

### ### contents

The paper lives up to its name. It gives a full axiomatic account of a gradual type theory (GTT) based on CBPV along with the strongest possible metatheory based on observational equivalence. The main thrust of the work is that gradual typing should enable type-based equational reasoning, in particular it should obey beta and eta rules for all type constructors. The authors show that from this starting point and an abstract specification of upcasts and downcasts most of the equational theory falls into place.

Any particular implementation of GTT needs to fix the behavior of certain downcasts. The authors show with examples that there is some design space for creating concrete implementations of GTT. They give examples for a CBV calculus and for a calculus inspired by Lisp/Scheme, which rely on different representation types.

### ### evaluation

I'm probably forgetting some of the contributions as the paper really contains a wealth of material and results of high quality. That said, the writing and presentation style does not always reach the quality of the material. The writing is often clipped and the presentation abridged. In some places the reader is drowned in unnecessary (trivial) details, in other places the reader is overwhelmed with background information that is not strictly necessary to follow the paper.

My recommendation is to definitely publish this paper, but before that there are lots of smallish details to be fixed which are listed below in the detailed comments. On a larger scale there are two bigger changes that would make the paper much more accessible (and here I assume that many readers will stop after the introduction):

1. give an accessible high-level overview of the results as part of the introduction; it is way too compressed as it stands in the submission
2. (for the brave readers that carry on) include a couple of worked out examples in the text, rather than just compressed remarks in the running text.
3. move trivial details into an appendix. In particular, full page figures of congruence rules where one feels obliged to check if anything happens.

### ### gripes

the citation format is confusing, but should be fixable by using a different macro.

theorems and corollaries have one global numbering, whereas lemmas are numbered by chapter. This should be unified.

the text is often very (too) short and clipped. An archival publication requires more care

than that.

for the sake of the future readers, it would be good to make the summary in section 1 more accessible. Rather than just presenting a compressed list of contributions, it would be better to give a high-level overview with enough detail so as not to require readers to delve into all the details. Those interested in detail should/will read on.

Some examples are discussed superficially in the running text. It would be nice to have a few worked out examples.

# detailed comments

## abstract *\*type-based reasoning is preserved\**, *\*gradual type soundness\**

It is not quite clear to this reviewer what exactly is meant with type-based reasoning. It refers to type soundness, but do we expect more from (syntactic) type soundness than Milner's slogan well-typed programs do not go wrong?

The second phrase is also undefined IMHO. I took it to mean *\*type soundness for gradual types\**.

It would be good to express more precisely what you want in the abstract, without recourse to yet-to-be-defined notions.

## page 4, -8 *\*(in CBN...)\**

This remark felt cryptic to me on the first reading and the reference to CBN felt wrong. Then I realized that the intention was to say that the condition  $x$  would be a thunk in CBN and thus be able not to terminate or cause an effect. This could be stated more clearly.

## page 5, after line 4

Wondering what can be said about call-by-need? If anything?

## page 5, 10

*\*error\** is not a verb, so *\*erroring\** and *\*do not error\** (line -12) is grammatically incorrect.  
*\*error\** -> *\*err\**

## page 5, 12

*\*high-level syntax\** can you elaborate? example?

## page 6, 11

*\*pattern, match\** -> *\*pattern match\**  
*\*This\** without a referent is confusing.

## page 7

what is \*approximational reasoning\*?

\* line -7: at this point, \*complex values\* and \*complex stacks\* are unclear.

## page 8, -6

\*We prove many theorems...\* Please be more specific. Just identify the main theorems. You want to the reader an incentive...

## page 9, section 2.1

The purpose of this section not quite clear to me. It's supposed to introduce the syntax and some typing rules of GTT. Apparently, it's also supposed to serve as an introduction to CBPV. I think it's overloaded as it is conceived. It contains too much information for a specialist in CBPV. At the same time, it contains too little information (and sometimes too much) for someone not familiar

with CBPV. It also seems that many of the properties mentioned in this section are not exploited later in the paper (for instance, the references to focusing which are insightful, but not leading anywhere). To conclude, it would be good to have a section here that is targeted to an audience that

are not CBPV experts, but which nevertheless presents only the properties needed to understand the rest of the paper.

For those, it would be good to explain the philosophy of CBPV in general terms and maybe highlight the differences to notions familiar to a larger audience (e.g. monads).

## page 10

\*In focusing terminology...\*

This is an interesting remark, but probably underappreciated by readers unfamiliar with focusing.

\*thinkability\*

explain here or drop. This section is about background, not your results.

## page 12

\*running a function\* @14: counter(my) intuition. does it matter for the message of the paper?

\*considered equal\* @18: which judgment implies this equality? again, does it matter for this paper?

typo @-21: \*class [of] terms\*

\*focusing\* @-10: see above

## page 13

the two paragraphs, on embedding and on extensionality, are fairly compressed. I think a table would be more accessible.

