetic of finite types.

As for proof terms (and contexts, commands), they are now defined with all the expressiveness of dPA\(\omega\) (see Chapter 5). Each constructor in the syntax of formulas is reflected by a constructor in the syntax of proofs and by the dual co-proof (i.e. destructor) in the syntax of evaluation contexts. Namely, the syntax is an extension of dL\(\tilde{\varphi}\)’s syntax which now includes:

- the usual proofs \( \mu e.c \) and contexts \( \tilde{\mu} a.c \) of the \( \lambda \tilde{\mu} \)-calculus;
- pairs \( (p_1,p_2) \), which inhabit the conjunction type \( A_1 \land A_2 \);
- co-pairs \( \tilde{\mu}(a_1,a_2).c \), which bind the variables \( a_1 \) and \( a_2 \) in the command \( c \);
- injections \( i_1(p) \) for the logical disjunction;
- co-injections or pattern-matching \( \tilde{\mu}(a_1,c_1|a_2,c_2) \) which bind the variables \( a_1 \) in \( c_1 \) and \( a_2 \) in \( c_2 \);
- pairs \( (t,p) \) where \( t \) is a term and \( p \) a proof, which inhabit the dependent sum type \( \exists x^T.A \);
- dual co-pairs \( \tilde{\mu}(x,a).c \) which bind the (term and proof) variables \( x \) and \( a \) in the command \( c \);
- functions \( \lambda x.p \), which inhabit the dependent product type \( \forall x^T.A \);
- dual stacks \( t \cdot e \), where \( t \) is a term and \( e \) a context whose type might be dependent in \( t \);
- functions \( \lambda a.p \), which inhabit the dependent product type \( \Pi a : A.B \);
- dual stacks \( q \cdot e \), where \( q \) is a term and \( e \) a context whose type might be dependent in \( q \) if \( q \) is \( \text{neq} \);
- a proof term \( \text{ref i} \) which is the proof of atomic equalities \( t = t \);
- the dual destructor \( \tilde{\rho}.c \) which allows to type the command \( c \) modulo an equality of terms;

\(^3\)See Lemma 6.16 for the realizability interpretation and Lemma 6.31 for the CPS translation of the \( \tilde{\lambda}_{[\text{UT}}{\text{●\text{●}}}] \)-calculus.
8.1. dLPA\(^\omega\): A SEQUENT CALCULUS WITH DEPENDENT TYPES FOR CLASSICAL ARITHMETIC

<table>
<thead>
<tr>
<th>Closures</th>
<th>( l ) ::= ( c\tau )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands</td>
<td>( c ) ::= ( \langle p</td>
</tr>
<tr>
<td>Proof terms</td>
<td>( p,q ) ::= ( a</td>
</tr>
<tr>
<td></td>
<td>(</td>
</tr>
<tr>
<td>Proof values</td>
<td>( V ) ::= ( a</td>
</tr>
<tr>
<td>Contexts</td>
<td>( e ) ::= ( f</td>
</tr>
<tr>
<td>Forcing contexts</td>
<td>( f ) ::= ( []</td>
</tr>
<tr>
<td>Stores</td>
<td>( \tau ) ::= ( \varepsilon</td>
</tr>
<tr>
<td>Storables</td>
<td>( p_\tau ) ::= ( V</td>
</tr>
<tr>
<td>Terms</td>
<td>( t,u ) ::= ( x</td>
</tr>
<tr>
<td>Terms values</td>
<td>( V_t ) ::= ( x</td>
</tr>
<tr>
<td>Delimited continuations</td>
<td>( c_\phi ) ::= ( \langle \mu_\Phi</td>
</tr>
<tr>
<td></td>
<td>( e_\phi ) ::= ( \mu\alpha.c_\phi \tau</td>
</tr>
<tr>
<td>NEF</td>
<td>( c_\Phi ) ::= ( \langle \mu_\Phi</td>
</tr>
<tr>
<td>( p_\Phi.q_\Phi )</td>
<td>( a</td>
</tr>
<tr>
<td></td>
<td>(</td>
</tr>
<tr>
<td>( e_\Phi )</td>
<td>( \star</td>
</tr>
</tbody>
</table>

Figure 8.1: The language of dLPA\(^\omega\)

- operators \( \text{ind}_{ax}[p_0 | p_S] \) and \( \text{cofix}_{bx}[p] \), as in dPA\(^\omega\), for inductive and coinductive reasoning;
- delimited continuations through proofs \( \mu\Phi.c_\Phi \) and the context \( \Phi \);  
- a distinguished context \( [] \) of type \( \bot \), which allows us to reason ex-falso.

As in dL_\Phi, the syntax of NEF proofs, contexts and commands is defined as a restriction of the previous syntax. Here again, they are defined (modulo \( \alpha \)-conversion) with only one distinguished context variable \( \star \) (and consequently only one binder \( \mu\star.c \)) and without stacks of the shape \( t \cdot e \) or \( q \cdot e \) (to avoid applications). The commands \( c_\Phi \) within delimited continuations are again defined as commands of the shape \( \langle \Phi|\Phi \rangle \) or formed by a NEF proof and a context of the shape \( \mu\Phi.c_\Phi \tau, \mu(a_1,c_\Phi) | a_2.c_\Phi' | \tilde{\mu}(a_1,a_2).c_\Phi | \tilde{\mu}(x,a).c_\Phi \) or \( \tilde{\mu}(x,a).c_\Phi \).

We adopt a call-by-value evaluation strategy except for fixpoint operators\(^4\), which are evaluated in a lazy way. To this purpose, we use stores in the spirit of the \( \lambda_{[f_\mu\tau\star]} \)-calculus, which are thus defined as lists of bindings of the shape \( [\alpha := p] \) where \( p \) is a value or a (co-)fixpoint, and of bindings of the shape \( [\alpha := e] \) where \( e \) is any context. We assume that each variable occurs at most once in a store \( \tau \), therefore we reason up to \( \alpha \)-reduction and we assume the capability of generating fresh names. Apart from evaluation contexts of the shape \( \mu\alpha.c \) and co-variables \( \alpha \), all the contexts are forcing contexts since they eagerly require a value to be reduced. The resulting language is given in Figure 8.1

\(^4\)To highlight the duality between inductive and coinductive fixpoints, we evaluate both in a lazy way. Even though this is not indispensable for inductive fixpoints, we find this approach more natural in that we can treat both in a similar way in the small-step reduction system and thus through the CPS translation or the realizability interpretation.
### Basic rules

\[
\langle \lambda x. p[V_i \cdot e] \rangle \tau \rightarrow \langle p[V_i/x] \parallel e \rangle \tau
\]
\[
(q \in \text{NEF}) \quad \langle \lambda a.p[q \cdot e] \rangle \tau \rightarrow \langle \mu \hat{\mu}.(\langle \parallel a.\langle p[\parallel \hat{\mu}] \rangle \parallel e \rangle) \parallel e \rangle \tau
\]
\[
(q \notin \text{NEF}) \quad \langle \lambda a.p[q \cdot e] \rangle \tau \rightarrow \langle q[a].\langle p[\parallel e] \rangle \parallel e \rangle \tau
\]
\[
(e \neq e_\emptyset) \quad \langle \mu a.c[e] \rangle \tau \rightarrow c[e][a := e]
\]
\[
(V \parallel \hat{\mu}a.cr') \tau \rightarrow c[r[a := V] \tau']
\]

### Elimination rules

\[
\langle \mu \hat{\mu} \cdot c[e] \rangle \tau \rightarrow \langle \mu \hat{\mu} \cdot c[e] \rangle \tau'
\]
\[
\langle \mu a.c[e_\emptyset] \rangle \tau \rightarrow c[e_\emptyset/a] \tau
\]
\[
\langle \mu \hat{\mu}.(p[\parallel \hat{\mu}] \parallel e) \rangle \tau \rightarrow \langle p[\parallel e] \rangle \tau
\]

### Delimited continuations

(if \(c\tau \rightarrow c\tau')

\[
\langle i_t(V) \parallel \hat{\mu}(a_1.c_1 | a_2.c_2) \rangle \tau \rightarrow c_i[r[a_i := V]]
\]
\[
\langle \langle V_1, V_2 \rangle \parallel \hat{\mu}(a_1,a_2) \rangle \tau \rightarrow c[r[a_1 := V_1, a_2 := V_2]]
\]
\[
\langle \langle V, V \rangle \parallel \hat{\mu}(x,a) \rangle \tau \rightarrow c[t/x][r[a := V]]
\]
\[
\langle \text{refl} \parallel \hat{\mu}.c \rangle \tau \rightarrow c\tau
\]

### Call-by-value

(a fresh)

\[
\langle i_t(p) \parallel e \rangle \tau \rightarrow \langle p[\parallel \hat{\mu}.a.(i_t(a) \parallel e)] \parallel e \rangle \tau
\]

(a fresh)

\[
\langle \langle p_1.p_2 \rangle \parallel e \rangle \tau \rightarrow \langle p_1[\parallel \hat{\mu}a_1.(p_2[\parallel a_2].\langle (a_1,a_2) \parallel e \rangle)] \parallel e \rangle \tau
\]

(a fresh)

\[
\langle \langle V_t, p \parallel e \rangle \tau \rightarrow \langle p[\parallel \hat{\mu}.a.(V_t,a) \parallel e \rangle \parallel e \rangle \tau
\]

### Laziness

(a fresh)

\[
\langle \text{cofix}_{bx}^V[p] \parallel e \rangle \tau \rightarrow \langle a[e] \parallel a := \text{cofix}_{bx}^V[p] \rangle \tau
\]

(a fresh)

\[
\langle \text{ind}_{bx}^V[p_0 | p_3] \parallel e \parallel e \rangle \tau \rightarrow \langle a[e] \parallel a := \text{ind}_{bx}^V[p_0 | p_3] \rangle \tau
\]

### Lookup

\[
\langle V[a] \parallel e \parallel e \rangle \tau' \rightarrow \langle V[e] \parallel a := e \parallel e \rangle \tau'
\]
\[
\langle a[f] \parallel e \parallel a := V \parallel e \parallel e \rangle \tau' \rightarrow \langle V[e] \parallel a := V \parallel e \parallel e \rangle \tau'
\]

(b' fresh)

\[
\langle a[f] \parallel e \parallel a := \text{cofix}_{bx}^V[p] \parallel e \parallel e \rangle \tau' \rightarrow \langle p[V_i/x][b'/b] \parallel b \parallel a.(a[f]) \parallel e \parallel e \parallel e \rangle \tau' \rightarrow \langle y.\text{cofix}_{bx}^y[p] \parallel e \parallel e \rangle \tau
\]
\[
\langle a[f] \parallel e \parallel a := \text{ind}_{bx}^V[p_0 | p_3] \parallel e \parallel e \rangle \tau' \rightarrow \langle p_0[\parallel \hat{\mu}.a.(a[f]) \parallel e \parallel e \parallel e \rangle \tau
\]

(b' fresh)

\[
\langle a[f] \parallel e \parallel a := \text{ind}_{bx}^V[p_0 | p_3] \parallel e \parallel e \rangle \tau' \rightarrow \langle p_3[t/x][b'/b] \parallel b \parallel a.(a[f]) \parallel e \parallel e \parallel e \rangle \tau' \rightarrow \langle y.\text{ind}_{bx}^y[p_0 | p_3] \parallel e \parallel e \rangle \tau
\]

### Terms

(if \(t \rightarrow_\beta t')

\[
T[t] \tau \rightarrow T[t'] \tau
\]
\[
(\forall a.(p[a]) \tau \rightarrow \langle (t,p') \parallel a \parallel \tau
\]
\[
T \parallel \text{wit} \parallel p \tau \rightarrow_\beta T[t]
\]
\[
(\lambda x.t)V_t \rightarrow_\beta t[V_t/x]
\]
\[
\text{rec}_{xy}^0[t_0 | t_s] \rightarrow_\beta t_0
\]
\[
\text{rec}_{xy}^{S(a)}[t_0 | t_s] \rightarrow_\beta t_s[u/x][\text{rec}_{xy}^{S(a)}[t_0 | t_s]/y]
\]

where:

\[
C_t[ , ] := \langle [ , ] \parallel e \rangle \parallel \langle \text{ind}_{ax}^V[p_0 | p_3] \parallel e \rangle \parallel \langle \text{cofix}_{bx}^V[p] \parallel e \rangle \parallel \langle \lambda x.p[ , ] \parallel e \rangle
\]
\[
T[ , ] := C_t[ , ] \parallel T[[ , u] | T[\text{rec}_{xy}^{S(a)}[t_0 | t_s]]
\]

Figure 8.2: Reduction rules of dLPA
8.1. dLPA\textsuperscript{co}: A SEQUENT CALCULUS WITH DEPENDENT TYPES FOR CLASSICAL ARITHMETIC

8.1.2 Reduction rules

Concerning the reduction system of dLPA\textsuperscript{co}, which is given in Figure 8.2, there is not much to say. The basic rules are those of the call-by-value $\lambda\mu\nu$-calculus and of dL\textsubscript{\textsc{e}}. The rules for delimited continuations are exactly the same as in dL\textsubscript{\textsc{e}}, except that we have to prevent $\hat{e}$ from being caught and stored by a proof $\mu\alpha.c$. We thus distinguish two rules for commands of the shape $\langle\mu\alpha.c|e\rangle$, depending on whether $e$ is of the shape $e_{\text{\textsc{e}}}$ or not. In the former case, we perform the substitution $[e_{\text{\textsc{e}}}/\alpha]$, which is linear since $\mu\alpha.c$ is necessarily nef. We should also mention in passing that we abuse the syntax in every other rules, since $e$ should actually refer to $e$ or $e_{\text{\textsc{e}}}$ (or the reduction of delimited continuations would be stuck). Elimination rules correspond to commands where the proof is a constructor (say of pairs) applied to values, and where the context is the matching destructor. Call-by-value rules correspond to (co-)fixpoints are reduced on an external device.

8.1.3 Typing rules

The language of types and formulas is the same as for dPA\textsuperscript{co}. As explained, terms are simply typed, with the set of natural numbers as the sole ground type. The formulas are inductively built on atomic equalities of terms, by means of conjunctions, disjunctions, first-order quantifications, dependent products and co-inductive formulas. As in dL\textsubscript{\textsc{e}}, the dependent product $\Pi a:A.B$ corresponds to the usual implication if $a$ does not occur in the conclusion $B$. Formulas and types are formally defined by:

\[
\begin{align*}
\text{Types} & :& T, U & := & N \mid T \rightarrow U \\
\text{Formulas} & :& A, B & := & T \mid \perp \mid t = u \mid A \land B \mid A \lor B \mid \forall x.T.A \mid \exists x.T.A \mid \Pi a : A.B \mid v.f_x.A.
\end{align*}
\]

Formulas are considered up to equational theory on terms, as often in Martin-Löf’s intensional type theory. We denote by $A \equiv B$ the reflexive-transitive-symmetric closure of the relation $\Rightarrow$ induced by the reduction of terms and nef proofs as follows:

\[
\begin{align*}
A[t] & \Rightarrow A[t'] & \text{whenever } t \rightarrow_\beta t' \\
A[p] & \Rightarrow A[q] & \text{whenever } \forall \alpha (\langle p|\alpha \rangle \rightarrow \langle q|\alpha \rangle)
\end{align*}
\]

in addition to the reduction rules for equality and for coinductive formulas:

\[
\begin{align*}
0 = S(t) & \Rightarrow \perp \\
S(t) = 0 & \Rightarrow \perp \\
S(t) = S(u) & \Rightarrow t = u \\
v.f_x.A & \Rightarrow A[t/x][v.f_x.A/f(y) = 0]
\end{align*}
\]

We work with one-sided sequents\footnote{This is essentially an aesthetic choice, which we hope to ease the readability of sequents. On top of that, it avoids us to deal with unified contexts $\Gamma \cup \Delta$ (see Section 4.2.3.2) as we would have done with two-sided sequents.} where typing contexts are defined by:

\[
\Gamma, \Gamma' ::= \epsilon \mid \Gamma, x : T \mid \Gamma, \alpha : A \mid \Gamma, \alpha : A^\perp \mid \Gamma, \hat{e} : A^\perp.
\]

using the notation $\alpha : A^\perp$ for an assumption of the refutation of $A$. This allows us to mix hypotheses over terms, proofs and contexts while keeping track of the order in which they are added (which is necessary because of the dependencies). We assume that a variable occurs at most once in a typing context.
We define nine syntactic kinds of typing judgments:

- six in regular mode, that we write $\Gamma \vdash^\sigma J$:
  1. $\Gamma \vdash^\sigma t : T$ for typing terms,
  2. $\Gamma \vdash^\sigma p : A$ for typing proofs,
  3. $\Gamma \vdash^\sigma e : A^\sigma$ for typing contexts,
  4. $\Gamma \vdash^\sigma e$ for typing commands,
  5. $\Gamma \vdash^\sigma c \sigma$ for typing closures,
  6. $\Gamma \vdash^\sigma \tau : (\Gamma'; \sigma')$ for typing stores;
- three more for the dependent mode, that we write $\Gamma \vdash_d^\sigma J; \sigma$:
  7. $\Gamma \vdash_d^\sigma e : A^\sigma; \sigma$ for typing contexts,
  8. $\Gamma \vdash_d^\sigma c; \sigma$ for typing commands,
  9. $\Gamma \vdash_d^\sigma c r; \sigma$ for typing closures.

