Modular, Higher-Order Cardinality Analysis in Theory and Practice

Extended version

Ilya Sergey
IMDEA Software Institute
ilya.sergey@imdea.org

Dimitrios Vytiniotis Simon Peyton Jones
Microsoft Research
{dimitris,simonpj}@microsoft.com

Abstract
Since the mid ‘80s, compiler writers for functional languages (especially lazy ones) have been writing papers about identifying and exploiting thunks and lambdas that are used only once. However it has proved difficult to achieve both power and simplicity in practice. We describe a new, modular analysis for a higher-order language, which is both simple and effective, and present measurements of its use in a full-scale, state of the art optimising compiler. The analysis finds many single-entry thunks and one-shot lambdas and enables a number of program optimisations.

Categories and Subject Descriptors D.1.1 [Programming Techniques]: Applicative (Functional) Programming; F.3.2 [Logics and Meanings of Programs]: Semantics of Programming Languages — Program analysis, Operational semantics

Keywords compilers, program optimisation, static analysis, functional programming languages, Haskell, lazy evaluation, thunks, cardinality analysis, types and effects, operational semantics

1. Introduction
Consider these definitions, written in a purely functional language like Haskell:

\[
\begin{align*}
\text{wurble1}, \text{wurble2} & : (\text{Int} \to \text{Int}) \to \text{Int} \\
wurble1 \ k & = \text{sum} (\text{map} \ k \ [1..10]) \\
wurble2 \ k & = \ 2 \ * \ k \ 0
\end{align*}
\]

\[
\begin{align*}
f1 & : [\text{Int}] \to \text{Int} \\
f1 \ xs & = \text{let} \ ys = \text{map} \ \text{costly} \ xs \ \\
& \quad \quad \text{in} \ \text{wurble} \ \langle \text{n. sum (map (+ n) ys)} \rangle
\end{align*}
\]

Here we assume that costly is some function that is expensive to compute and \(\text{wurble}1\) is either \(\text{wurble1}\) or \(\text{wurble2}\). If we replace \(\text{ys}\) by its definition, we could transform \(f1\) into \(f2\):

\[
\begin{align*}
f2 \ xs & = \text{wurble} \ \langle \text{n. sum (map (+ n) (map costly xs))} \rangle
\end{align*}
\]

A compiler like GHC can now use short-cut deforestation to fuse the two maps into one, eliminating the intermediate list altogether, and offering a substantial performance win (Gill et al. 1993).

Does this transformation make the program run faster or slower? It depends on \(\text{wurble}\)! For example, \(\text{wurble1}\) calls its function argument ten times, so if \(\text{wurble} = \text{wurble1}\), function \(f2\) would compute \(\text{costly}\) ten times for each element of \(\text{xs}\); whereas \(f1\) would do so only once. On the other hand if \(\text{wurble} = \text{wurble2}\), which calls its argument exactly once, then \(f2\) is just as efficient as \(f1\), and \(\text{map/map}\) fusion can improve it further.

The reverse is also true. If the programmer writes \(f2\) in the first place, the full laziness transformation (Peyton Jones et al. 1996) will float the sub-expression (\(\text{map costly xs}\)) out of the \(\langle\text{\_\_}\rangle\) expression, so that it can be shared. That would be good for \(\text{wurble1}\) but bad for \(\text{wurble2}\).

What is needed is an analysis that can provide a sound approximation of how often a function is called — we refer to such an analysis as a cardinality analysis. An optimising compiler can then use the results of the analysis to guide its transformations. In this paper we provide just such an analysis:

1. We characterise two different, useful forms of cardinality, namely (a) how often a function is called, and (b) how often a thunk is forced in a lazy language (Section 2). Of these, the former is relevant under both call-by-need and call-by-value, while the latter is specific to call-by-need.
2. We present a backwards analysis that can soundly and efficiently approximate both forms of cardinality for a non-strict, higher-order language (Section 3). A significant innovation is our use of call demands to model the usage of a function; this makes the analysis both powerful and modular.
3. We prove that our algorithm is sound; for example if it claims that a function is called at most once, then it really is (Section 4). This proof is not at all straightforward, because it must take account of sharing — that is the whole point! So we cannot use standard denotational techniques, but instead must use an operational semantics that models sharing explicitly.
4. We formalise a number of program optimisations enabled by the results of the cardinality analysis, prove them sound and, what is more important, improving (Section 5).
5. We have implemented our algorithm by extending the Glasgow Haskell Compiler (GHC), a state of the art optimising compiler for Haskell. Happily, the implementation builds directly on GHC’s current strictness and absence analyser, and is both simple and efficient (Section 5).
6. We measured how often the analysis finds called-once functions and used-once thunks (Section 7); and how much this knowledge improved the performance of real programs (Sections 7.1, 7.2). The analysis proves quite effective in that many one-shot lambdas and single-entry thunks are detected (in the range 0-30%, depending on the program). Improvements in per-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

POPL ’14, January 22–24, 2014, San Diego, CA, USA.
Copyright © 2014 ACM 978-1-4503-2544-8/14/01…$15.00.
http://dx.doi.org/10.1145/2535838.2535861
performance are modest but consistent (a few percent); programs already optimised by GHC are a challenging target!

We discuss related work in Section 8. Distinctive features of our work are (a) the notion of call demands, (b) a full implementation measured against a state of the art optimising compiler, and (c) the combination of simplicity with worthwhile performance improvements.

2. What is Cardinality Analysis?

Cardinality analysis answers three inter-related questions, in the setting of a non-strict, pure functional language like Haskell:

- How many times is a particular, syntactic lambda-expression called (Section 2.1)?
- Which components of a data structure are never evaluated; that is, are absent (Section 2.4)?
- How many times is a particular, syntactic thunk evaluated (Section 2.3)?

2.1 Call cardinality

We saw in the introduction an example where it is helpful to know when a function calls its argument at most once. A lambda that is called at most once is called a one-shot lambda, and they are extremely common in functional programming: for example a continuation is usually one-shot. So cardinality analysis can be a big win when optimising continuation-heavy programs.

Nor is that all. As we saw in the Introduction, inlining under a one-shot lambda (to transform \(f1\) into \(f2\)) allows short-cut deforestation to fuse two otherwise-separate calls of map. But short-cut deforestation itself introduces many calls of of the function build:

\[
\text{build} :: (\forall b. (a \to b \to b) \to b \to b) \to [a] \\
\text{build } g = g [\cdot] 
\]

You can see that build calls its argument exactly once, and inlining \(y\)s in calls like (build \([\cdot] \ldots y\ldots\)) turns out to be crucial to making short-cut deforestation work in practice. Gill devotes a section of his thesis to elucidating this point (\cite{Gill1996} Chapter 4.3). Gill lacked an analysis for one-shot lambdas, so his implementation (still extant in GHC today) relies on a gross hack: he taught GHC's optimiser to behave specially for build itself, and a couple of other functions. No user-defined function will have this good behaviour. Our analysis subsumes the hack, by providing an analysis that deduces the correct one-shot information for build, as well as many other functions.

2.2 Currying

In a higher order language with curried functions, we need to be careful about the details. For example, consider:

\[
f3 \; a = \text{wurble} \; a \; (\lambda x. \text{let t = costly x in } \lambda y. \; t + y) \\
\text{wurble1} \; g = g \; 2 \; a + \; 3 \; a \\
\text{wurble2} \; g = \text{sum} \; (\lambda a. \; [1 \ldots 1000])
\]

If wurble was wurble1, then in f3 it would be best to inline t at its use site, thus:

\[
f4 \; a = \text{wurble1} \; a \; (\lambda x. \; \lambda y. \text{costly x + y})
\]

The transformed f4 is much better than f3: it avoids allocating a thunk for t, and avoids allocating a function closure for the \(y\). But if f3 called wurble2 instead, such a transformation would be disastrous. Why? Because wurble2 applies its argument g to one argument a, and the function thus computed is applied to each of 1000 integers. In f3 we will compute \(\text{costly a}\) once, but f4 will compute it 1000 times, which is arbitrarily bad.