@-1 \*we find that having both... most natural\*

That is not a technical argument, but an esthetical(?). Can you give it a convincing basis? Why can't you make do with just one dynamic type and use F or U to mediate? If this is not viable, why?

##page 14

@-13: what is the difference between  $U( ? \rightarrow F? )$  and  $U( ? \rightarrow \iota )$

##page 16

1st paragraph: is this explaining a design choice or is this informal reasoning that is a consequence of previous choices?

##page 17

@-1: should be A equiprecise A'

It should be said upfront that your precision relation includes the conversion rules. This is notable, because it is different than in other work.

##page 18

These (congruence) rules are really boring and should be moved to an appendix, perhaps giving one example in the main text.

(If I missed any interesting rule, please highlight that!)

##page 19

@17:  $F1+1 \rightarrow F(1+1)$

##page 21, lemma 3.2

In UpL, it seems like A' needs some upper bound in the assumption.

In DnL, B' needs a lower bound, and the typing should be  $B \sqsubseteq B'$ .

##page 22, def 2

This looks to me like the map of the functors F and U, resp.

@15-16: \*behaviorally equivalent\*

It should be made clear that this is the program of the upcoming subsection.

#page 23, thm 4

item 1: blob: FA  $\rightarrow$  blob: FA' (2x)

#page 24

@-10: there is an inline-example here that should be worked out in more detail: the example should demonstrate the two ways of casting  $A1 \times A2 \rightarrow B$

@-1: last cast should be  $\llbracket UB \searrow swarrow UB \rrbracket$  (double brackets)  
(if you don't wish to make this distinction, you should say this explicitly)

##page 25, def 3

This definition is pretty sloppy and could be made more formal by using the notation  $C[X_i, Y_j]$  introduced below.

Right after the definition (or along with it), I would define the instantiation and abbreviation used in line @-3.

This could be used to make the statement of lemma 3.4 more formal; the actual proof is trivial.

@-10: it's confusing to use the same  $i$  to range over independent ranges.  
I'm not sure why this is called a \*complex value\*. According to def 2, it should be a stack.

Same at @-2

#page 26

@3: not a complex value according to 2.1

##page 27

@-8: the  $\llbracket \cdot \rrbracket$  notation is only defined for types of the form  $UB$ , so what is this supposed to mean? It looks ok in principle, but I'm confused by the notation (which seems to be used inconsistently)

#page 28

@4, @5 more of the same confusion

#page 29

@-6 \*taking having\* ?

#page 30

@2 first line doesn't make sense

@12: equiprecision for  $*:B \dashv\dashv S[S'/*]$  (not  $x'$ )

@-11:  $UB \times 1 = A \dashv\dashv$  no clear what you refer to

@-8:  $\text{cons} \dashv\dashv$  pair

#page 32

@5  $\vdash$  is missing (first formula)

@7 what's the meaning of the notation on lhs of equiprecision?

@16: y is missing before ":"

@Thm 12: assumptions on z and \* are missing

#page 33

@-18 don't --> do not

@-4 \*almost every reduction\* fuzzy

##page 34

@1: \*split to\* syntax is garbled

@4: don't you need  $A \sqsubseteq G$  to avoid looping reduction in DecompUp and DecompDn?

Silly has been called Stupid elsewhere (Featherweight Java)

@-10 \*note finally that\* why is that? explain!

##page 35

at end of 4.2: you've given a CBV translation. How about a CBN translation? Would it be interesting to derive? What other variations might be contemplated?

##page 36

@3 standard for observational equivalence is F1, why do you choose  $F(1+1)$ ?

@6 \*any valid interpretation\* did we define that already?

#page 37

@7 recursive -> isorecursive

@13 Figure 11 should be called out before discussion. \*diff\* is not an English word.

@22,23: \*embedded models upcast\*, \*projection models downcast\*  
but this is true in both, value and computation types? why this strange formulation?

@Def 5.1 Assumption  $A \sqsubseteq A'$  missing?

@-5 \*properties are often occur more naturally\* --> garbled

@-3 looks like the definition of a Galois connection to me. what's the relation?

##page 41

@fig 12 is not called out from the text and not explained, either.

I don't quite understand the notation for  $\eta$  (last line).

Shouldn't the case for 1 be like this:

$x_1 . E[< \eta \nwarrow 1 > x_1 / x]$

and analogous for the remaining three cases?

You are also abbreviating  $\eta x$  to  $x$  etc, which is left unexplained.

The notation for the  $\zeta$  cases is really cryptic on first reading (for the choice of behaviors). Unacceptable without explanation.

##page 42

@lemma 5.5:  $V[V/x] \rightarrow V'[V/x]$ , and  $\text{ret } V' \rightarrow \text{ret } V$

@Definition 10

How can a definition come with a proof? You need to formulate a separate lemma.