In each case, $\sigma$ is a list of dependencies—we explain the presence of a list of dependencies in each case thereafter—, which are still defined from the following grammar:

$$\sigma ::= \varepsilon \mid \sigma[p\mid q]$$

The substitution on formulas according to a list of dependencies $\sigma$ is defined by:

$$\varepsilon(A) \triangleq \{A\} \quad \sigma[p\mid q](A) \triangleq \begin{cases} \sigma(A[p\mid q]) & \text{if } q \in \text{ nef} \\ \sigma(A) & \text{otherwise} \end{cases}$$

Because the language of proof terms now include constructors for pairs, injections, etc, the notation $A[p\mid q]$ does not refer to usual substitutions properly speaking: $p$ can be a pattern (for instance $(a_1, a_2)$) and not only a variable.

We shall attract the reader’s attention to the fact that all typing judgments include a list of dependencies. As in the $\tilde\lambda_{[\text{tur}]}$-calculus, when a proof or a context is caught by a binder, say $V$ and $\bar{v}a$, the substitution $[V/a]$ is not performed but rather put in the store: $\tau[a := V]$. This forces us to slightly change the rules from $dL_\Phi$. Indeed, consider for instance the reduction of a dependent function $\lambda a. p$ (of type $\Pi a : A. B$) applied to a stack $V \cdot e$:

$$(\langle \lambda a. p \rangle V \cdot e) \tau \rightarrow (\mu \bar{v} a. (\langle p \rangle \bar{v} a)) e \tau \rightarrow (\mu \bar{v} a. (\langle p \rangle \bar{v} a)) e [a := V] \rightarrow (p) e [a := V]$$

which we examined in details in the previous chapter (see Section 7.1.3). In $dL_\Phi$, the reduced command was $(\langle p \rangle [V/a]) e$, which was typed with the (Cut) rule over the formula $B[V/a]$. In the present case, $p$ still contains the variable $a$, whence his type is still $B[a]$, whereas the type of $e$ is $B[V]$. We thus need to compensate the missing substitution.

We are mostly left with two choices. Either we mimic the substitution in the type system, which would amount to the following typing rule:

$$\frac{\Gamma, \Gamma' \vdash \tau(c) \quad \Gamma \vdash \tau : \Gamma'}{\Gamma \vdash c \tau} \quad \text{where:} \quad \begin{align*} \tau[a := p_N](c) & \triangleq \tau(c[p_N/a]) & (p \in \text{ nef}) \\ \tau[a := e](c) & \triangleq \tau(c) & (p \notin \text{ nef}) \end{align*}$$

Or we type stores in the spirit of the $\tilde\lambda_{[\text{tur}]}$-calculus, and we carry along the derivations all the bindings susceptible to be used in types, which constitutes again a list of dependencies.

The former solution has the advantage of solving the problem before typing the command, but it has the flaw of performing computations which would not occur in the reduction system. For instance, the substitution $\tau(c)$ could duplicate co-fixpoints (and their typing derivations), which would never happen in the calculus. That is the reason why we privilege the other solution, which is closer to the calculus in our opinion. Yet, it has the inconvenient that if forces us to carry a dependencies list even in regular mode. Since this list is fixed (it does not evolve in the derivation except when stores occur), we differentiate the denotation of regular typing judgments, written $\Gamma \vdash^\sigma J$, from the one judgments in dependent mode, which we write $\Gamma \vdash_d^\sigma J; \sigma$ to highlight that $\sigma$ grows along derivations. The type system we obtain is given in Figure 8.3.
8.1. dLPA\textsuperscript{\omega}: A SEQUENT CALCULUS WITH DEPENDENT TYPES FOR CLASSICAL ARITHMETIC

Regular types

\[
\begin{align*}
\Gamma \vdash \sigma \tau : (\Gamma'; \sigma') & \quad \Gamma, \Gamma' \vdash \sigma \tau \alpha : A \quad (\tau_\varphi) \\
\Gamma \vdash \sigma \tau [a := p] : (\Gamma', a : A; \sigma'[a[p]]) & \quad \Gamma \vdash \sigma \tau [\alpha := e] : (\Gamma', \alpha : A^\mu; \sigma') \\
\Gamma \vdash \sigma \rho : A & \quad \Gamma \vdash \sigma e : B^\mu \quad (\text{CUT}) \\
\sigma (A) = \sigma (B) & \\
\Gamma \vdash \sigma (p[e]) & \\
(a : A) \in \Gamma & \quad (\alpha : A^\mu) \in \Gamma \\
\Gamma \vdash \sigma a : A & \quad \Gamma \vdash \sigma \alpha : A^\mu \\
\Gamma, \sigma \vdash A \quad \Gamma \vdash \sigma c & \\
\Gamma, \sigma \vdash A \text{ c} & \\
\Gamma \vdash \sigma \rho p : A & \quad \Gamma \vdash \sigma p_1 : A & \quad \Gamma \vdash \sigma p_2 : B \\
\Gamma \vdash \sigma (p_1, p_2) : A \land B \\
\Gamma \vdash \sigma t : T & \quad \Gamma \vdash \sigma p : A & \quad \Gamma \vdash \sigma e : A[t/x] \quad (\sigma_\varphi) \\
\Gamma \vdash \sigma t : \Gamma & \quad \Gamma \vdash \sigma e : (\forall x. T).A \quad (\sigma_\varphi) \\
\Gamma \vdash \sigma \lambda x p : \forall x. T. A & \quad \Gamma \vdash \sigma q : A & \quad \Gamma \vdash \sigma e : B[q/a] \quad \text{if } q \not\in \text{ nef } \text{ then } a \not\in A \\
\Gamma \vdash \sigma \lambda a p : \Pi a : A B & \quad \Gamma \vdash \sigma q : A & \quad \Gamma \vdash \sigma e : (\Pi a : A B) \quad (\sigma_\varphi) \\
\Gamma \vdash \sigma [] : A^\mu & \\
\Gamma \vdash \sigma t : T & \quad \Gamma \vdash \sigma p_0 : A[0/x] & \quad \Gamma, x : T, a : A \vdash \sigma p : A & \quad f \text{ positive in } A \\
\Gamma \vdash \sigma \text{ cofix} p_\lambda [p] : \forall x. T A & \\
\end{align*}
\]

Dependent mode

\[
\begin{align*}
\Gamma, \Phi : A^\mu & \vdash \delta_{A^\mu} c_{\delta A} : \tau \quad (\mu_\Phi) \\
\sigma (A) = \sigma (B) & \\
\Gamma, \phi : A^\mu, \varphi \vdash \delta_{B^\mu} c_{\delta B} : \sigma \{p\} \\
\Phi, \Phi' \vdash \tau : (\Gamma', \sigma') & \quad \Gamma' \vdash \tau \alpha : A \quad (\text{CUT}_\varphi) \\
\Gamma, c_{\delta A} \vdash \sigma \quad (\rho_\delta) \\
\Gamma, a : A \vdash \delta_{A^\mu} c_{\delta A} : A^\mu; \sigma \{p_{\lambda}N\} \\
\Gamma, a : A \vdash \delta_{A^\mu} c_{\delta A} : A^\mu; \sigma \{p_{\lambda}N\} & \quad \Gamma, x : T, a : A \vdash \delta_{A^\mu} c_{\delta A} : A^\mu; \sigma \{p_{\lambda}N\} \\
\forall i \in \{1, 2\} \\
\Gamma, \delta_{A^\mu} c_{\delta A} : A^\mu; \sigma \{p_{\lambda}N\} & \quad \Gamma, \delta_{A^\mu} c_{\delta A} : A^\mu; \sigma \{p_{\lambda}N\} \\
\end{align*}
\]

Terms

\[
\begin{align*}
\Gamma \vdash \sigma 0 : N & \quad (0) \\
\Gamma \vdash \sigma \text{ t} : N & \quad (S) \\
\Gamma \vdash \sigma \text{ S}(t) : N & \quad (\text{S}) \\
\Gamma \vdash \sigma \text{ t} : \text{ U} & \quad (\text{L}) \\
\Gamma \vdash \sigma \text{ t} : \text{ S}(\text{ t}) & \quad (\text{L}) \\
\Gamma \vdash \sigma \text{ t} : \text{ U} & \quad (\text{L}) \\
\Gamma \vdash \sigma \text{ t} : \text{ U} & \quad (\text{L}) \\
\Gamma \vdash \sigma \text{ t} : \text{ U} & \quad (\text{L}) \\
\Gamma \vdash \sigma \text{ t} : \text{ U} & \quad (\text{L}) \\
\Gamma \vdash \sigma \text{ t} : \text{ U} & \quad (\text{L}) \\
\Gamma \vdash \sigma \text{ t} : \text{ U} & \quad (\text{L}) \\
\Gamma \vdash \sigma \text{ t} : \text{ U} & \quad (\text{L}) \\
\Gamma \vdash \sigma \text{ t} : \text{ U} & \quad (\text{L}) \\
\Gamma \vdash \sigma \text{ t} : \text{ U} & \quad (\text{L}) \\
\Gamma \vdash \sigma \text{ t} : \text{ U} & \quad (\text{L}) \\
\end{align*}
\]

Figure 8.3: Type system for dLPA\textsuperscript{\omega}

205
8.1.4 Subject reduction

It only remains to prove that typing is preserved along reduction. As for the $\lambda_{[\text{l} \text{u} \text{r} \ast \ast]}$-calculus, the proof is simplified by the fact that substitutions are not performed (except for terms), which keeps us from proving the safety of the corresponding substitutions. Yet, we first need to prove some technical lemmas about dependencies. As in the previous chapter, we define a relation $\sigma \Rightarrow \sigma'$ between lists of dependencies, which expresses the fact that any typing derivation obtained with $\sigma$ could be obtained as well as with $\sigma'$:

$$\sigma \Rightarrow \sigma' \triangleq \sigma(A) = \sigma(B) \Rightarrow \sigma'(A) = \sigma'(B)$$

(for any $A, B$)

We first show that the cases which we encounter in the proof of subject reduction satisfy this relation:

**Lemma 8.1** (Dependencies implication). The following holds for any $\sigma, \sigma', \sigma''$:

1. $\sigma \sigma'' \Rightarrow \sigma \sigma' \sigma''$
2. $\sigma\{a_1,a_2\}\{V_1,V_2\} \Rightarrow \sigma\{a_1|V_1|a_2|V_2\}$
3. $\sigma|\{i\}(V) \Rightarrow \sigma|\{i\}(V)$
4. $\sigma\{a(x)|t(V)\} \Rightarrow \sigma\{a(V)|\{x|t\}\}$
5. $\sigma|\{i\}(p_1,p_2) \Rightarrow \sigma|\{i\}(p_1,p_2)$
6. $\sigma|\{-\}(p) \Rightarrow \sigma|\{-\}(p)$
7. $\sigma|\{-\}(t,p) \Rightarrow \sigma|\{-\}(t,p)$

where the fourth item abuse the definition of list of dependencies to include a substitution of terms.

*Proof.* All the properties are trivial from the definition of the substitution $\sigma(A)$. □

**Proposition 8.2** (Dependencies weakening). If $\sigma, \sigma'$ are two dependencies list such that $\sigma \Rightarrow \sigma'$, then any derivation using $\sigma$ can be one using $\sigma'$ instead. In other words, the following rules are admissible:

$$\Gamma \vdash^\sigma J \quad (w)$$

$$\Gamma \vdash^\sigma J \quad (\sigma' d)$$

*Proof.* Simple induction on the typing derivations. The rules $(\emptyset)$ and $(\text{CurT})$ where the list of dependencies is used exactly match the definition of $\Rightarrow$. Every other case is direct using the first item of Lemma 8.1. □

We also need a simple lemma about stores to simplify the proof of subject reduction:

**Lemma 8.3.** The following rule is admissible:

$$\frac{\Gamma \vdash^\sigma \tau_0 : (\Gamma_0;\sigma_0) \quad \Gamma_0 \vdash^\sigma_0 \tau_1 : (\Gamma_1;\sigma_1)}{\Gamma \vdash^\sigma \tau_0 \tau_1 : (\Gamma_0,\Gamma_1;\sigma_0,\sigma_1)} \quad (\tau \tau')$$

*Proof.* By induction on the structure of $\tau_1$. □

**Lemma 8.4** (Safe term substitution). If $\Gamma \vdash^\sigma t : T$ then for any conclusion $J$ for typing proofs, contexts, terms, etc; the following holds:

1. If $\Gamma, x : T, \Gamma' \vdash^\sigma J$ then $\Gamma, \Gamma'[t/x] \vdash^\sigma J[t/x]$.
2. If $\Gamma, x : T, \Gamma' \vdash J; \sigma$ then $\Gamma, \Gamma'[t/x] \vdash J[t/x]; \sigma[t/x]$.

*Proof.* By induction on typing rules. □

**Theorem 8.5** (Subject reduction). For any context $\Gamma$ and any closures $c\tau$ and $c'\tau'$ such that $c\tau \rightarrow c'\tau'$, we have:
8.1. dLPA\textsuperscript{\textomega}: A SEQUENT CALCULUS WITH DEPENDENT TYPES FOR CLASSICAL ARITHMETIC

1. If $\Gamma \vdash c t$ then $\Gamma \vdash c^t \tau'$.
2. If $\Gamma \vdash d t \epsilon$ then $\Gamma \vdash d^t \epsilon \tau'; \epsilon$.

Proof. The proof follows the usual proof of subject reduction, by induction on the typing derivation and the reduction $c t \rightarrow c^t \tau'$. Since there is no substitution but for terms (proof terms and contexts being stored), there is no need for auxiliary lemmas about the safety of substitution. We sketch it by examining all the rules from Figure 8.3 from top to bottom.

- The cases for reductions of $\lambda$ are identical to the cases proven in the previous chapter for $dL_{\text{fp}}$.

- The rules for reducing $\mu$ and $\bar{\mu}$ are almost the same except that elements are stored, which makes it even easier. For instance in the case of $\bar{\mu}$, the reduction rule is:

$$\langle \nu a. c t \rangle_{\tau_0} \rightarrow c t_{\tau_0}[a := V]_{\tau_1}$$

A typing derivation in regular mode for the command on the left-hand side is of the shape:

$$\begin{array}{c}
\Pi_c \\
\Pi_{\tau_1}
\end{array}$$

Thus we can type the command on the right-hand side:

$$\begin{array}{c}
\Pi_c \\
\Pi_{\tau_0} \\
\Pi_{\tau_1}
\end{array}$$

As for the dependent mode, the binding $\{a|p\}$ within the list of dependencies is compensated when typing the store as shown in the last derivation.