So our analysis of wurble2 must be able to report “wurble2’s argument g is called once (applied to one argument), and the result is called many times”. We formalise this by giving a usage signature to wurble, like this:

\[
\text{wurble1} :: U \to C^\omega (C^\omega (U)) \\
\text{wurble2} :: U \to C^\omega (C^\omega (U))
\]

The notation \(C^\omega (C^\omega (U))\) is a usage demand: it describes how a (function) value is used. The demand type \(U \to C^\omega (C^\omega (U))\) describes how a function uses its arguments, therefore it gives a usage demand for each argument. (The \(\cdot\) has no significance; we are just using to seeing something after the final arrow!) Informally, the \(C^\omega (d)\) means “this argument is called once (applied to one argument), and the result is used with usage \(d\)”, whereas \(C^\omega (d)\) means “this argument may be called many times, with each result used with usage \(d\)”. The \(U\) means “is used in some unknown way (or even not used at all)”. Note that wurble1’s second argument usage is \(C^\omega (C^\omega (U))\), not \(C^\omega (C^\omega (U))\); that is, in all cases the result of applying g to one argument is then called only once.

2.3 Absence

Consider this function

\[
f \; x = \text{case } x \; \text{of } (p, q) -> <\text{fbody}>
\]

A strictness analyser can see that \(f\) is strict in \(x\), and so can use call-by-value. Moreover, rather than allocate a pair that is passed to \(f\), which immediately takes it apart, GHC uses a worker/wrapper transformation to pass the pieces separately, thus:

\[
f \; x = \text{case } x \; \text{of } (p, q) -> \text{fw} \; p \; q \\
fw \; p \; q = <\text{fbody}>
\]

Now \(f\) (the “wrapper”) is small, and can be inlined at \(f\)’s call sites, often eliminating the allocation of the pair; meanwhile \(fw\) (the “worker”) does the actual work. Strictness analysis, and the worker/wrapper transform to exploit its results, are hugely important to generating efficient code for lazy programs \cite{PeytonJones1994}. \cite{PeytonJones1998}.

In general, \(f\)’s right-hand side often does not have a syntactically visible case expression. For example, what if \(f\) simply called another function \(g\) that was strict in \(x\)? Fortunately the worker/wrapper transform is easy to generalise. Suppose the right hand side of \(f\) was just \(<\text{fbody}\)\}. Then we would transform to

\[
f \; x = \text{case } x \; \text{of } (p, q) -> \text{fw} \; p \; q \\
fw \; p \; q = \text{let } x = (p, q) \; \text{in } <\text{fbody}>
\]

Now we hope that the binding for \(x\) will cancel with case expressions in \(<\text{fbody}\)\}, and indeed it usually proves to be so \cite{PeytonJones1998}.

But what if \(<\text{fbody}\)\} did not use \(q\) at all? Then it would be stupid to pass \(q\) to \(fw\). We would rather transform to:

\[
f \; x = \text{case } x \; \text{of } (p, q) -> \text{fw} \; p \\
fw \; p = \text{let } x = (p, \text{error "urk"}) \; \text{in } <\text{fbody}>
\]

This turns out to be very important in practice. Programmers seldom write functions with wholly-unused arguments, but they frequently write functions that use only part of their argument, and ignoring this point leads to large numbers of unused arguments being passed around in the “optimised” program after the worker-wraper transformation. Absence analysis has therefore been part of GHC since its earliest days \cite{PeytonJones1994}, but it has never been formalised. In the framework of this paper, we give \(f\) a usage signature like this:

\[
f :: U(U, A) \rightarrow \cdot
\]