@-2 \*variable-arity\*

even after reading what follows, it's not quite Scheme-ish as your formal framework talks about curried functions whereas Scheme's functions are curried - at least the ones that go with the dot notation mentioned a little later.

##page 43

@-6 \*type is isomorphic\*

I can see this. But can you write down this iso? Does it have a term representation?

#page 44

@fig 13, rule  $\eta$

$< \eta \nwarrow B >$  is not an expression  $\rightarrow < \eta \nwarrow B > x_B / x$

similarly for  $x$  and  $U$

@-8 this is the mention of the dot args stuff referred to

##page 46

\*tediously explicit definition\*

it seems that some  $[[ \_ ]]$  are missing in the definition:

@7:  $[[ E_t ]]$ ,  $[[ E_f ]]$

It would be better to have it in a figure with an explicit reference to the rest of the definition.

@16 this seems to be the first time that you refer to a dynamic type interpretation by

some  $\rho$ . In definition 7 and 10, a DTI was introduced as an isomorphism. Definition 6 (of DTI) speaks of  $\rho$ , but no such  $\rho$  was explicitly given in defs 7 and 10. Here you are referring to  $\rho$  and in fig 14 to  $\rho_{\text{up}}$  and  $\rho_{\text{dn}}$ , which was never defined.

## page 47, fig 14

- \* in several places (e.g., for  $A_1 + A_2$  and  $A_1 \times A_2$ ), the typing of the assumption for  $x$  or  $\bullet$  are missing.
- \* @8 cast factoring uses the notation  $\lfloor A \rfloor$  which is not defined (but should produce the ground type underlying  $A$ ). This line of the definition is not necessarily terminating because  $\lfloor ? \times ? \rfloor = ? \times ?$
- \* @15 rhs of case for  $F_1$  should be  $\bullet$
- \* @12, @17 inconsistent notation: in @12  $[x_2/x]$  vs @17  $[x_2]$  + some more cases like that
- \* @26/27 is it correct that the same  $\rho$  as in @6/7 works here ?  
This would imply that  $\iota \cong F?$  and  $UG \cong G \dots$

## page 51, @-3

Could you informally explain the imposed restrictions?

##page 52, fig 17

Not called out in the text. Nothing happens in this figure and it should be relegated to an appendix with the clear statement that it's completely unsurprising.

@-6 "but not does not" -> "but does not"

##page 53, fig 18 and 19

Not called out in the text. Could you not move the obvious rules (or the ones that we've seen before) in an appendix and only highlight the ones that matter at this point?  
I think it would boil down to the  $\beta\eta$  rules for  $\mu$  and  $\nu$  types.

##page 54, def 11

Badly phrased. "We define  $E^\dagger = E'$  inductively by the equations give in figure ..." And move the equations into a figure. Very straightforward, perhaps a few exemplary cases suffice if space is scarce?  
In the lines for unit and pair, on rhs:  $V \dashrightarrow V^\dagger$

@-1: I suggest to define thunkability first, and then discuss that translated complex values satisfy it. It's obvious after the reader has seen the definition and thus easier to follow.

##page 55

@9 can you reformulate this sentence:

"linear in x if M behaves as if when it is forced, the first thing it does is forces x ,  
and the is the only time it uses x"

I don't think it's incorrect, but it would be more accessible if untangled.

@-12 "Furhmann" --> "Führmann" (as in the reference, \citet could help if it would work in the jfp bib style)

##page 57, fig 20

which definition of S is used here?

##page 58

@2 "for the step-indexed logical relation later"

That's super terse! Please elaborate and expand to 1-2 proper sentences.

@3 "only defined for terms of type  $F(1+1)$ "

That doesn't seem to be right.

Unless you are alluding to fig 20 such that S is always the evaluation context to the toplevel.

Is everything consistent with that assumption?

@27 the wording suggests that you are defining  $\text{result}(M)$  in terms of  $\text{result}(M)$ .

The clean way would be to define it by cases on the possible outcomes in Corollary 4.

##page 59, def 16

Why is this a definition? It is formulated like a lemma and thus requires a (admittedly trivial) proof.

##page 60

@-12-(-8)

It would help the reader to spell out the meanings of each of these relations.

Lemma 7.4 gives a helpful characterization; could it not serve as a definition?

##page 61, corollary 5.3

The relation  $\leq \equiv$  appears in fig 22, but not in lemma 7.4.

Is there something missing?

##page 63, fig 23

I got confused because the right header belongs to the second block of equations.

Perhaps some clarification is in order that the two definitions are mutually recursive.

@discussion ending with "Nakano's later modality"

Does that mean it is actually easier to define the logical relation for CBPV than it would be for either CBV or CBN?