- Similarly, elimination rules for contexts $\bar{\mu}[a_1,c_1|a_2,c_2], \bar{\mu}(a_1,a_2).c, \bar{\mu}(x).a$ or $\bar{\nu}.c$ are easy to check, using Lemma 8.1 and the rule $(tp)$ in dependent mode to prove the safety with respect to dependencies.

- The cases for delimited continuations are identical to the corresponding cases for $dL_{\text{fp}}$.

- The cases for the so-called “call-by-value” rules opening constructors are straightforward, using again Lemma 8.1 in dependent mode to prove the consistency with respect to the list of dependencies.

- The cases for the lazy rules are trivial.

- The first case in the “lookup” section is trivial. The three lefths correspond to the usual unfolding of inductive and co-inductive fixpoints. We only sketch the latter in regular mode. The reduction rule is:

$$\langle a|f\rangle_{\tau_0}[a := \text{cofix } b_{\text{bx}}[p]]_{\tau_1} \rightarrow \langle p|t/x|b'|b\rangle[\mu a.(a|f)\rangle_{\tau_1}]_{\tau_0}[b' := \lambda y.\text{cofix } b_{\text{bx}}[p]]$$

The crucial part of the derivation for the left-hand side command is the derivation for the cofix in the store:

$$\begin{array}{c}
\Pi_{\tau_0} \\
\Pi_f \\
\Pi_p
\end{array}$$
Then, using this derivation, we can type the store of the right-hand side command:

\[
\begin{array}{c}
\Pi_p \\
\Gamma, y : T \vdash \sigma \quad y : T
\end{array}
\]

It only remains to type (we avoid the rest of the derivation, which is less interesting) the proof \(p[t/x]\) with this new store to ensure us that the reduction is safe (since the variable \(a\) will still be of type \(v^f_x A\) when typing the rest of the command):

\[
\begin{array}{c}
\Pi_p \\
\Gamma, b : \forall y. v^f_x A \vdash \sigma \quad p[t/x] : A[t/x][v^f_x A/f(y) = 0]
\end{array}
\]

\[\equiv A[t/x][v^f_x A/f(y) = 0] \]

• The cases for reductions of terms are easy. Since terms are reduced in place within proofs, the only things to check is that the reduction of with preserves types (which is trivial) and that the \(\beta\)-reduction verifies the subject reduction (which is a well-known fact).

\[\square\]

### 8.1.5 Natural deduction as macros

We can recover the usual proof terms for elimination rules in natural deduction systems, and in particular the ones from \(dPA^\omega\), by defining them as macros in our language. The definitions are straightforward, using delimited continuations for \(let \ldots in\) and the constructors over \(\text{Nef}\) proofs which might be dependently typed:

\[
\begin{align*}
let a = p in q & \triangleq \mu a. \langle p \mid \mu a. \langle q \mid a_p \rangle \rangle \\
split p as (a_1, a_2) in q & \triangleq \mu a. \langle p \mid \mu \langle a_1, a_2 \rangle. \langle q \mid a_2 \rangle \rangle \\
case p of [a_1 \mid p_1 \mid a_2 \mid p_2] & \triangleq \mu a. \langle p \mid \mu \langle a_1 \mid p_1 \rangle. \langle a_2 \mid p_2 \rangle \rangle \rangle \\
dest p as (a, x) in q & \triangleq \mu a. \langle p \mid \mu \langle x, a \rangle. \langle q \mid a_p \rangle \rangle \\
prf p & \triangleq \mu \Phi. \langle p \mid \mu \Phi. \langle x, a \rangle. \langle \Phi \mid a \rangle \rangle \\
subst p q & \triangleq \mu a. \langle p \mid \mu q. \langle q \mid a \rangle \rangle \\
\text{exfalso } p & \triangleq \mu a. \langle p \mid \mu q. \langle q \mid a \rangle \rangle \\
catch_a p & \triangleq \mu a. \langle p \mid a \rangle \\
\text{throw ap} & \triangleq \mu a. \langle p \mid a \rangle
\end{align*}
\]

where \(a_p = \Phi\) if \(p\) is \(\text{Nef}\) and \(a_p = a\) otherwise.

**Proposition 8.6** (Natural deduction). The typing rules from \(dPA^\omega\), given in Section 8.1.5, are admissible

**Proof.** Straightforward derivations, the cases for \(prf\ p q\) and \(subst\ p q\) are given in Section 7.5.4 \(\square\)

One can even check that the reduction rules in \(dLPA^\omega\) for these proofs almost mimic the ones of \(dPA^\omega\). To be more precise, the rules of \(dLPA^\omega\) do not allow to simulate each rule of \(dPA^\omega\), due to the head-reduction strategy, amongst other things. Nonetheless, up to a few details the reduction of a command in \(dLPA^\omega\) follows one particular reduction path of the corresponding proof in \(dPA^\omega\), or in other word, one reduction strategy.

The main result is that using the macros, the same proof terms are suitable for countable and dependent choice [70]. We do not state it here, but following the approach of [70], we could also extend \(dLPA^\omega\) to obtain a proof for the axiom of bar induction.
8.2. SMALL-STEP CALCULUS

\[
\begin{array}{c}
\Gamma \vdash p : \exists x^T.A & \quad \Gamma, x : T, a : A \vdash q : B[(x,a)/\bullet] \quad p \not\in \mathrm{NEF} \Rightarrow \bullet \not\in B \\
\frac{}{\Gamma \vdash \text{dest } p \text{ as } (x,a) \text{ in } q : B[p/\bullet]} & \text{(dest)} \\
\Gamma \vdash p : A_1 \wedge A_2 & \quad \Gamma, a_1 : A_1, a_2 : A_2 \vdash q : B[(a_1,a_2)/\bullet] \quad p \not\in \mathrm{NEF} \Rightarrow \bullet \not\in B \\
\frac{}{\Gamma \vdash \text{split } p \text{ as } (a_1,a_2) \text{ in } q : B[p/\bullet]} & \text{(split)} \\
\Gamma \vdash p : A_1 \vee A_2 & \quad \Gamma, a_i : A_i \vdash q : B[i(a_i)/\bullet] \quad \text{for } i = 1, 2 \quad p \not\in \mathrm{NEF} \Rightarrow \bullet \not\in B \\
\frac{}{\Gamma \vdash \text{case } p \text{ of } [a_1,p_1] \mid a_2,p_2 : B[p/\bullet]} & \text{(case)} \\
\Gamma, a : A \vdash q : B[a/\bullet] & \quad p \not\in \mathrm{NEF} \Rightarrow \bullet \not\in B \\
\frac{}{\Gamma \vdash \text{let } a = p \text{ in } q : B[p/\bullet]} & \text{(let)} \\
\Gamma, \alpha : \mathbb{A}^\mathbb{U} + p : A & \quad \Gamma \vdash \text{catch}_\alpha p : A \\
\Gamma, \alpha : \mathbb{A}^\mathbb{U} + p : A & \quad \Gamma \vdash \text{throw } \alpha \ p : B \\
\end{array}
\]

Figure 8.4: Typing rules of dPA\text{\textcircled{O}}

\[\text{Theorem 8.7 (Countable choice [70])}. \text{ We have:}\]
\[
AC_N := \lambda H. \lambda x_0. \lambda a = \text{cofix}^0_{bn} [\text{dest } Hn \text{ as } (y,c) \text{ in } (\lambda n \text{. wit } (\text{nth}_n a), \lambda n \text{. prf } (\text{nth}_n a))] \\
\vdash \forall x^N. \exists y^T. P(x,y) \Rightarrow \exists f^N. \forall x^T. (f(0) = x_0 \wedge \forall n^N. P(f(n), f(s(n)))
\]

where \text{nth}_n a := \pi_1(\text{ind}^n_{x,a}[a | \pi_2(c)]).

\textit{Proof.} See Figure 8.5 \hfill \square

\[\text{Theorem 8.8 (Dependent choice [70])}. \text{ We have:}\]
\[
DC := \lambda H. \lambda x_0. \lambda a = (x_0, \text{cofix}^0_{bn} [\text{dest } Hn \text{ as } (y,c) \text{ in } (y,(c,b y))]) \\
\vdash \forall x^T. \exists y^T. P(x,y) \Rightarrow \forall x^T_0. \exists f \in T^N. (f(0) = x_0 \wedge \forall n^N. P(f(n), f(s(n)))
\]

where \text{nth}_n a := \text{ind}^n_{x,a}[a | (\text{wit } (\text{prf } d), \pi_2(\text{prf } (\text{prf } (d))))].

\textit{Proof.} Left to the reader. \hfill \square

8.2 Small-step calculus

Once more, we follow Danvy’s methodology of semantic artifacts to obtain a continuation-passing style translation and a realizability interpretation. We first decompose the reduction system of dLP\text{\textcircled{O}} into small-step reduction rules, that we denote by $\sim_s$. This requires a refinement and an extension of the syntax, that we shall now present. To keep us from boring the reader stiff with new (huge) tables for the syntax, typing rules and so forth, we will introduce them step by step. We hope it will help the reader to convince herself of the necessity and of the somewhat naturality of these extensions.

First of all, we need to refine the syntax to distinguish between strong and weak values in the syntax of proof terms. As in the $\lambda I_{\text{let}, \text{pr}, \text{\bullet}}$-calculus, this refinement is induced by the computational behavior of the calculus: weak values are the ones which are stored by $\bar{\mu}$ binders, but which are not values enough to be eliminated in front of a forcing context, that is to say variables. Indeed, if we observe the reduction system, we see that in front of a forcing context $f$, a variable leads a search through the store for a “stronger” value, which could incidentally provoke the evaluation of some fixpoints. On the other
CHAPTER 8. A SEQUENT CALCULUS WITH DEPENDENT TYPES FOR CLASSICAL ARITHMETIC

Notations:

- \( \text{nath}, p \triangleq \pi_1(\text{ind}'_{xx}[p \mid \pi_2(s)]) \)
- \( A^n \triangleq \nu_f^0[A(x) \land f(S(x)) = 0] \)
- \( \text{str}^t_{\infty} H \triangleq \text{cofix}_{bt}[(Hn, b(S(n)))] \)
- \( A(x) \triangleq \exists y^n.T.P(x, y) \)

Typing derivation for \( \text{nath} \) (\( \Pi_{\text{nath}} \)):

\[
\begin{align*}
\vdash & n : N + n : N \quad \text{(Axn)} \\
\vdash & a : A^n_{\infty}, n : N \quad \text{(Axr)} \\
\vdash & \text{ind}^t_{xx} [a \mid \pi_2(s)] : A^n_{\infty} \quad \text{(ind)} \\
\vdash & a : A^n_{\infty}, n : N \quad \text{(def)}
\end{align*}
\]

Typing derivation for \( \text{str}^0_{\infty} \) (\( \Pi_{\text{str}^0_{\infty}} \)):

\[
\begin{align*}
\vdash & 0 : N \quad \text{(Axr)} \\
\vdash & H : \forall x^N.\exists z^T.P(x, y) \quad \text{Ax}
\end{align*}
\]

Typing derivation for \( AC_N \):

\[
\begin{align*}
\vdash & \text{nath}_n a : A(n) \quad \text{(def)} \\
\vdash & a : A^n_{\infty}, n : N \quad \text{(def)} \\
\vdash & \text{wit}(\text{nath}_n a) : T \\
\vdash & a : A^n_{\infty} \quad \text{(wit)} \\
\vdash & a : A^n_{\infty}, x : N \quad \text{prf}(\text{nath}_n a) : P(x, \text{wit}(\text{nath}_n a)) \\
\vdash & a : A^n_{\infty}, x : N \quad \text{prf}(\text{nath}_n a) : P(x, \lambda n. \text{wit}(\text{nath}_n a)x) \\
\vdash & a : A^n_{\infty} \quad \text{(pr)} \\
\vdash & H : \forall x^N.\exists z^T.P(x, y) \quad \text{let} \\
\vdash & \lambda a \text{str}^0_{\infty} H \quad \text{in} \quad \text{l.et}(\text{nath}_n a, \lambda n. \text{prf}(\text{nath}_n a) : \exists y^{N\to T}.\forall x^N.P(x, f(x))) \\
\vdash & \lambda n. \text{let} a = \text{str}^0_{\infty} H \quad \text{let} \quad \text{let} \quad \text{let}
\end{align*}
\]

where we omit the conversion \( P(x, (\lambda n. \text{wit}(\text{nath}_n a))x) \equiv P(x, \text{wit}(\text{nath}_n a)) \) on the right-hand side derivation.

Figure 8.5: Proof of the axiom of countable choice in \( d\text{LPA}^\omega \)

210
hand, strong values are the ones which can be reduced in front of the matching forcing context, that is
to say functions, \( \text{ref} \ lệnh \), pairs of (weak) values, injections or dependent pairs:

| Weak values | \( V ::= a | v \) |
|-------------|------------------|
| Strong values | \( v ::= I(V) | (V,V) | (V,\lambda x.p) | \lambda a.p | \text{ref } \leqnl \) |

This allows to distinguish commands of the shape \( \langle v \| f \rangle \tau \), where the forcing context (and next the
strong value) are examined to determine whether the command reduces or not; from commands of the
shape \( \langle a \| f \rangle \tau \) where the focus is put on the variable \( a \), which leads to a lookup for the associated proof
in the store.

Next, we need to explicit the reduction of terms. To this purpose, we include a machinery to evaluate
terms in a way which resemble the evaluation of proofs. In particular, we define new commands which
we write \( \hat{c} x.c \) or stacks of the shape \( u \pi \). These constructions are the usual ones of the \( \lambda \mu \pi \)-calculus (which
are also the ones for proofs). We also extend the definitions of commands with delimited continuations
to include the corresponding commands for terms:

| Commands | \( c ::= \langle p|e \rangle | \langle t|\pi \rangle \) |
|-----------|----------------------------------|
| Co-terms | \( \pi ::= t \cdot \pi | \hat{\mu} x.c \) |
| Delimited continuations | \( c_{\pi}^{T} ::= \cdots | \langle t|\pi_{\Phi} \rangle \) |
| continuations | \( \pi_{\Phi} ::= t \cdot \pi_{\Phi} | \hat{\mu} x.c_{\Phi} \) |

We give typing rules for these new constructions, which are the usual rules for typing contexts in the
\( \lambda \mu \pi \)-calculus:

\[
\begin{align*}
\Gamma \vdash t : T & \quad \Gamma \vdash \pi : U^{\perp} \\
\Gamma \vdash t \cdot \pi : (T \to U)^{\perp} & \quad (\to_t) \\
\Gamma \vdash c : (\Gamma, x : T) & \quad (\hat{\mu}_x) \\
\Gamma \vdash \hat{\mu} x.c : T^{\perp} & \quad (\text{cut}_t)
\end{align*}
\]

It is worth noting that the syntax as well as the typing and reduction rules for terms now match exactly
the ones for proofs.\(^6\) In other words, with these definitions, we could abandon the stratified presentation
without any trouble, since reduction rules for terms will naturally collapse to the ones for proofs.