\footnote{We will always use “called” to mean “applied to one argument”}.
Consider these definitions that pass to \( f \) a data type with just one constructor. The following:

\[
g \cdot y = f \cdot y \text{ (costly } y)\]

Since \( f \) is not strict in \( c, g \) must build a thunk for (costly \( y \)) to pass to \( f \). In call-by-need evaluation, thunks are memoised. That is, when a thunk is evaluated at run-time, it is overwritten with the value so that if it is evaluated a second time the already-computed value can be returned immediately. But in this case we can see that \( f \) never evaluates its second argument more than once, so the memoisation step is entirely wasted. We call these single-entry thunks.

Memoisation is not expensive, but it is certainly not free. Operationally, a pointer to the thunk must be pushed on the stack when evaluation starts, it must be black-holed to avoid space leaks \cite{Jones92}, and the update involves a memory write. If cardinalityanalysis can identify single-entry thunks, as well as one-shot lambdas, that would be a Good Thing. And so it can: we give \( f \) the usage signature:

\[
f :: \omega + U \rightarrow 1 * U \rightarrow \bullet\]

The “\( \omega + \)” modifier says that \( f \) may evaluate its first argument more than once, while the “\( 1 * \)” says that it evaluates its second argument at most once.

2.4 Thunk cardinality

Consider these definitions:

\[
f :: \text{Int} \rightarrow \text{Int} \rightarrow \text{Int}
f x c = \begin{cases} c + 1 & \text{if } x > 0 \\ c - 1 & \text{if } x = 0 \\ \text{else} \end{cases}
\]

\[
g y = f y \text{ (costly } y)\]

The function \( g \) is called at most once. For example consider the call

\[
f 2 g = g \text{ (seq)} 1 \rightarrow f 1 :: 1 * U \rightarrow \bullet\]

The function \( \text{seq} \) evaluates its first argument (to head-normal form) and returns its second argument. If its first argument is a function, the function is evaluated to a lambda, but not called. Notice that \( f 2 \)'s usage type says that \( g \) is evaluated more than once, but applied only once. For example consider the call

\[
f (\langle x \cdot x + y \rangle)\]

How many times is \( y \) evaluated? For \( f \) equal to \( f 1 \) the answer is zero; for \( f 2 \) and \( f 3 \) it is one.

2.5 Call vs Evaluation

For functions, there is a difference between being evaluated once and called once, because of Haskell’s \( \text{seq} \) function. For example:

\[
f 1 g = g \text{ (seq)} 1 \rightarrow f 1 :: 1 * U \rightarrow \bullet \\
f 2 g = g \text{ (seq)} 2 \rightarrow f 2 :: \omega + C^1(U) \rightarrow \bullet \\
f 3 g = g \text{ (seq)} 3 \rightarrow f 3 :: 1 * C^1(U) \rightarrow \bullet \\
\]

The function \( \text{seq} \) evaluates its first argument (to head-normal form) and returns its second argument. If its first argument is a function, the function is evaluated to a lambda, but not called. Notice that \( f 2 \)'s usage type says that \( g \) is evaluated more than once, but applied only once. For example consider the call

\[
f (\langle x \cdot x + y \rangle)\]

How many times is \( y \) evaluated? For \( f \) equal to \( f 1 \) the answer is zero; for \( f 2 \) and \( f 3 \) it is one.

3. Formalising Cardinality Analysis

We now present our analysis in detail. The syntax of the language we analyse is given in Figure 1. It is quite conventional; just lambda calculus with pairs and (non-recursive) let-expressions. Constants \( \kappa \) include literals and primitive functions over literals, as well as Haskell’s built-in \( \text{seq} \). We use A-normal form \cite{SabryF92} so that the issues concerning thunks show up only for \( \text{let} \) and not also for function arguments.