Finally, in order to maintain typability when reducing dependent pairs of the strong existential
type, we need to add what we call co-delimited continuations. We saw in the previous chapter that the
CPS translation of pairs \( (t,p) \) was not the expected one, and we mentioned the fact that it reflected
the need for a special reduction rule. Indeed, consider such a pair of type \( \exists x^T.A \), the standard way of
reducing it would be a rule like:

\[
\langle (t,p)|\langle e \rangle \rangle \tau \leadsto_s \langle t|\hat{\mu} x.(p|\hat{\mu}a.\langle \langle x,a \rangle|e \rangle)) \rangle \tau
\]

but such a rule does not satisfy subject reduction. Indeed, consider a typing derivation for the left-hand
side command, when typing the pair \( (t,p) \), \( p \) is of type \( A[t] \). On the command on the right-hand side,
the variable \( a \) will then also be of type \( A[t] \), while it should be of type \( A[x] \) for the pair \( (x,a) \) to be
typed. We thus need to compensate this mismatching of types, by reducing \( t \) within a context where \( a \)
is not linked to \( p \) but to a co-reset \( \Phi \) (dually to reset \( \Psi \)), whose type can be changed from \( A[x] \) to \( A[t] \)
thanks to a list of dependencies:

\[
\langle (t,p)|\langle e \rangle \rangle_p \tau \leadsto_s \langle p|\hat{\mu} \Phi.(t|\hat{\mu} x.\langle \Phi|\hat{\mu}a.\langle \langle x,a \rangle|e \rangle)) \rangle_p \tau
\]

We thus equip the language with new contexts \( \hat{\mu} \Phi.c_{\Phi} \), which we call co-shifts, and where \( c_{\Phi} \)
is a command whose last cut is of the shape \( \langle \Phi|e \rangle \). This corresponds formally to the following syntactic

\(^6\)Except for substitutions of terms, which we could store as well
sets, which are dual to the ones introduced for delimited continuations:

\[
\begin{align*}
\text{Contexts} & \quad e & ::= & \cdots | \mu \Phi . c_{\Phi} \\
\text{Co-delimited} & \quad c_{\Phi} & ::= & \langle p_N \parallel e_{\Phi} \rangle | \langle t \parallel \pi_{\Phi} \rangle | \langle \Phi \parallel e \rangle \\
\text{continuations} & \quad e_{\Phi} & ::= & \mu a . c_{\Phi} | \mu [a_1 . c_{\Phi} | a_2 . c_{\Phi}'] | \mu (a_1 , a_2) . c_{\Phi} | \mu (x , a) . c_{\Phi} \\
\pi_{\Phi} & ::= & t \cdot \pi_{\Phi} | \mu x . c_{\Phi} \\
\text{NEF} & \quad e_N & ::= & \cdots | \mu \Phi . c_{\Phi}
\end{align*}
\]

This might seem to be a heavy addition to the language, but we insist on the fact that these artifacts are merely the dual constructions of delimited continuations that we introduced in dL. With a very similar intuition. In particular, it might be helpful for the reader to think of the fact that we introduced delimited continuations for type safety of the evaluation of dependent products in \( \Pi a : A . B \) (which naturally extends to the case \( \forall x . T . A \)). Therefore, to maintain type safety of dependent sums in \( \exists x . T . A \), we need to introduce the dual constructions of co-delimited continuations. We also give typing rules to these constructions, which are dual to the typing rules for delimited-continuations:

\[
\begin{align*}
\Gamma, \Phi : A \vdash_d c_{\Phi}; \sigma & \quad \frac{}{\Gamma \vdash^\sigma \mu \Phi . c_{\Phi} : A^\mu} \\
\Gamma, \Gamma' \vdash^\sigma e : A^\mu \quad \sigma (A) = \sigma (B) & \quad \frac{}{\Gamma, \Phi : B , \Gamma' \vdash_d (\Phi \parallel e); \sigma}
\end{align*}
\]

Note that we also need to extend the definition of list of dependencies so as to include bindings of the shape \( \{ x | t \} \) for terms, and that we have to give the corresponding typing rules to type commands of terms in dependent mode:

\[
\begin{align*}
c : (\Gamma , x : T ; \sigma (x | t)) & \quad \frac{}{\Gamma \vdash_d \mu x . c : T^\mu ; \sigma (\cdot | t)} \\
\Gamma, \Gamma' \vdash^\sigma t : T \quad \Gamma, \Phi : B , \Gamma' \vdash_d \pi : A^\mu ; \sigma (\cdot | t) & \quad \frac{}{\Gamma, \Phi : B , \Gamma' \vdash_d (\parallel \pi); \sigma}
\end{align*}
\]

The small-step reduction system is given in Figure 8.6. The rules are written \( c , \ell_s \vdash t \cdot c' , \ell_s \) where the annotation \( \ell_s , \ell \) on commands are indices (i.e. \( c , p , e , V , f , t , \pi , V_i \)) indicating which part of the command is in control. As in the \( \tilde{\lambda} (\ell_s , \ell) \)-calculus, we observe an alternation of steps descending from \( p \) to \( f \) for proofs and from \( t \) to \( V_i \) for terms. The descent for proofs can be divided in two main phases. During the first phase, from \( p \) to \( e \) we observe the call-by-value process, which extracts values from proofs, opening recursively the constructors and computing values. In the second phase, the core computation takes place from \( V \) to \( f \), with the destruction of constructors and the application of function to their arguments. The laziness corresponds precisely to a skip of the first phase, waiting to possibly reach the second phase before actually going through the first one.

We briefly state the important properties of this system.

**Proposition 8.9 (Subject reduction).** The small-step reduction rules satisfy subject reduction.

**Proof.** The proof is again a tedious induction on the reduction \( \sim_s \). There is almost nothing new in comparison with the cases for the big-step reduction rules: the cases for reduction of terms are straightforward, as well as the administrative reductions changing the focus on a command. We only give the case for the reduction of pairs \( (t , p) \). The reduction rule is:

\[
\langle (t , p) \parallel e \rangle_p \tau \sim_s \langle p \parallel \mu \Phi . \langle t \parallel \mu x . \langle \Phi \parallel \mu a . \langle (x , a) \parallel e \rangle \rangle \rangle_p \tau
\]

Consider a typing derivation for the command on the left-hand side, which is of the shape (we omit the rule \( (l) \) and the store for conciseness):

\[
\begin{align*}
\Pi_p & \quad \Pi_t \quad \Pi_e \\
\Gamma \vdash^\sigma t : T & \quad \Gamma \vdash^\sigma p : A [ t / x ] \quad \Gamma \vdash^\sigma (t , p) ; \exists x . T . A \\
\Rightarrow \Gamma \vdash^\sigma ((t , p) \parallel e) & \quad (l) \quad (\exists) \quad (\text{Cur})
\end{align*}
\]
### 8.2. SMALL-STEP CALCULUS

<table>
<thead>
<tr>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \langle p | e \rangle c \tau \rightsquigarrow_s \langle p | e \rangle_p )</td>
</tr>
<tr>
<td>( \langle t | \pi \rangle c \tau \rightsquigarrow_s \langle t | \pi \rangle_t )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Delimited continuations</th>
</tr>
</thead>
<tbody>
<tr>
<td>(for any ( i, o ))</td>
</tr>
<tr>
<td>( \langle \mu \Phi.c \tau'' \rangle_p \tau \rightsquigarrow_s \langle \mu \Phi.c \tau'' \rangle_p \tau' )</td>
</tr>
<tr>
<td>( \langle \mu \Phi.(p</td>
</tr>
<tr>
<td>(if ( c, \tau \rightsquigarrow_s c_0 \tau ))</td>
</tr>
<tr>
<td>(for any ( i, o ))</td>
</tr>
<tr>
<td>( \langle V</td>
</tr>
<tr>
<td>( \langle V</td>
</tr>
<tr>
<td>(if ( c, \tau \rightsquigarrow_s c_0 \tau ))</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proofs</th>
</tr>
</thead>
<tbody>
<tr>
<td>( e \neq e_b )</td>
</tr>
<tr>
<td>( \langle \mu a.c \rangle_p \tau \rightsquigarrow_s c_0 \tau [\alpha \gets e] )</td>
</tr>
<tr>
<td>( \langle \mu a.c \rangle_{e_b} \tau \rightsquigarrow_s c_0 [e_{b_0} \alpha] \tau )</td>
</tr>
<tr>
<td>(a fresh)</td>
</tr>
<tr>
<td>( \langle (p_1, p_2) \rangle_e \tau \rightsquigarrow_s \langle p_1 | \mu a_1, p_2 | \mu a_2, (\langle (a_1, a_2) \rangle e) \rangle_p \tau )</td>
</tr>
<tr>
<td>(a fresh)</td>
</tr>
<tr>
<td>( \langle \iota_0(p) \rangle_p \tau \rightsquigarrow_s \langle p | \mu a | \iota_0(a) \rangle_p \tau )</td>
</tr>
<tr>
<td>(a fresh)</td>
</tr>
<tr>
<td>( \langle (t, t) \rangle_p \tau \rightsquigarrow_s \langle p | \mu \Phi.\langle t | \mu x \rangle \langle \Phi | \mu a | \langle x, a \rangle \rangle \rangle_p \tau )</td>
</tr>
<tr>
<td>(y, a fresh)</td>
</tr>
<tr>
<td>( \langle \text{ind}_{b_b}^b[p</td>
</tr>
<tr>
<td>(y, a fresh)</td>
</tr>
<tr>
<td>( \langle \text{cofix}_{b_b}^b[p] \rangle_e \tau \rightsquigarrow_s \langle \mu \Phi.(t</td>
</tr>
<tr>
<td>(\langle V | e \rangle_p \tau \rightsquigarrow_s \langle V | e \rangle_e )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contexts</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \langle V</td>
</tr>
<tr>
<td>( \langle V | \mu a.c \rangle \tau' \rightsquigarrow_s c_0 \tau \tau [a := V] \tau' )</td>
</tr>
<tr>
<td>( \langle V | e \rangle_c \tau \rightsquigarrow_s \langle V | e \rangle_e \tau )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \langle a</td>
</tr>
<tr>
<td>( \langle v</td>
</tr>
<tr>
<td>(b' fresh)</td>
</tr>
<tr>
<td>( \langle a</td>
</tr>
<tr>
<td>( \langle a</td>
</tr>
<tr>
<td>(b' fresh)</td>
</tr>
<tr>
<td>( \langle a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Forcing contexts</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \langle \lambda x.p[t \cdot e] \rangle \tau \rightsquigarrow_s \langle \mu \Phi.(t | \mu x \langle p</td>
</tr>
<tr>
<td>( \langle \lambda x.p</td>
</tr>
<tr>
<td>( \langle \lambda x.p</td>
</tr>
<tr>
<td>( \langle \lambda x.p</td>
</tr>
<tr>
<td>( \langle \lambda t</td>
</tr>
<tr>
<td>( \langle (V_1, V_2)</td>
</tr>
<tr>
<td>( \langle (V_f, V)</td>
</tr>
<tr>
<td>( \langle \text{refl} | \mu z.c \rangle \tau \rightsquigarrow_s c_0 \tau )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \langle t u</td>
</tr>
<tr>
<td>(x fresh)</td>
</tr>
<tr>
<td>( \langle S(t)</td>
</tr>
<tr>
<td>(x, a fresh)</td>
</tr>
<tr>
<td>( \langle \text{wit} \ p</td>
</tr>
<tr>
<td>(t \notin V_1)</td>
</tr>
<tr>
<td>( \langle \text{rec}_{1}^{2}</td>
</tr>
<tr>
<td>( \langle \text{rec}_{1}^{3}</td>
</tr>
<tr>
<td>( \langle \text{rec}_{1}^{3}</td>
</tr>
<tr>
<td>( \langle \lambda x. t \mu u \cdot \pi \rangle \tau \rightsquigarrow_s \langle u | \mu x. \langle t</td>
</tr>
<tr>
<td>( \langle V_f</td>
</tr>
<tr>
<td>( \langle V_f</td>
</tr>
</tbody>
</table>

Figure 8.6: Small-step reduction rules
CHAPTER 8. A SEQUENT CALCULUS WITH DEPENDENT TYPES FOR CLASSICAL ARITHMETIC

Then we can type the command on the right-hand side with the following derivation:

\[
\frac{
\Pi_{(x,a)} \quad \Pi_p \quad \Pi_x
\}
\begin{array}{c}
\Gamma, x : T, a : A[x] \vdash \sigma \langle \langle x, a \rangle \rangle e : A[x] \mu \\
\Gamma, x : T \vdash \sigma \mu a. \langle \langle x, a \rangle \rangle e : A[x] \mu \\
\Gamma, \Phi : A[t] \vdash \langle \langle \Phi \mu \beta a. \langle \langle x, a \rangle \rangle e \rangle \rangle T ; \sigma \cdot \{ t \} \\
\Pi_p \quad \Pi_p \quad \Pi_p
\end{array}
\]

\[\frac{
\Pi_p \quad \Pi_p
\}
\begin{array}{c}
\Gamma, \Phi : A[t] \vdash \langle \langle \Phi \mu \beta a. \langle \langle x, a \rangle \rangle e \rangle \rangle \mu T \mid x \vdash \langle \langle \Phi \mu \beta a. \langle \langle x, a \rangle \rangle e \rangle \rangle A[t] \mu \\
\end{array}
\] \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{1cm} \hspace{
dependencies as for the translation of dL\textsubscript{ω}. For instance, we could pick the calculus of constructions [28] as a very general target language, in which we would dispose of dependent types and of the expressive power to encode the type of second-order vectors from \(F_1\).

We choose to leave the choice of our target language ambiguous, and give the most general translation possible. We thus assume that the proof terms of the target language contain at least constructors for pairs, injections, equality and the same destructors as in dL\textsubscript{ω} (i.e. split, case, dest, subst, exfalso), as well as a way to encode vectors. We do not add substitutions to those proofs, but a thorough definition of the translation should also include an explicit renaming procedure, for the reasons invoked in Section 6.4.1.

This being said, the translation is derived directly from the small-step reduction rules. As for the \(\lambda\textsubscript{\omega}[l\textsubscript{\omega}r\textsubscript{\omega}]\)-calculus, the different levels \(p,e,V,f,v\) and \(t,\pi,V\) are reflected in a translation \([\_\_\_\_\_]\), for each level \(i\). The main subtlety concerns the way we handle inductive and co-inductive fixpoints, and more generally the store. Observe that in dL\textsubscript{ω} we managed to delimit the unfolding of fixpoints to the store, everything happening as if they were special cells producing computations. In other words, we could have been one step further to remove fixpoints from the syntax of proofs, limiting their occurrences strictly to the store. This is actually what is done through the translation, where we mark some cells with \(\text{IND}\) and \(\text{COFIX}\). The computational content of the fixpoint is thus decomposed step by step, each step being produced by the lookup function, that is defined (in pseudo-code) as follows:

\[
\text{lookup}\ k\ r_1[\kappa := p]\tau_2\ k \rightarrow \text{match } (\kappa,p) \text{ with }
\]

\[
| \ a,e \quad \rightarrow \ e\ r_1[a := V]\tau_2\ k
\]

\[
| \ a,V \quad \rightarrow \ V\ r_1[a := V]\tau_2\ k
\]

\[
| \ a,\text{COFIX}\ b\ x\ P \quad \rightarrow \ (p[t/x][b'/b])\ r_1[b' := \lambda\ y.\text{cofix}\ b\ x\ P]\ (\lambda\ r q \ r[a := q]\tau_2\ k)
\]

\[
| \ a,\text{IND}\ b\ x\ p_0\ P \quad \rightarrow \ p_0\ r_1[\lambda\ r q \ r[a := q]\tau_2\ k]
\]

\[
| \ a,\text{IND}\ b\ x\ S(t)\ p_0\ P \quad \rightarrow \ (p_3[t/x][b'/b])\ r_1[b' := \text{IND}\ b\ x\ p_0\ P]\ (\lambda\ r q \ r[a := q]\tau_2\ k)
\]

where in each case \(b'\) is fresh. In practice, this simply corresponds to a store where cells include a flag so that the lookup function given above could be implemented in the target language by means of pattern-matching using injections and case. The lookup function is now the only piece of the whole translation which actually has the computational content of a fixpoint.

The full translation is given by Figure 8.7 and is by construction correct with respect to reduction. In particular, we could again prove by a tedious induction on the reduction \(\rightsquigarrow_s\) that the normalization is preserved:

**Proposition 8.11.** If \([\text{ct}]\) normalizes, then so does \(\text{ct}\) for \(\rightsquigarrow_s\).

In what concerns the typing of the translation, in the case where we erase the dependencies, it would simply amount to the typing of the translation for the \(\lambda\textsubscript{\omega}[l\textsubscript{\omega}r\textsubscript{\omega}]\)-calculus, that is to say that the translation of typing judgments for proofs (resp. contexts, etc) will be of the shape:

\[
[\Gamma \vdash^* p : A] \quad \triangleq \quad (\exists \ [p]_p : [\Gamma]_{\Gamma \vdash p} \ i(A))
\]

where again:

\[
Y \vdash_p A \quad \triangleq \quad \forall Y < : Y. Y \vdash (Y \vdash_p A) \rightarrow \bot.
\]

The only novelty with respect to the CPS translation for the \(\lambda\textsubscript{\omega}[l\textsubscript{\omega}r\textsubscript{\omega}]\)-calculus sites in the lookup function in the cases of \(\text{IND}\) and \(\text{COFIX}\). However, it is easy to check that in both cases, through the translation (and already in the small-step reduction system) these elements take a continuation at level \(f\) and put in active position a proof at level \(p\) in front of a continuation which is built to be at level \(e\). In particular, types are respected in the sense that \(\text{lookup}\ a \ (r[a := \text{COFIX}\ b\ x\ P]\ p)\ k_f\) is indeed of type \(\bot\). We claim
### Commands

\[
\begin{align*}
\Gamma \vdash \Phi & \quad \Rightarrow \quad \Gamma \vdash \Phi \quad \Gamma \vdash \epsilon \\
\Gamma \vdash \phi & \quad \Rightarrow \quad \Gamma \vdash \phi \\
\Gamma \vdash \epsilon & \quad \Rightarrow \quad \Gamma \vdash \epsilon
\end{align*}
\]

### Proofs

\[
\begin{align*}
\Gamma, \eta \vdash \phi & \quad \Rightarrow \quad \Gamma \vdash \phi \quad \Gamma \vdash \epsilon \\
\Gamma, \eta \vdash \phi & \quad \Rightarrow \quad \Gamma \vdash \phi \\
\Gamma \vdash \epsilon & \quad \Rightarrow \quad \Gamma \vdash \epsilon
\end{align*}
\]

### Contexts

\[
\begin{align*}
\Gamma, \eta \vdash \phi & \quad \Rightarrow \quad \Gamma \vdash \phi \\
\Gamma, \eta \vdash \phi & \quad \Rightarrow \quad \Gamma \vdash \phi \\
\Gamma \vdash \epsilon & \quad \Rightarrow \quad \Gamma \vdash \epsilon
\end{align*}
\]

### Weak values

\[
\begin{align*}
\Gamma \vdash \eta \quad \Rightarrow \quad \Gamma \vdash \eta \\
\Gamma \vdash \epsilon & \quad \Rightarrow \quad \Gamma \vdash \epsilon
\end{align*}
\]

### Forcing contexts

\[
\begin{align*}
\Gamma, \eta \vdash \phi & \quad \Rightarrow \quad \Gamma \vdash \phi \\
\Gamma, \eta \vdash \phi & \quad \Rightarrow \quad \Gamma \vdash \phi \\
\Gamma \vdash \epsilon & \quad \Rightarrow \quad \Gamma \vdash \epsilon
\end{align*}
\]

### Strong values

\[
\begin{align*}
\Gamma \vdash \eta \quad \Rightarrow \quad \Gamma \vdash \eta \\
\Gamma \vdash \epsilon & \quad \Rightarrow \quad \Gamma \vdash \epsilon
\end{align*}
\]

### Environments

\[
\begin{align*}
\Gamma \vdash \eta \quad \Rightarrow \quad \Gamma \vdash \eta \\
\Gamma \vdash \epsilon & \quad \Rightarrow \quad \Gamma \vdash \epsilon
\end{align*}
\]

### Terms

\[
\begin{align*}
\Gamma \vdash \eta \quad \Rightarrow \quad \Gamma \vdash \eta \\
\Gamma \vdash \epsilon & \quad \Rightarrow \quad \Gamma \vdash \epsilon
\end{align*}
\]

---

Figure 8.7: Continuation-and-store-passing style translation
than once we understood how the translation of the $\bar{\lambda}_{[\mu v \tau \star]}$-calculus was typed, this setting is more or less the same and should not give us a hard time.

However, in the case where we would like to obtain a translation compatible with dependent types, we know that we need to refine the typing of terms and NEF proof terms, as we did in $\mathsf{dL}_\phi$. This is certainly possible, in particular given a NEF proof term $p$, it is still possible to pass the continuation $\lambda t.a$ to $\sqbracks{p}$ to force the extraction of a proof $p^*_N$. This should allow us to refine the type of $\sqbracks{p}$ to obtain something like:

$$\forall Y \prec p. A \triangleq \forall Y < : Y. Y \to \forall R. \forall a : (Y \prec p). R(a) \to R(p^*_N).$$

However, due to the laziness and the two layers of alternation between proof and contexts, we should probably proceed to a second extraction to obtain a strong value, and cleverly handle the store while doing so. In the absence of a real motivation for such a translation, we did not take the time to study the question more in depth. However we are confident in the fact that the main difficulties has been studied in the previous chapters, so that if it was worthwhile, with time and rigor, it should be possible to methodically obtain a translation of types compatible with the dependencies.

### 8.4 Normalization of $\mathsf{dLPA}^\omega$

#### 8.4.1 A realizability interpretation of $\mathsf{dLPA}^\omega$

We shall now present the realizability interpretation of $\mathsf{dLPA}^\omega$, which will finally give us a proof of its normalization. Here again, the interpretation combines ideas of the interpretations for the $\bar{\lambda}_{[\mu v \tau \star]}$-calculus (Chapter 6) and for $\mathsf{dL}_\phi$ through the embedding in Lepigre’s calculus (Chapter 7). Namely, as for the $\bar{\lambda}_{[\mu v \tau \star]}$-calculus, formulas will be interpreted by sets of proofs-in-store of the shape $(p|\tau)$, and the orthogonality will be defined between proofs-in-store $(p|\tau)$ and contexts-in-store $(e|\tau')$ such that the stores $\tau$ and $\tau'$ are compatible.

We recall the main definition necessary to the realizability interpretation:

**Definition 8.12 (Proofs-in-store).** We call closed proof-in-store (resp. closed context-in-store, closed term-in-store, etc) the combination of a proof $p$ (resp. context $e$, term $t$, etc) with a closed store $\tau$ such that $\mathsf{FV}(p) \subseteq \mathsf{dom}(\tau)$. We use the notation $(p|\tau)$ to denote such a pair. In addition, we denote by $\Lambda_p$ (resp. $\Lambda_e$, etc.) the set of all proofs and by $\Lambda^+_p$ (resp. $\Lambda^+e$, etc.) the set of all proofs-in-store.

We denote the sets of closed closures by $C_0$, and we identify again $(c|\tau)$ with the closure $c\tau$ when $c$ is closed in $\tau$. We can now define the notion of pole, which has to satisfy an extra condition due to the presence of delimited continuations

**Definition 8.13 (Pole).** A subset $\bot \in C_0$ is said to be saturated or closed by anti-reduction whenever for all $(c|\tau), (c'|\tau') \in C_0$, we have

$$(c'|\tau' \in \bot) \land (c\tau \to c'|\tau') \Rightarrow (c\tau \in \bot)$$

It is said to be closed by store extension if whenever $c\tau$ is in $\bot$, for any store $\tau'$ extending $\tau$, $c\tau'$ is also in $\bot$:

$$(c\tau \in \bot) \land (\tau \triangleleft \tau') \Rightarrow (c\tau' \in \bot)$$

It is said to be closed under delimited continuations if whenever $c[e/\hat{\Phi}]\tau$ (resp. $c[V/\hat{\Phi}]\tau$) is in $\bot$, then $(\mu \hat{\Phi}.c|e)\tau$ (resp. $(\nu \hat{\Phi}.c).\tau$) belongs to $\bot$:

$$(c[e/\hat{\Phi}]\tau \in \bot) \Rightarrow ((\mu \hat{\Phi}.c|e)\tau \in \bot) \quad (c[V/\hat{\Phi}]\tau \in \bot) \Rightarrow ((\nu \hat{\Phi}.c)\tau \in \bot)$$

A pole is defined as any subset of $C_0$ that is closed by anti-reduction, by store extension and under delimited continuations.
We can verify that the set of normalizing command is indeed a pole:

**Proposition 8.14.** The set $\parallel = \{c\tau \in C_0 : c\tau \text{ normalizes} \}$ is a pole.

**Proof.** The first two conditions have already been verified for the $\lambda_\{V,\ast\}$-calculus. The third one is straightforward, since if a closure $\mu(\Phi, c[\epsilon] e)\tau$ is not normalizing, it is easy to verify that $c[e/\Phi]$ is not normalizing either. Roughly, there is only two possible reduction steps for a command $(\mu(\Phi, c[\epsilon] e)\tau)$: either it reduces to $(\mu(\Phi, c[\epsilon] e)\tau')$, in which case $c[e/\Phi]\tau$ also reduces to a closure which is almost $(c'\tau')[e/\Phi]$; or $c$ is of the shape $(p\[\Phi])$ and it reduces to $c[e/\Phi]\tau$. In both cases, if $(\mu(\Phi, c[\epsilon] e)\tau$ can reduce, so can $c[e/\Phi]\tau$. The same reasoning allows us to show that if $c[V/\Phi]\tau$ normalizes, then so does $(V\parallel \mu(\Phi, c)e)\tau$ for any value $sV$.

We now recall the notion of compatible stores, which allows us to define an orthogonality relation between proofs- and contexts-in-store.

**Definition 8.15 (Compatible stores and union).** Let $\tau$ and $\tau'$ be stores, we say that:

- they are *independent* and note $\tau \# \tau'$ when $\text{dom}(\tau) \cap \text{dom}(\tau') = \emptyset$.
- they are *compatible* and note $\tau \circ \tau'$ whenever for all variables $a$ (resp. co-variables $\alpha$) present in both stores: $a \in \text{dom}(\tau) \cap \text{dom}(\tau')$; the corresponding proofs (resp. contexts) in $\tau$ and $\tau'$ coincide.
- $\tau'$ is an *extension* of $\tau$ and we write $\tau < \tau'$ whenever $\text{dom}(\tau) \subseteq \text{dom}(\tau')$ and $\tau \circ \tau'$.
- the compatible union $\overline{\tau \tau'}$ of compatible closed stores $\tau$ and $\tau'$, is defined as $\text{join}(\tau, \tau')$, which itself given by:

$$
\text{join}(\tau_0[a := p], \tau_0'[a := p]) \triangleq \tau_0[\alpha := p] \text{join}(\tau_1, \tau_1') \quad \text{(if $\tau_0 \# \tau_0'$)}
$$

$$
\text{join}(\tau_0[a := e], \tau_0'[\alpha := e]) \triangleq \tau_0[\alpha := e] \text{join}(\tau_1, \tau_1') \quad \text{(if $\tau_0 \# \tau_0'$)}
$$

$$
\text{join}(\tau \tau') \triangleq \tau \tau' \quad \text{(if $\tau \# \tau'$)}
$$

The next lemma (which follows from the previous definition) states the main property we will use about union of compatible stores.

**Lemma 8.16.** If $\tau$ and $\tau'$ are two compatible stores, then $\tau < \overline{\tau \tau'}$ and $\tau' < \overline{\tau \tau'}$. Besides, if $\tau$ is of the form $\tau_0[x := t] \tau_1$, then $\overline{\tau \tau'}$ is of the form $\overline{\tau_0[x := t] \tau_1}$ with $\tau_0 < \overline{\tau_0}$ and $\tau_1 < \overline{\tau_1}$.

We recall the definition of the orthogonality relation with respect to a pole, which is identical to the one for the $\lambda_\{V,\ast\}$-calculus:

**Definition 8.17 (Orthogonality).** Given a pole $\parallel$, we say that a proof-in-store $(p|\tau)$ is *orthogonal* to a context-in-store $(e|\tau')$ and write $(p|\tau) \parallel (e|\tau')$ if $\tau$ and $\tau'$ are compatible and $(p|e)\overline{\tau \tau'} \in \parallel$. The orthogonality between terms and coterm is defined identically.

We are now equipped to define the realizability interpretation of dLPA$^\omega$. Firstly, in order to simplify the treatment of coinductive formulas, we extend the language of formulas with second-order variables $X, Y, \ldots$ and we replace $v_x^T A$ by $v_x^{\Sigma} A[X(y)/f(y) = 0]$. The typing rule for co-fixpoint operators then becomes:

$$
\Gamma \vdash \sigma \quad t : T \quad \Gamma, x : T, \bar{b} : \forall y^T X(y) \vdash p : A \quad X \text{ positive in } A \quad X \notin \text{FV} (\Gamma)
$$

$$
\Gamma \vdash \sigma \quad \text{cofix}_{bs}^\Gamma[p] : v_x^{\Sigma} A \quad \text{(cofix)}
$$

Secondly, as in the interpretation of dL$\Phi^\parallel$ through Lepigre’s calculus, we introduce two new predicates, $p \in A$ for nef proofs and $t \in T$ for terms. This allows us to decompose the dependent products and sums into:

$$
\forall x^T A \triangleq \forall x.(x \in T \rightarrow A) \quad \Pi a : A B \triangleq \forall a.(a \in A \rightarrow B) \quad \text{(if } a \in \text{FV}(B))
$$

$$
\exists x^T A \triangleq \exists x.(x \in T \rightarrow A) \quad \Pi a : A B \triangleq A \rightarrow B \quad \text{(if } a \notin \text{FV}(B))
$$

218
This corresponds to the language of formulas and types defined by:

**Types**

\[ T, U ::= N \mid T \rightarrow U \mid t \in T \]

**Formulas**

\[ A, B ::= \top \mid \bot \mid X(t) \mid t = u \mid A \land B \mid A \lor B \mid a \in A \mid \forall x.A \mid \exists x.A \mid v_{Xx}^t.A \]

and to the following inference rules:

\[
\begin{align*}
\frac{\Gamma \vdash \sigma \nu : A \quad x \notin \text{FV}(\Gamma)}{\Gamma \vdash \sigma \nu : \forall x.A} & \quad (\nu^\forall) \\
\frac{\Gamma \vdash \sigma \nu : A \quad \forall x.A}{\Gamma \vdash \sigma \nu : \forall x.A} & \quad (\nu^\forall) \\
\frac{\Gamma \vdash \sigma \nu : A[q/a]}{\Gamma \vdash \sigma \nu : \exists x.A} & \quad (\nu^\exists) \\
\frac{\Gamma \vdash \sigma \nu : A[t/x]}{\Gamma \vdash \sigma \nu : (\exists x.A)^\perp} & \quad (\nu^\exists) \\
\frac{\Gamma \vdash \sigma \nu \pi : A[t/\bot]}{\Gamma \vdash \sigma \nu \pi : T} & \quad (\nu^\forall)
\end{align*}
\]

These rules are exactly the same as in Lepigre’s calculus \[103\] up to our stratified presentation in a sequent calculus fashion and modulo our syntactic restriction to \text{NEF} proofs instead of his semantical restriction. It is a straightforward verification to check that the typability is maintained through the decomposition of dependent products and sums.

Another similarity with Lepigre’s realizability model is that truth/falsity values will be closed under observational equivalence of proofs and terms. To this purpose, for each store \( \tau \) we introduce the relation \( \equiv\tau \), which we define as the reflexive-transitive-symmetric closure of the relation \( \triangleright^\tau \):

\[ t \triangleright^\tau t' \quad \text{whenever} \quad \exists \tau', \forall \pi, ((t\|\pi)\tau \rightarrow (t'\|\pi)\tau') \]

\[ p \triangleright^\tau q \quad \text{whenever} \quad \exists \tau', \forall f ((p\|f)\tau \rightarrow (q\|f)\tau') \]

All this being settled, it only remains to determine how to interpret coinductive formulas. While it would be natural to try to interpret them by fixpoints in the semantics, this poses difficulties for the proof of adequacy. We will discuss this matter in the next section, but as for now, we will give a simpler interpretation. We stick to the intuition that since \text{cofix} operators are lazily evaluated, they actually are realizers of every finite approximation of the (possibly infinite) coinductive formulas. Consider for instance the case of a stream

\[ \text{str}^{0}_{\omega}\rho \triangleq \text{cofix}^{0}_{\omega}\rho \left( (px, b(S(x))) \right) \]

of type \( v_{Xx}^0.A(x) \land f(S(x)) = 0 \). Such stream will produce on demand any tuple \((p\_0, (p\_1, \ldots, (p\_n, ]) \ldots)\)

where \( \square \) denotes the fact that it could be any term, in particular \( \text{str}^{n+1}\omega\rho \). So that \( \text{str}^{n\_\omega}\rho \) should be a successful defender of the formula

\[ (A(0) \land (A(1) \land \ldots (A(n) \land \top) \ldots) \]

Since \text{cofix} operators only reduce when they are bound to a variable in a front of a forcing context, it suggests to interpret the coinductive formula \( v_{Xx}^0.A(x) \land X(S(x)) \) at level \( f \) as the union of all the opponents to a finite approximation.