3.1 Usage demands

Our cardinality analysis is a backwards analysis over an abstract domain of usage demands. As with any such analysis, the abstract domain embodies a balance between the cost of the analysis and its precision. Our particular choices are expressed in the syntax of usage demands, given in Figure 1. A usage demand \( d \) is one of the following:

- \( U(d_1^1, d_2^1) \) applies to pairs. The pair itself is evaluated and its first component is used as described by \( d_1^1 \) and its second by \( d_2^1 \).
- \( C^n(U) \) applies to functions. The function is called at most \( n \) times, and on each call the result is used as described by \( d \).
- Call demands are, to the best of our knowledge, new.
- \( U \), or “used”, indicating no information; the demand can use the value in an arbitrary way.
- \( HU \), or “head-used”, is a special case; it is the demand that \( \text{seq} \) places on its first argument: \( \text{seq} : U \rightarrow \bullet \).

A usage demand \( d \) always uses the root of the value exactly once; it cannot express absence or multiple evaluation. That is done by \( d^1 \), which is either \( A \) (absent), or \( n * d \) indicating that the value is used at most \( n \) times in a way described by \( d \). In both \( C^n(d) \) and \( n * d \), the multiplicity \( n \) is either \( 1 \) or \( \omega \) (meaning “many”). Notice that a call demand \( C^n(d) \) has a \( d \) inside it, not a \( d^1 \); if a function is called, its body is evaluated exactly once. This is different from pairs. For example, if we have

\[
\text{let } x = (e_1, e_2) \text{ in } \text{fst } x + \text{fst } x
\]

then \( e_1 \) is evaluated twice.

Both \( U \) and \( HU \) come with some non-syntactic equalities, denoted by \( \equiv \) in Figure 1 and necessary for the proof of well-typedness (Section 4). For example, \( U \) is equivalent to a pair demand whose components are used many times, or a many-call-demand where the result is used in an arbitrary way. Similarly, for pairs \( HU \) is
Figure 2: Demands and demand operations

\[ \mu(d^\dagger) = m \]
\[ \mu(A) = 0 \quad \mu(n \ast d) = n \]
\[ d_1^\dagger \land d_2^\dagger = d_1^\dagger \land d_2^\dagger = d_3^\dagger \]
\[ A \land d^\dagger = d^\dagger \]
\[ d^\dagger \land A = d^\dagger \]
\[ n_1 \ast d_1 \land n_2 \ast d_2 = \omega \ast (d_1 \land d_2) \]
\[ A \cup d^\dagger = d^\dagger \]
\[ d^\dagger \cup A = d^\dagger \]
\[ n_1 \ast d_1 \cup n_2 \ast d_2 = (n_1 \cup n_2) \ast (d_1 \cup d_2) \]
\[ d_1 \land d_2 = d_3 \quad d_3 \land d_2 = d_3 \]
\[ d \land U = U \]
\[ U \land d = U \]
\[ d \land HU = U \]
\[ HU \land d = d \]
\[ C_n^A(d_1) \land C_n^A(d_2) = C_n^A(d_1 \land d_2) \]
\[ U(d_1^\dagger, d_2^\dagger) \land U(d_3^\dagger, d_4^\dagger) = U(d_1^\dagger \land d_3^\dagger, d_2^\dagger \land d_4^\dagger) \]
\[ \varphi_1 \land \varphi_2 = \varphi_3 \quad \varphi_1 \lor \varphi_2 = \varphi_3 \]
\[ \varphi_1 \land \varphi_2 = \{ (x : d_1^\dagger, d_2^\dagger) \mid \varphi_i(x) = d_i^\dagger \} \]
\[ \varphi_1 \lor \varphi_2 = \{ (x : d_1^\dagger \lor d_2^\dagger) \mid \varphi_i(x) = d_i^\dagger \} \]
\[ \tau_1 \cup \tau_2 = \tau_3 \]
\[ (d_1^\dagger \rightarrow \tau_1) \cup (d_2^\dagger \rightarrow \tau_2) = (d_1^\dagger \uparrow \land d_2^\dagger \uparrow) \rightarrow (\tau_1 \cup \tau_2) \]
\[ (\tau_1 : \tau_1) \cup (\tau_2 : \tau_2) = (\tau_3 : \tau_3) \]
\[ (\tau_1 : \tau_1) \land (\tau_2 : \tau_2) = (\tau_1 \land \tau_2 : \tau_1 \land \tau_2) \]
\[ n \ast d_1^\dagger = d_2^\dagger \quad n \ast \tau_1 = \tau_2 \quad n \ast \varphi_1 = \varphi_2 \]
\[ 1 \ast d^\dagger = d^\dagger \quad \omega \ast d^\dagger = d^\dagger \land d^\dagger \quad n \ast e = \ast \quad n \ast \varphi = \{ x : n \ast \varphi(x) \mid x \in \text{dom}(\varphi) \} \]
\[ n_1 \cup n_2 = n_3 \]
\[ 1 \cup 1 = 1 \quad \omega \cup n = \omega \quad n \cup \omega = \omega \]
\[ a \subseteq b \quad a \subseteq b \Rightarrow (a \cup b) = b \]