To this end, given a coinductive formula \( v_{Xx}^0.A \) where \( X \) is positive in \( A \), we define its finite approximations by:

\[ F^{0}_{A,t} \triangleq \top \quad F^{n+1}_{A,t} \triangleq A[t/x][F^n_{A,y}/X(y)] \]

Since \( f \) is positive in \( A \), we have for any integer \( n \) and any term \( t \) that \( ||F^n_{A,t}||_f \subseteq ||F^{n+1}_{A,t}||_f \). We can finally define the interpretation of coinductive formulas by:

\[ ||v_{Xx}^t.A||_f \triangleq \bigcup_{n \in \mathbb{N}} ||F^n_{A,t}||_f \]
\[
\begin{align*}
||\bot||_f & \triangleq \Lambda_f^T \\
||\top||_f & \triangleq \emptyset \\
||\overline{F}(t)||_f & \triangleq F(t) \\
||t = u||_f & \triangleq \begin{cases} \{ (\overline{e}.c(r) : cr \in \bot) \} & \text{if } t \equiv_r u \\
\{ \Lambda^T_f \} & \text{otherwise} \end{cases} \\
||p \in A||_f & \triangleq \{ (V[r] \in |A|_V : V \equiv_r p) \}^{\mu_f} \\
||T \rightarrow B||_f & \triangleq \{ (V \cdot e[r] : (V[r]) \in |T| V \land (e[r]) \in ||B||_e) \} \\
||A \rightarrow B||_f & \triangleq \{ (V \cdot e[r] : (V[r]) \in |A|_V \land (e[r]) \in ||B||_e) \} \\
||T \land A||_f & \triangleq \{ (\overline{\mu}(x,a).c(r) : \forall \tau', V \in |T| V', V \in |A|_V', \tau \circ \tau' \Rightarrow c[V'/x] \overline{\tau}'[a : V] \in \bot) \} \\
||A_1 \lor A_2||_f & \triangleq \{ (\overline{\mu}(a_1,a_2).c(r) : \forall \tau', V \in |A_1|_V', V \in |A_2|_V', \tau \circ \tau' \Rightarrow c[V'/x] \overline{\tau}'[a_1 := V_1][a_2 := V_2] \in \bot) \} \\
||A_1 \land A_2||_f & \triangleq \{ (\overline{\mu}(a_1,a_2).c(r) : \forall \tau' \land (V[r]) \in |T| V \land (e[r]) \in ||B||_e) \} \\
||\exists x. A||_f & \triangleq (\bigcap_{t \in A_t} ||A[t/x]||_f) \\
||\forall x. A||_f & \triangleq (\bigcap_{t \in A_t} ||A[t/x]||_f) \\
||\forall^{\mu_f}_t A||_f & \triangleq (\bigcap_{t \in A_t} ||A[p/a]||_{\mu_f}^{\mu_f}) \\
||\forall^{v_f}_t A||_f & \triangleq \bigcup_{n \in N} ||F^n_{A_t}||_f \\
|A|_V & \triangleq ||A||_V^{\mu_f} = \{ (V[r] : \forall f \tau', \tau \circ \tau' \land (f[\tau']) \in ||A||_f \Rightarrow (V[r]) \cup (F[\tau']) \} \\
|A|_V & \triangleq ||A||_V^{\mu_f} = \{ (F[r] : \forall \tau' \land (V[\tau']) \in |A|_V \Rightarrow (V[r]) \cup (F[\tau']) \} \\
|A|_p & \triangleq ||A||_p^{\mu_f} = \{ (p[r] : \forall \tau' \land (E[\tau']) \in ||A||_E \Rightarrow (t[r]) \cup (E[\tau']) \} \\
|N|_{V_1} & \triangleq \{ (S^n(0)[r]) : n \in \mathbb{N} \} \\
|t|_V & \triangleq \{ (V[r] : (V[r]) \in |T| V) \} \\
|T \rightarrow U|_{V_1} & \triangleq \{ (\lambda x. t[r] : \forall \tau' \land (V_1[\tau']) \in |T|_{V_1} \Rightarrow (t[V'/x] \overline{\tau}'[a]) \in |U|_{V_1}) \} \\
|T|_\tau & \triangleq ||A||_{V^\tau} = \{ (F[r] : \forall \tau' \land (V[\tau']) \in |A|_V \Rightarrow (V[r]) \cup (F[\tau']) \} \\
|T|_t & \triangleq ||A||_{t^\tau} = \{ (V[r] : \forall F \tau' \land (F[\tau']) \in ||A||_F \Rightarrow (V[r]) \cup (F[\tau']) \} \\
\end{align*}
\]

where:

- \( p \in S_f \) (resp. \( e,V,\text{etc.} \)) denote \( (p[r]) \in S \) (resp. \( (e[r]),(V[r]),\text{etc.} \)).
- \( F \) is a function from \( \Lambda_f \) to \( \mathcal{P}(\Lambda_f^T) \).

Figure 8.8: Realizability interpretation for dLPA^{\omega_0}

The realizability interpretation of closed formulas and types is defined in Figure 8.8 by induction on the structure of formulas at level \( f \), and by orthogonality at levels \( V,e,p \). When \( S \) is a subset of \( \mathcal{P}(\Lambda_f^T) \) (resp. \( \mathcal{P}(\Lambda_f^T),\mathcal{P}(\Lambda_f^T),\mathcal{P}(\Lambda_f^T) \)), we use the notation \( S^{\mu_f} \) (resp. \( S^{\mu_f}, \text{etc.} \)) to denote its orthogonal set restricted to \( \Lambda_f^T \) (resp. \( \Lambda_f^T, \text{etc.} \)):

\[
S^{\mu_f} \triangleq \{ (f[r]) \in \Lambda_f^T : \forall (p[r']) \in S, r \circ r' \Rightarrow (p[r]) \overline{\tau}' \in \bot \}
\]

At level \( f \), closed formulas are interpreted by sets of strong forcing contexts-in-store \( (f[r]) \). As observed in the previous section, these sets are besides closed under the relation \( \equiv_r \) along their component \( r \), we thus denote them by \( \mathcal{P}(\Lambda_f^T) \). Second-order variables \( X,Y,\ldots \) are then interpreted by functions from the set of terms \( \Lambda_t \) to \( \mathcal{P}(\Lambda_f^T) \) and as usual for each such function \( F \) we add a predicate symbol \( \overline{F} \) in the language.

We shall now prove the adequacy of the interpretation with respect to the type system. To this end, we need to recall a few definitions and lemmas. Since stores only contain proof terms, we need
to define valuations for term variables in order to close formula\(^9\). These valuations are defined by the usual grammar:

\[
\rho := ε | ρ[x → V_t] | ρ[X → F]
\]

We denote by \((p|τ)_ρ\) (resp. \(p_ρ, A_ρ\)) the proof-in-store \((p|τ)\) where all the variables \(x ∈ \text{dom}(ρ)\) (resp. \(X ∈ \text{dom}(ρ)\)) have been substituted by the corresponding term \(ρ(x)\) (resp. falsity value \(ρ(x)\)).

**Definition 8.18.** Given a closed store \(τ\), a valuation \(ρ\) and a fixed pole \(⊥\), we say that the pair \((τ, ρ)\) realizes \(Γ\), which we write\(^{10}\) \((τ, ρ) ⊨ Γ\), if:

1. for any \((a : A) ∈ Γ\), \((a|τ)_ρ ∈ |A_ρ|_V\)
2. for any \((α : A^*_ρ) ∈ Γ\), \((α|τ)_ρ ∈ |A_ρ|_e\)
3. for any \(a|p⟩ ∈ σ\), \(a ≡_τ p\)
4. for any \((x : T) ∈ Γ\), \(x ∈ \text{dom}(ρ)\) and \((ρ(x)|τ)_ρ ∈ |T_ρ|_V\)

We recall two key properties of the interpretation, whose proofs are similar to the proofs for the corresponding statement in the \(\lambda[⊥,τ,⊥,ε,τ]\)-calculus (Lemma 6.16 and Proposition 6.14):

**Lemma 8.19** (Store weakening). Let \(τ\) and \(τ’\) be two stores such that \(τ ⊲ τ’\), let \(Γ\) be a typing context, let \(⊥\) be a pole and \(ρ\) a valuation. The following statements hold:

1. \(τ τ' = τ'\)
2. If \((p|τ)_ρ ∈ |A_ρ|_p\) for some closed proof-in-store \((p|τ)_ρ\) and formula \(A\), then \((p|τ’)_ρ ∈ |A_ρ|_p\). The same holds for each level \(e, E, V, f, t, π, V_t\) of the interpretation.
3. If \((τ, ρ) ⊨ Γ\) then \((τ’ , ρ) ⊨ Γ\).

**Proposition 8.20** (Monotonicity). For any closed formula \(A\), any type \(T\) and any given pole \(⊥\), we have the following inclusions:

\[|A|_V ⊆ |A|_p \quad |A|_f ⊆ |A|_e \quad |T|_V ⊆ |T|_f\]

Finally we can check that the interpretation is indeed defined up to the relations \(≡_τ:\)

**Lemma 8.21.** For any store \(τ\) and any valuation \(ρ\), the component along \(τ\) of the truth and falsity values defined in Figure 8.3 are closed under the relation \(≡_τ:\)

1. if \((f|τ)_ρ ∈ |A_ρ|_f\) and \(A_ρ ≡_τ B_ρ\), then \((f|τ)_ρ ∈ |B_ρ|_f\),
2. if \((V_t|τ)_ρ ∈ |A_ρ|_V\) and \(A_ρ ≡_τ B_ρ\), then \((V_t|τ)_ρ ∈ |B_ρ|_V\).

The same applies with \(|A_ρ|_p\), \(|A_ρ|_e\), etc.

**Proof.** By induction on the structure of \(A_ρ\) and the different levels of interpretation. The different base cases \((p ∈ A_ρ, t ∈ T, t = u)\) are direct since their components along \(τ\) are defined modulo \(≡_τ\), the other cases are trivial inductions. \(\Box\)

**Proposition 8.22** (Adequacy). The typing rules are adequate with respect to the realizability interpretation. In other words, if \(Γ\) is a typing context, \(⊥\) a pole, \(ρ\) a valuation and \(τ\) a store such that \((τ, ρ) ⊨ Γ\); \(σ\), then the following hold:

1. If \(v\) is a strong value such that \(Γ ⊢ v : A\) or \(Γ ⊢_d v : A; σ\), then \((v|τ)_ρ ∈ |A_ρ|_V\).

\(^9\)Alternatively, we could have modified the small-step reduction rules to include substitutions of terms.

\(^{10}\)Once again, we should formally write \((τ, ρ) ⊨ Γ\) but we will omit the annotation by \(⊥\) as often as possible.
2. If \( f \) is a forcing context such that \( \Gamma \vdash^\sigma f : A \equiv f \) or \( \Gamma \vdash^\rho f : A \equiv f \), then \((f|\tau)_\rho \in \|A_\rho\|_f\).

3. If \( V \) is a weak value such that \( \Gamma \vdash^\sigma V : A \equiv V \) or \( \Gamma \vdash^\rho V : A \equiv V \), then \((V|\tau)_\rho \in \|A_\rho\|_V\).

4. If \( e \) is a context such that \( \Gamma \vdash^\sigma e : A \equiv e \) or \( \Gamma \vdash^\rho e : A \equiv e \), then \((e|\tau)_\rho \in \|A_\rho\|_e\).

5. If \( p \) is a proof term such that \( \Gamma \vdash^\rho p : A \equiv p \) or \( \Gamma \vdash^\rho p : A \equiv p \), then \((p|\tau)_\rho \in \|A_\rho\|_p\).

6. If \( V_t \) is a term value such that \( \Gamma \vdash^\rho V_t : T \equiv V_t \), then \((V_t|\tau)_\rho \in \|T_\rho\|_{V_t}\).

7. If \( \pi \) is a term context such that \( \Gamma \vdash^\rho \pi : T \equiv \pi \), then \((\pi|\tau)_\rho \in \|T_\rho\|_{\pi}\).

8. If \( t \) is a term such that \( \Gamma \vdash^\rho t : T \equiv t \), then \((t|\tau)_\rho \in \|T_\rho\|_{t}\).

9. If \( \tau' \) is a store such that \( \Gamma \vdash^\rho \tau' : (\Gamma';\sigma') \equiv\tau' \), then \((\tau\tau'|\rho) \equiv (\Gamma',\sigma';\rho')\).

10. If \( c \) is a command such that \( \Gamma \vdash^\rho c \equiv \Gamma \vdash^\rho c \), then \((c\tau|\rho) \equiv \perp\).

11. If \( \tau\tau' \) is a closure such that \( \Gamma \vdash^\rho \tau\tau' \equiv \Gamma \vdash^\rho \tau\tau' \), then \((c\tau\tau'|\rho) \equiv \perp\).

**Proof.** The proof is done by induction on the typing derivation such as given in the system extended with the small-step reduction \( \rightsquigarrow_s \). Most of the cases correspond to the proof of adequacy for the interpretation of the \( \Lambda_{\{|\tau|\}} \)-calculus, so that we only give the most interesting cases. To lighten the notations, we omit the annotation by the valuation \( \rho \) whenever it is possible.

- **Case (\( \exists \)).** We recall the typing rule through the decomposition of dependent sums:

\[
\begin{align*}
\Gamma \vdash^\sigma t : u \in T & \quad \Gamma \vdash^\rho p : A[u/x] \\
\hline \\
\Gamma \vdash^\rho (t,p) : (u \in T \land A[u]) 
\end{align*}
\]

By induction hypothesis, we obtain that \((t|\tau) \in \|u \in T|\_\tau\) and \((p|\tau) \in \|A[u]|_\rho\). Consider thus any context-in-store \((e|\tau') \in \|u \in T \land A[u]|_e\) such that \(\tau\) and \(\tau'\) are compatible, and let us denote by \(\tau_0\) the union \(\tau\tau'\). We have:

\[
\langle(t,p)|e\rangle_{\rho_{\tau_0}} \rightsquigarrow_s \langle p\parallel \Phi.\langle t\parallel \mu x.\langle \Phi\parallel \mu a.\langle (x,a)|e\rangle\rangle\rangle_{\rho_{\tau_0}}
\]

so that by anti-reduction, we need to show that \(\mu \Phi.\langle t\parallel \mu x.\langle \Phi\parallel \mu a.\langle (x,a)|e\rangle\rangle\rangle_{\rho_{\tau_0}} \equiv (\Gamma',\sigma';\rho')\). Let us then consider a value-in-store \((V|\tau'_0) \in \|A[u]|_\tau\) such that \(\tau_0\) and \(\tau'_0\) are compatible, and let us denote by \(\tau_1\) the union \(\tau\tau'_0\). By closure under delimited continuations, to show that \((V|\mu \Phi.\langle t\parallel \mu x.\langle \Phi\parallel \mu a.\langle (x,a)|e\rangle\rangle\rangle_{\rho_{\tau_1}} \equiv \perp\). Thus it suffices to show that the cotermin-in-store \((\mu \Phi.\langle V\parallel \mu a.\langle (x,a)|e\rangle\rangle\rangle_{\rho_{\tau_1}} \equiv \perp\).

Consider a term value-in-store \((V_t|\tau'_1) \in \|u \in T|V_t\) such that \(\tau_1\) and \(\tau'_1\) are compatible, and let us denote by \(\tau_2\) the union \(\tau\tau'_1\). We have:

\[
\langle V_t\parallel \mu x.\langle V\parallel \mu a.\langle (x,a)|e\rangle\rangle\rangle_{\tau_2} \rightsquigarrow_s \langle V\parallel \mu a.\langle (V_t,a)|e\rangle\rangle\rangle_{\tau_2} \rightsquigarrow_s \langle (V_t,a)|e\rangle\rangle_{\tau_2}[a := V]
\]

It is now easy to check that \((A_t,a)\rangle\rangle_{\tau_2}[a := V]\rangle\rangle_{\tau_2} \in \|u \in T \land A[u]|_\tau\) and to conclude, using Lemma 8.19 to get \((e|\tau_2[a := V]) \in \|u \in T \land A[u]|_e\), that this closure is finally in the pole.

- **Case (\( \equiv_{\tau} \),\( \equiv_t \)).** These cases are direct consequences of Lemma 8.21 since if \(A \equiv B\), in particular \(A \equiv_{\tau} B\) and thus \(|A|_\tau = |B|_\tau\).

- **Case (\( \text{ref}1 \),\( \equiv_t \)).** The case for \( \text{ref}1 \) is trivial, while it is trivial to show that \((\mu \Phi.\langle p|e\rangle|\tau) \equiv \perp\) if \((p|\tau) \in \|A|_\rho\) and \((e|\tau) \in \|A[u]|_e\). Indeed, either \(t \equiv_{\tau} u\) and thus \(A[t] \equiv_{\tau} A[u]\) (Lemma 8.21) or \(t \not\equiv_{\tau} u\) and \(\|t = u|_f = \Lambda_f\).
8.4. NORMALIZATION OF dLPA^ω

- **Case** \( (V^r) \). This case is standard in a call-by-value language with value restriction. We recall the typing rule:

\[
\Gamma \vdash^\sigma v : A \quad x \notin \text{FV}(\Gamma) \\
\frac{}{\Gamma \vdash^\sigma v : \forall x.A} \quad (\forall^r)
\]

The induction hypothesis gives us that \( (v|\tau)_p \) is in \( |A_p|_V \) for any valuation \( \rho[x \mapsto t] \). Then for any \( t \), we have \( (v|\tau)_p \in |A_p[t/x]|_{F^\mu}^\omega \) so that \( (v|\tau)_p \in (\bigcap_{\rho \in \Lambda} |A[t/x]|_{F^\mu}^\omega) \). Therefore if \( (f|\tau')_p \) belongs to \( |V_x.A_p|_F = (\bigcap_{\rho \in \Lambda} |A[t/x]|_{F^\mu}^\omega) \), we have by definition that \( (v|\tau)_p \perp_\mu (f|\tau')_p \).

- **Case** \( (\text{ind}) \). We recall the typing rule:

\[
\begin{array}{c}
\Gamma \vdash^\sigma t : \text{N} \\
\Gamma \vdash^\sigma p_0 : A[0/x] \\
\Gamma, x : T, a : A \vdash^\sigma p_S : A[S(x)/x]
\end{array} \\
\frac{}{\Gamma \vdash^\sigma \text{ind}^\mu_{bx}[p_0 | p_S] : A[t/x]} \quad (\text{ind})
\]

We want to show that \( (\text{ind}^\mu_{bx}[p_0 | p_S] | \tau)_p \in |A[t]|_p \). Let us then consider \( (e|\tau')_p \in |A[t]|_p \) such that \( \tau \) and \( \tau' \) are compatible, and let us denote by \( \tau_0 \) the union \( \tau \tau' \). By induction hypothesis, we have \( \tau_0 \in \mathbb{N} \) and we have:

\[
\langle \text{ind}^\mu_{bx}[p_0 | p_S] | e \rangle_{\tau_0} \sim_s \langle \mu \Phi.(t)\tilde{\mu}y.(a\|\Phi)[a := \text{ind}^\mu_{bx}[p_0 | p_S]] | e \rangle_{\tau_0}
\]

so that by anti-reduction and closure under delimited continuations, it is enough to show that the coterm-in-store \( (\mu y.(a|e)[a := \text{ind}^\mu_{bx}[p_0 | p_S]] | \tau_1) \) is in \( |t|_N \). Let us then consider \( (V_i|\tau'_i)_p \in |t|_N \) such that \( \tau_0 \) and \( \tau'_i \) are compatible, and let us denote by \( \tau_1 \) the union \( \tau_0 \tau'_i \). By definition, \( V_i = S^0(0) \) for some \( n \in \text{N} \) and \( t = S^0(0) \), and we have:

\[
\langle S^0(0)|\mu y.(a|e)[a := \text{ind}^\mu_{bx}[p_0 | p_S]] | \tau_1 \rangle \sim_s \langle a|e \rangle_{\tau_1}[a := \text{ind}^{S^0(0)}_{bx}[p_0 | p_S]]
\]

We conclude by showing by induction on the natural numbers that for any \( n \in \text{N} \), the value-in-store \( (a|\tau_1[a := \text{ind}^{S^0(0)}_{bx}[p_0 | p_S]]) \) is in \( |A[S^0(0)]|_V \). Let us consider \( (f|\tau'_i)_p \in |A[S^0(0)]|_F \) such that the store \( \tau_1[a := \text{ind}^{S^0(0)}_{bx}[p_0 | p_S]] \) and \( \tau'_i \) are compatible, and let us denote by \( \tau_2[a := \text{ind}^{S^0(0)}_{bx}[p_0 | p_S]] \) their union.

- If \( n = 0 \), we have:

\[
\langle a|f \rangle_{\tau_2[a := \text{ind}^{S^0(0)}_{bx}[p_0 | p_S]]} \sim_s \langle p_0|\tilde{\mu}a.(a|f)_{\tau'_i} \rangle_{\tau_2}
\]

We conclude by anti-reduction and the induction hypothesis for \( p_0 \), since it is easy to show that \( (\tilde{\mu}a.(a|f)_{\tau'_i} \rangle_{\tau_2} \in |A[0]|_\epsilon \).

- If \( n = S(m) \), we have:

\[
\langle a|f \rangle_{\tau_2[a := \text{ind}^{S(m)}_{bx}[p_0 | p_S]]} \sim_s \langle p_0[S^0(0)/x][b'|b]\|\tilde{\mu}a.(a|f)_{\tau'_i} \rangle_{p_0} \tau_2[b' := \text{ind}^{S(m)}_{bx}[p_0 | p_S]]
\]

Since we have by induction that \( (b'|\tau_2[b' := \text{ind}^{S(m)}_{bx}[p_0 | p_S]]) \in |A[S^0(0)]|_V \), we can conclude by anti-reduction, using the induction hypothesis for \( p_S \) and the fact that \( (\tilde{\mu}a.(a|f)_{\tau'_i} \rangle_{\tau_2} \) belongs to \( |A[S^0(0)]|_\epsilon \).

\(^{13}\)Recall that any term \( t \) of type \( T \) can be given the type \( t \in T \).
CHAPTER 8. A SEQUENT CALCULUS WITH DEPENDENT TYPES FOR CLASSICAL ARITHMETIC

• Case (cofix). We recall the typing rule:

\[
\Gamma \vdash \tau : T \quad \Gamma, x : T, b : \forall y. X(y) \vdash \sigma \quad \rho : A \quad X \text{ positive in } A \quad X \notin FV(\Gamma)
\]

\[
\Gamma \vdash \sigma \quad \text{cofix}_{b_{x}}[p] : v_{x}^{\tau}A
\]

\[\text{(cofix)}\]

We want to show that \((\text{cofix}_{b_{x}}[p])[\tau] \in \forall v_{x}^{\tau}A\), let us then consider \((e|\tau') \in \forall v_{x}^{\tau}A\), such that \(\tau\) and \(\tau'\) are compatible, and let us denote by \(r_{0}\) the union \(\tau \tau'\). By induction hypothesis, we have \(\tau \in \| t \|_{t}\) and we have:

\[
\langle \text{cofix}_{b_{x}}[p]\rangle e_{r_{0}} \leadsto_{\tau} \langle \mu \Phi.(t\mu y.\langle a \| \Phi\rangle[a := \text{cofix}_{b_{x}}[p]]\rangle e_{r_{0}}
\]

so that by anti-reduction and closure under delimited continuations, it is enough to show that the cterm-in-store \((\mu y.(\langle a \| \Phi\rangle[a := \text{cofix}_{b_{x}}[p]]\rangle r_{0})\) is in \(\| t \|_{t}\). Let us then consider \((V_{i}|r_{0}') \in \| t \|_{i}\) such that \(r_{0}\) and \(r_{0}'\) are compatible, and let us denote by \(r_{2}\) the union \(r_{0}r_{0}'\). We have:

\[
\langle V_{i}\| y.\langle a \| \Phi\rangle[a := \text{cofix}_{b_{x}}[p]]\rangle r_{1} \leadsto_{\tau} \langle a \| \Phi\rangle r_{1}[a := \text{cofix}_{b_{x}}[p]]
\]

It suffices to show now that the value-in-store \((a|r_{1}[a := \text{cofix}_{b_{x}}[p]])\) is in \(\forall v_{x}^{\tau}A\). By definition, we have:

\[
|v_{x}^{\tau}A|_{V} = (\bigcup_{n \in \mathbb{N}} |F_{A,V}|_{f})^{+\tau} = \bigcap_{n \in \mathbb{N}} |F_{A,V}|_{f}^{\tau} = \bigcap_{n \in \mathbb{N}} |F_{A,V}|_{f}
\]

We conclude by showing on the natural numbers that for any \(n \in \mathbb{N}\) and any \(V_{i}\), the value-in-store \((a|r_{1}[a := \text{cofix}_{b_{x}}[p]])\) is in \(\bigcap_{n \in \mathbb{N}} |F_{A,V}|_{f}\).

The case \(n = 0\) is trivial since \(\bigcap_{n = 0} |F_{A,V}|_{f} = |A|_{V} = \Lambda_{V}^{+\tau}\). Let then \(n\) be an integer and any \(V_{i}\) be a term value. Let us consider \((f|r_{1}') \in \bigcap_{n \in \mathbb{N}} |F_{A,V}|_{f}\) such that \(r_{1}[a := \text{cofix}_{b_{x}}[p]]\) and \(r_{1}'\) are compatible, and let us denote by \(r_{2}[a := \text{cofix}_{b_{x}}[p]]\) \(r_{2}'\) their union. By definition, we have:

\[
\langle a|f\rangle r_{2}[a := \text{cofix}_{b_{x}}[p]] r_{2}' \leadsto_{\tau} \langle p[V_{i}/x]|b'/b\rangle |\mu a.\langle a|f\rangle r_{2}' | r_{2}'[b' := \lambda y.\text{cofix}_{b_{x}}[p]]
\]

It is straightforward to check, using the induction hypothesis for \(n\), that \((b'|r_{2}[b' := \lambda y.\text{cofix}_{b_{x}}[p]])\) is in \(\forall y. y \in T \rightarrow |F_{A,y}|_{f}\). Thus we deduce by induction hypothesis for \(p\), denoting by \(S\) the function \(t \mapsto |F_{A,t}|_{f}\), that:

\[
(p[V_{i}/x]|b'/b)|r_{2}[b' := \lambda y.\text{cofix}_{b_{x}}[p]]) \in |A[V_{i}/x][S/X]|_{p} = |A[V_{i}/x][F_{A,y}^{n}/X(y)]|_{p} = |F_{A,y}^{n+1}\|
\]

It only remains to show that \((\mu a.\langle a|f\rangle r_{2}' | r_{2})\) is in \(\bigcap_{n \in \mathbb{N}} |F_{A,V}|_{f}\), which is trivial from the hypothesis for \(f\).

We can finally deduce from Propositions 8.14 and 8.22 that dLPA\(^{\omega}\) is normalizable and sound.

**Theorem 8.23** (Normalization). If \(\Gamma \vdash \sigma c\), then \(c\) is normalizable.

**Theorem 8.24** (Consistency). \(\forall d_{LPA^{\omega}} : \perp\)

**Proof.** Assume there is such a proof \(p\), by adequacy \((p|\epsilon)\) is in \(\perp\) for any pole. Yet, the set \(\perp \equiv \emptyset\) is a valid pole, and with this pole, \(\perp\|_{p} = \emptyset\), which is absurd. \(\square\)

### 8.4.2 About the interpretation of coinductive formulas

While our realizability interpretation finally gave us a proof of normalization and soundness for dLPA\(^{\omega}\), it has two aspects that we could find unsatisfactory. First, regarding the small-step reduction system, one could have expected the lowest level of interpretation to be \(\nu\) instead of \(f\). Moreover, if we observe our definition, we notice that most of the cases of || \(\cdot\) ||_{f} are in fact defined by orthogonality to a subset
of strong values. Indeed, except for coinductive formulas, we could indeed have defined instead an interpretation $|\cdot|_v$ of formulas at level $v$ and then the interpretation $\|\cdot\|_f$ by orthogonality:

\[
\begin{align*}
|\bot|_v & \triangleq 0 \\
|t = u|_v & \triangleq \begin{cases} \text{refl} & \text{if } t \equiv u \\ 0 & \text{otherwise} \end{cases} \\
|p \in A|_v & \triangleq \{(v|r) \in |A|_v : v \equiv t p \} \\
|T \rightarrow B|_v & \triangleq \{(\lambda x.p|r) : \forall V \tau' \tau \tau' \cdot (V|\tau) \in |T|_v \Rightarrow (p[V/x]|\tau') \in |B|_v \} \\
|A \rightarrow B|_v & \triangleq \{(\lambda a.p|r) : \forall V \tau' \tau \tau' \cdot (V|\tau) \in |A|_v \Rightarrow (p[\tau\tau'|a := V]) \in |B|_v \} \\
|T \wedge A|_v & \triangleq \{(V|\tau) : (V|\tau) \in |T|_v \wedge (V|\tau) \in |A|_v \} \\
|A_1 \wedge A_2|_v & \triangleq \{(V_1|\tau), (V_2|\tau) : (V_1|\tau) \in |A_1|_v \wedge (V_2|\tau) \in |A_2|_v \} \\
|A_1 \vee A_2|_v & \triangleq \{(i)(V|\tau) : (V|\tau) \in |A_1|_v \} \\
|\exists x.A|_v & \triangleq \bigcup_{t \in A_\tau} [A[t/x]|_v \\
|\forall x.A|_v & \triangleq \bigcap_{t \in A_\tau} [A[t/x]|_v \\
|\forall a.A|_v & \triangleq \bigcap_{p \in A_\tau} [A[p/x]|_v \\
\|A\|_f & \triangleq \{(f|\tau) : \forall \nu \nu' \tau : \tau \circ \tau' \wedge (v|\tau) \in |A|_v \Rightarrow (v|\tau') \parallel (F|\tau) \} \\
\end{align*}
\]

If this definition is somewhat more natural, it poses a problem for the definition of coinductive formulas. Indeed, there is a priori no strong value in the orthogonal of $\|v'_\tau A\|_f$, which is:

\[
(\|v'_\tau A\|_f) \parallel v = \left( \bigcup_{n \in \mathbb{N}} F_{A,\tau,f}^n \right) \parallel v = \bigcap_{n \in \mathbb{N}} (\|F_{A,\tau,f}^n\|_f) \parallel v.
\]

For instance, consider again the case of a stream of type $v'_\tau A(x) \wedge f(S(x)) = 0$, a strong value in the intersection should be in every $|A(0) \wedge (A(1) \wedge \ldots (A(n) \wedge \tau) \ldots)|_v$, which is not possible due to the finiteness of terms.\footnote{Yet, it might possible to consider interpretation with infinite proof terms, the proof of adequacy for proofs and contexts (which are finite) will still work exactly the same. However, another problem will arise for the adequacy of the cofix operator. Indeed, with the interpretation above, we would obtain the inclusion $\bigcup_{n \in \mathbb{N}} (\|F_{A,\tau,f}^n\|_f) \subseteq (\cap_{n \in \mathbb{N}} (\|F_{A,\tau,f}^n\|_f) \parallel f) = \|v'_\tau A\|_f$ which is strict in general. By orthogonality, this gives us that $\|v'_\tau A\|_v \subseteq \bigcup_{n \in \mathbb{N}} (\|F_{A,\tau,f}^n\|_f) \parallel v$, while the proof of adequacy only proves that $(a|\tau[a := \text{cofix}_I^{|v|}(x|p)])$ belongs to the latter set.}

Thus the definition $|v'_\tau A|_v \triangleq \bigcap_{n \in \mathbb{N}} |F_{A,\tau,f}^n|_v$ would give $|v'_\tau A|_v = 0 = \bot|_v$.