Figure 3: Algorithmic cardinality analysis specification, part 1.

\[ \mu(d^\dagger) = m \quad \mu(A) = 0 \quad \mu(n \ast d) = n \]
\[ d_1^\dagger \land d_2^\dagger = d_3^\dagger \]
\[ A \land d^\dagger = d^\dagger \]
\[ d^\dagger \land A = d^\dagger \]
\[ n_1 \ast d_1 \land n_2 \ast d_2 = \omega \ast (d_1 \land d_2) \]
\[ A \cup d^\dagger = d^\dagger \]
\[ d^\dagger \cup A = d^\dagger \]
\[ n_1 \ast d_1 \cup n_2 \ast d_2 = (n_1 \cup n_2) \ast (d_1 \cup d_2) \]

3.2 Usage analysis

The analysis itself is shown in Figures 3 and 4. The main judgement form is written thus

\[ P \vdash \tau \downarrow d \Rightarrow (\tau ; \varphi) \Rightarrow \varphi \]

which should be read thus: in signature environment \( P \), and under usage demand \( d \), the term \( \tau \) places demands \( (\tau ; \varphi) \) on its components, and elaborates to an annotated term \( \varphi \). The syntax of each of these components is given in Figure 1 and their roles in the judgement are the following:
The signature environment $P$ maps some of the free variables of $e$ to their usage signatures, $\rho$ (Section 3.5). Any free variables outside the domain of $P$ have an uninformative signature.

The usage demand, $d$, describes the degree to which $e$ is evaluated, including how many times its sub-components are evaluated or called.

Using $P$, the judgement transforms the incoming demand $d$ into the demands $(\tau; \varphi)$ that $e$ places on its arguments and free variables respectively:

- The usage that $e$ places on its argument is given by $\tau$, which gives a demand $d^\tau$ for each argument.
- The usage that $e$ places on its free variables is given by its free-variable usage ($fv$-usage), $\varphi$, which is simply a finite mapping from variables to usage demands.

We will discuss the elaborated expressions $e'$ in Section 3.7.

For example, consider the expression

$$e = \lambda x . \text{case } x \text{ of } (p, q) \rightarrow (p, f \text{ True})$$

Suppose we place demand $C^1(U)$ on $e$, so that $e$ is called, just once. What demand does it then place on its arguments and free variables?

$$e \triangleright e \downarrow C^1(U) \Rightarrow (1 \ast U(\omega + U, A) \rightarrow ; \{ f \mapsto 1 \ast C^1(U)\})$$

That is, $e$ will use its argument once, its argument’s first component perhaps many times, but will ignore its arguments second component (the $A$ in the usage type). Moreover $e$ will call $f$ just once.

In short, we think of the analysis as describing a demand transformer, transforming a demand on the result of $e$ into demands on its arguments and free variables.