Interestingly, and this is the second case that we do not find completely satisfactory, we could have define instead the truth value of coinductive formulas directly by:

\[
|v'_\tau A|_v \triangleq |A[t/x]|[v'_{\tau X} A/f(y) = 0]|_v.
\]

Let us sketch the proof that such a definition is well-founded. We consider the language of formulas without coinductive formulas and extended with formulas of the shape $X(t)$ where $X, Y, \ldots$ are parameters. At level $v$, closed formulas are interpreted by sets of strong values-in-store $(v|\tau)$, and as parameters. These sets are besides closed under the relation $\equiv_t$ along their component $\tau$. If $A(x)$ is a formula whose only free variable is $x$, the function which associates to each term $t$ the set $|A(t)|_v$ is thus a function from $\Lambda_t$ to $\mathcal{P}(\Lambda^*_v)$, let us denote the set of these functions by $\mathcal{L}^*_v$.

**Proposition 8.25.** The set $\mathcal{L}^*_v$ is a complete lattice with respect to the order $\leq_{\mathcal{D}}$ defined by:

\[
F \leq_{\mathcal{D}} G \triangleq \forall t \in \Lambda_f, F(t) \subseteq G(t)
\]

**Proof.** Trivial since the order on functions is defined pointwise and the co-domain $\mathcal{P}(\Lambda^*_v)$ is itself a complete lattice. \(\square\)
We define valuations, which we write $\rho$, as functions mapping each parameter $X$ to a function $\rho(X) \in \mathcal{L}$. We then define the interpretations $|A|^\rho_x, |A|^\rho_f, \ldots$ of formulas with parameters exactly as above with the additional rule\footnote{Observe that this rule is exactly the same as in the previous section (see Figure 8.8).}

$$|X(t)|^\rho_x \triangleq \{(x, t) \in \rho(X)(t)\}$$

Let us fix a formula $A$ which has one free variable $x$ and a parameter $X$ such that sub-formulas of the shape $X t$ only occur in positive positions in $A$.

**Lemma 8.26.** Let $B(x)$ is a formula without parameters whose only free variable is $x$, and let $\rho$ be a valuation which maps $X$ to the function $t \mapsto |B(t)|_\nu$. Then $|A|^\rho_x = |A[B(t)/X(t)]|_\nu$.

**Proof.** By induction on the structure of $A$, all cases are trivial, and this is true for the basic case $A \equiv X(t)$:

$$|X(t)|^\rho_x = \rho(X)(t) = |B(t)|_\nu$$

Let us now define $\varphi_A$ as the following function:

$$\varphi_A : \begin{cases} \mathcal{L} & \rightarrow & \mathcal{L} \\ F & \mapsto & t \mapsto |A[t/x]|_\nu^{[X\mapsto F]} \end{cases}$$

**Proposition 8.27.** The function $\varphi_A$ is monotone.

**Proof.** By induction on the structure of $A$, where $X$ can only occur in positive positions. The case $|X(t)|_\nu$ is trivial, and it is easy to check that truth values are monotonic with respect to the interpretation of formulas in positive positions, while falsity values are anti-monotonic. \hfill $\Box$

We can thus apply Knaster-Tarski theorem to $\varphi_A$, and we denote by $gfp(\varphi_A)$ its greatest fixpoint. We can now define:

$$|v^f_{X,y}A|_\nu \triangleq gfp(\varphi_A)(t)$$

This definition satisfies the expected equality:

**Proposition 8.28.** We have:

$$|v^f_{X,y}A|_\nu = |A[t/x][v^y_{X,y}A/X(y)]|_\nu$$

**Proof.** Observe first that by definition, the formula $B(z) = |v^z_{X,y}A|_\nu$ satisfies the hypotheses of Lemma 8.26 and that $gfp(\varphi_A) = t \mapsto B(t)$. Then we can deduce:

$$|v^f_{X,y}A|_\nu = gfp(\varphi_A)(t) = \varphi_A(gfp(\varphi_A))(t) = |A[t/x]|_\nu^{[X\mapsto gfp(\varphi_A)]} = |A[t/x][v^y_{X,y}A/X(y)]|_\nu$$

Back to the original language, it only remains to define $|v^f_xA|_\nu$, as the set $|v^f_xA[X(y)/f(y) = 0]|_\nu$, that we just defined. This concludes our proof that the interpretation of coinductive formulas through the equation in Proposition 8.28 is well-founded.

We could also have done the same reasoning with the interpretation from the previous section, by defining $\mathcal{L}$ as the set of functions from $A_f$ to $\mathcal{P}(A^\rho_f)_e$. The function $\varphi_A$, which is again monotonic, is then:

$$\varphi_A : \begin{cases} \mathcal{L} & \rightarrow & \mathcal{L} \\ F & \mapsto & t \mapsto |A[t/x]|_\nu^{[X\mapsto F]} \end{cases}$$
8.5. CONCLUSION AND PERSPECTIVES

We recognize here the definition of the formula $F^n_{A,t}$. Defining $f^0$ as the function $t \mapsto \|T\|_f$ and $F^{n+1} \triangleq \varphi_A(f^n)$ we have:

$$\forall n \in \mathbb{N}, \|F^n_{A,t}\|_f = f^n(t) = \varphi^n_A(f^0)(t)$$

However, in both cases (defining primitively the interpretation at level $v$ or $f$), this definition does not allow us to prove the adequacy of the (cofix) rule. In the case of an interpretation defined at level $f$, the best that we can do is to show that for any $n \in \mathbb{N}$, $f^n$ is a post-fixpoint since for any term $t$, we have:

$$f^n(t) = \|F^n_{A,t}\|_f \subseteq \|F^{n+1}_{A,t}\|_f = f^{n+1}(t) = \varphi_A(f^n)(t)$$

With $\|v_{f,x}^A\|_f$ defined as the greatest fixpoint of $\varphi_A$, for any term $t$ and any $n \in \mathbb{N}$ we have the inclusion $f^n(t) \subseteq \text{gfp}(\varphi_A)(t) = \|v_{f,x}^A\|_f$ and thus:

$$\bigcup_{n \in \mathbb{N}} \|F^n_{A,t}\|_f = \bigcup_{n \in \mathbb{N}} f^n(t) \subseteq \|v_{f,x}^A\|_f$$

By orthogonality, we get:

$$\|v_{f,x}^A\|_f \subseteq \bigcap_{n \in \mathbb{N}} \|F^n_{A,t}\|_f$$

and thus our proof of adequacy from the last section is not enough to conclude that $\text{cofix}_{X_{k,x}[p]}^t \subseteq \|v_{f,x}^A\|_f$. For this, we would need to prove that the inclusion is an equality. An alternative to this would be to show that the function $t \mapsto \bigcup_{n \in \mathbb{N}} \|F^n_{A,t}\|_f$ is a fixpoint for $\varphi_A$. In that case, we could stick to this definition and happily conclude that it satisfies the equation:

$$\|v_{f,x}^A\|_f = \|A[t/x][v_{f,x}^A/X(y)]\|_f$$

This would be the case if the function $\varphi_A$ was Scott-continuous on $\mathcal{L}$ (which is a dcpo), since we could then apply Kleene fixed-point theorem to prove that $t \mapsto \bigcup_{n \in \mathbb{N}} \|F^n_{A,t}\|_f$ is the stationary limit of $\varphi^n_A(f_0)$. However, $\varphi_A$ is not Scott-continuous (the definition of falsity values involves double-orthogonal sets which do not preserve supremums), and this does not apply.

8.5 Conclusion and perspectives

Recap of the journey  In the end, we met our main objective, namely proving the soundness and the normalization of a language which includes proof terms for dependent and countable choice in a classical setting. This language, which we called dLPA$^\omega$, provides us with the same computational features as dPA$^\omega$ but in a sequent-calculus fashion. The calculus indeed includes co-fixpoint operators, which are lazily evaluated. To this end, dLPA$^\omega$ uses the design of the $\lambda_{(\forall\tau\star)}$-calculus of Ariola et al. [4], which we equipped in Chapter 6 with a type system and which we proved to be normalizing. In addition, the proof terms of dLPA$^\omega$ are dependently typed thanks to a restriction of dependencies to the negative-elimination-free fragment which makes them compatible with classical logic. These computational features allow dLPA$^\omega$ to internalize the realizability approach of [15, 40] as a direct proofs-as-programs interpretation: both proof terms for countable and dependent choices furnish a

---

14 To be honest, we should rather say that we could not manage to find a proof, and that we would welcome any suggestion from insightful readers.

15 In fact, Cousot and Cousot proved a constructive version of Kleene fixed-point theorem which states that without any continuity requirement, the transfinite sequence $(\varphi^n_A(f^0))_{n \in \Omega_A}$ is stationary [39]. Yet, we doubt that the gain of the desired equality is worth a transfinite definition of the realizability interpretation.

16 In fact, this is nonetheless a good news about our interpretation. Indeed, it is well-known that the more “regular” a model is, the less interesting it is. For instance, Streicher showed that the realizability model induced by Scott domains (using it as a realizability structure) was not only a forcing model by also equivalent to the ground model.
lazy witness for the ideal choice function which is evaluated on demand. At the risk of repeating
ourselves, this interpretation is in line with the slogan that with new programing principles—here the
lazy evaluation and the co-inductive objects—come new reasoning principles—here the axioms \( AC \)
and \( DC \).

In our search for a proof of normalization for \( dLPA^{\omega} \), we developed novel tools to study these side-
effects and dependent types in presence of classical logic. On the one hand, we set out in Chapter 7 the
difficulties related to the definition of a sequent calculus with dependent types. We proposed a formal-
ism, \( dL^{\hat{t}ate} \), which restricts the dependencies to proofs in the \( nsc/e.sc/fs \) fragment together. This restriction is
strengthened with an evaluation of dependently typed computations within delimited continuations;
while the type system is enriched with an explicit list of dependencies. This provides us with a calculus
whose reduction is safe, and which has the advantage of being suitable for a typed continuation-passing
style translation carrying the dependencies.

On the other hand, we defined a typed continuation-and-store passing style translation for the \( \lambda c[\tau.alt]\star \)-calculus, which we related to Kripke forcing semantics. Besides, we saw how to handle laziness
and explicit stores in a realizability interpretation \( \text{à la} \) Krivine. This might be a first step toward new
interpretations of different axioms using laziness within Krivine classical realizability. In a long term
perspective, it would be interesting to understand the impact of laziness and stores on the corresponding
realizability algebras. More generally, the algebraic models that we study in the last part of this thesis
are oriented toward the call-by-name and the call-by-value evaluation strategies. While it is probably
the case that these structures could be modified to obtain call-by-need algebras, the structure of such
algebras is not obvious \( a \ priori \).

Comparison with Krivine’s interpretations of dependent choice  At the end of the day, we pre-
sented a calculus, \( dLPA^{\omega} \), with the nice property of allowing for the direct definition of a proof term for
the axiom of dependent choice. Beside, we prove the normalization and soundness of \( dLPA^{\omega} \) by means
of a realizability interpretation \( \text{à la} \) Krivine. Yet, the computational content we give to the axiom of
dependent choice is pretty different of Krivine’s usual realizer of the same \( [94] \). Indeed, our proof uses
dependent types to get witnesses of existential formulas, and represents the choice function through
the lazily evaluated stream of its values. In turn, Krivine realizes a statement which is logically equiv-
alent to the axiom of dependent choice thanks to the instruction \( \text{quote} \), which injectively associates a
natural number to each closed \( \lambda c \)-term. In particular, such an instruction allows to compare the codes
of two programs, so that terms of the \( \lambda c \)-calculus extended with \( \text{quote} \) can reduce differently according
to the code of the arguments they are given. In a more recent work \( [102] \), Krivine proposes a realiz-
ability model which has a bar-recursor and where the axiom of dependent choice is realized using the
bar-recursion. This realizability model satisfies the continuum hypothesis and many more properties,
in particular the real numbers have the same properties as in the ground model. However, the very
structure of this model, where \( \Lambda \) is of cardinal \( \aleph_1 \) (in particular infinite streams of integer are terms),
makes it incompatible with the instruction \( \text{quote} \).

It is clear that the three approaches are different in terms of programming languages. Nonetheless,
it could be interesting to compare them from the point of view of the realizability models they give rise
to. We did not study at all this question for \( dLPA^{\omega} \), especially we do not know whether it is suitable
to define the same model of \( ZF + \neg AC + \neg CH \) (set theory with the negation of the axiom of choice
and the negation of continuum hypothesis). Neither do we know if the induced model is compatible
with the \( \text{quote} \) instruction (we conjecture that it is). It might be the case that our approach can be
related with the one with a bar-recursor in \( [102] \). In particular, our analysis of the interpretation of
co-inductive formulas may suggest that the interest of lazy co-fixpoints is precisely to approximate the
limit situation where \( \Lambda \) has infinite objects.

The study of the structures of Krivine realizability models is already a hard question, and so is in
general the problem of determining the consequences that a particular set of instructions or a specific

228
pole might have on on the model\textsuperscript{17}. Nonetheless, the question still holds.

**Reduction of the consistency of classical arithmetic in finite types with dependent choice to the consistency of second-order arithmetic**  
The standard approach to the computational content of classical dependent choice in the classical arithmetic in finite types is via realizability as initiated by Spector \cite{Spector1960} in the context of Gödel’s functional interpretation, and later adapted to the context of modified realizability by Berardi et al \cite{Berardi1997}. In the different settings of second-order arithmetic \cite{Simpson1986} and classical realizability, Krivine \cite{Krivine1993} gives a realization of a formulation of dependent choice over sets of numbers using side-effects (a clock or a quote operator).

In all these approaches, the correctness of the realizer, which implies consistency of the system, is itself justified by a use at the meta-level of a principle classically equivalent to dependent choice (dependent choice itself in Krivine, bar induction or update induction \cite{Krivine1994} in the case of Spector or Berardi et al).

Our approach is here different. Not only we directly interpret proofs of dependent choice in classical arithmetic computationally but we propose a path to a computational reduction of the consistency of classical arithmetic in finite types ($\text{PA}_\omega$) to the one of the target language $F_\Upsilon$. This system is an extension of system $F$, but it is not clear whether its consistency is conservative of not over system $F$. Ultimately, we would be interested in a computational reduction of the consistency of $\text{dPA}_\omega$ or $\text{dLPA}_\omega$ to the one of $\text{PA}_2$, that is to the consistency of second-order arithmetic. While it is well-known that $\text{DC}$ is conservative over second-order arithmetic with full comprehension (see \cite[Theorem VII.6.20]{Simpson1986}), it would nevertheless be very interesting to have such a direct computational reduction. The converse direction has been recently studied by Valentin Blot, who presented in \cite{Blot2018} a translation of System F into a simply-typed total language with a variant of bar recursion.

\textsuperscript{17}To quote the last PhD student in date who attempted to define purpose-oriented realizability models \cite{Blot2018}, they are like Forrest’s Gump chocolates boxes, “you never know what you’re gonna get”.

229
CHAPTER 8. A SEQUENT CALCULUS WITH DEPENDENT TYPES FOR CLASSICAL ARITHMETIC