3.3 Pairs and case expressions

With these definitions in mind, we can look at some of the analysis rules in Figure 2. Rule PAIR explains how to analyse a pair under a demand $U(d^1, d^2)$. We simply analyse the two components, under $d^1$ or $d^2$ respectively, and combine the results with “$\&$”. The auxiliary judgement $\triangleright^*$ (Figure 3) deals with the multiplicity of the argument demands $d^\tau$.

The “$\&$” operator, pronounced “both”, is defined in Figure 2 and combines the free-variable usages $\varphi_1$ and $\varphi_2$. For most the part the definition is straightforward, but there is a very important wrinkle for call demands:

$$C^{n1}(d^1) \& C^{n2}(d^2) = C^{\omega}(d^1 \cup d^2)$$

The “$\cup$” part is easy, since $n_1$ and $n_2$ are both at least 1. But note the switch from $\&$ to the least upper bound $\uplus$! To see why, consider what demand this expression places on $f$:

$$f \ 1 \ 2 \ + \ f \ 3 \ 4$$

Each call gives a usage demand for $f$ of $1 \ast C^1(C^1(U))$, and if we use $\&$ to combine that demand with itself we get $\omega \ast C^\omega(C^\omega(U))$. The inner “$1$” is a consequence of the switch to $\uplus$, and rightly expresses the fact that no partial application of $f$ is called more than once.

The other rules for pairs PAIRU, PAIRHU, and case expressions CASE should now be readily comprehensible ($\varphi_\setminus x, y$ stands for the removal of $(x, y)$ from the domain of $\varphi_\setminus$).

3.4 Lambda and application

Rule LAM for lambdas expects the incoming demand to be a call demand $C^{\omega}(d_\lambda)$. Then it analyses the body $e$ with demand $d_\gamma$ to give $(\tau; \varphi)$. If $n = 1$ the lambda is called at most once, so we can return $(\tau; \varphi)$; but if $n = \omega$ the lambda may be called more than once, and each call will place a new demand on the free variables. The $n \ast \varphi$ operation on the bottom line accounts for this multiplicity, and is defined in Figure 2. Rule LAMU handles an incoming demand of $U$ by treating it just like $C^0(U)$, while LAMHU deals with the head-used demand $HU$, where the lambda is not even called so we do not need to analyse the body, and $e$ is obtained from $e$ by adding arbitrary annotations. Similarly the return type $\tau$ can be any type, since the lambda-abstraction is not going to be applied, but is only head-used. Dually, given an application $(e \ y)$, rule APPA analyses $e$ with demand $C^1(d)$, reflecting that $e$ is here called once. This returns the demand $(d^\tau \rightarrow \tau_1; \varphi_1)$ on the context. Then we can analyse the argument under demand $d^\gamma$, using “$\ast$", yielding $\varphi_2$; and combine $\varphi_1$ and $\varphi_2$. Rule APPB applies when analysing $e_1$ yields the less-informative usage type $\setminus$.

3.5 Usage signatures

Suppose we have the term

$$\text{let } f = \lambda x . \lambda y . \text{True } \text{ in } f \ p \ q$$

We would like to determine the correct demands on $p$ and $q$, namely $l_\omega C^1(U)$ and $A$ respectively. The gold standard would be to analyse $f$’s right-hand side at every call site; that is, to behave as if $f$ were inlined at each call site. But that is not very modular; with deeply nested function definitions, it can be exponentially expensive to analyse each function body afresh at each call site; and it does not work at all for recursive functions. Instead, we want to analyse $f$, summarise its behaviour, and then use that summary at each call site. This summary is called $f$’s usage signature. Remember that the main judgement describes how a term transforms a demand for the value into demands on its context. So a usage signature must be a (conservative approximation of this) demand transformer.

There are many ways in which one might approximate $f$’s demand transformer, but rule LETDN (Figure 4) uses a particularly simple one:

- Look at $f$’s right-hand side $\lambda y_1 \ldots \lambda y_k . e_1$, where $e_1$ is not a lambda-expression.
- Analyse $e_1$ in demand $U$, giving $(\tau_1; \varphi_1)$.
- Record the triple $(k; \varphi(y); \tau_1)$ as $f$’s usage signature in the environment $P$ when analysing the body of the let.

Now, at a call site of $f$, rule VARDN calls transform($\rho, d$) to use the recorded usage signature $\rho$ to transform the demand $d$ for this occurrence of $f$.

What does transform($k; \tau; \varphi$, $d$) do (Figure 7)? If the demand $d$ on $f$ is stronger than $C^1(C^1(U))$, where the call demands are nested $k$ deep, we can safely unleash $(\tau; \varphi)$ at the call site. If not, we simply treat the function as if it were called many times, by ununlocking $\omega + \tau$ and multiplying both the demand type $\tau$ and the usage environment $\varphi$ (Figure 2). Rule LETDNABS handles the case when the variable is not used in the body.

3.6 Thunks

The LETDN rule unleashes (an approximation to) the demands of the right-hand side at each usage site. This is good if the right hand side is a lambda, but not good otherwise, for two reasons. Consider

$$\text{let } x = y + 1 \text{ in } x + x$$

How many times is $y$ demanded? Just once! The thunk $x$ is demanded twice, but $x$’s thunk is memoised, so the $y+1$ is evaluated only once. So it is wrong to unleash a demand on $y$ at each of $x$’s occurrence sites. Contrast the situation where $x$ is a function

$$\text{let } x = \lambda v . y + v \text{ in } x 42 + x \ 239$$

Here $y$ really is demanded twice, and LETDN does that. Another reason that LETDN would be sub-optimal for thunks is shown here:
This idea is embodied in the L
ET hand side.

If we analysed x
m
, the right hand side is not a lambda). Rule L
ET
A introduces a new binding on the heap. The rules EB
E, EAP
P, EPAIR and EPRED are standard. Notice that EB
E also fires only if the λ’s multiplicity m is non-zero. Note that the analysis does not assign zero-annotations to lambdas, but we need them for the soundness result.

Rule ELKP
V de-references a binding for an already-evaluated expression [x ↦ Val(v)], and in a standard semantics would return v leaving the heap unaffected. In our counting semantics however,

4. Soundness of the Analysis

We establish the soundness of our analysis in a sequence of steps. Soundness means that if the analysis claims that, say, a lambda is one-shot, then that lambda is only called once; and similarly for single-entry thunks. We formalise this property as follows:

- We present an operational semantics, written →, for the annotated language that counts how many times thunks have been evaluated and λ-abstractions have been applied. The semantics simply gets stuck when these counters reach zero, which will happen only if the claims of the analysis are false (Section 4.1).
- Our goal is to prove that if an expression e is elaborated to e by the analysis, then e in the instrumented semantics behaves identically to e in a standard un-instrumented call-by-need semantics (Section 4.2). For reasons of space we omit the rules for the un-instrumented call-by-need semantics which are completely standard (See [97]), and are identical to the rules of Figure 5 if one simply ignores all the annotations and the multiplicity side-conditions. We refer to this semantics as →.
- We prove soundness by giving a type system for the annotated terms, and showing that for well-typed terms, the instrumented semantics → simulates →, in a type-preserving way.

4.1 Counting operational semantics

We present a simple counting operational semantics for annotated terms in Figure 5. This is a standard semantics for call-by-need, except for the fact that multiplicity annotations decorate the terms, stacks, and heaps. The syntax for heaps, denoted with H, contains two forms of bindings, one for expressions [x ↦ Val(e)] and one for already evaluated expressions [x ↦ Val(v)]. The multiplicity m ∈ {0, 1, ∞} denotes how many more times are we allowed to de-reference this particular binding. The stacks, denoted with S, are just lists of frames. The syntax for frames includes application frames ( e y ), which store a reference y to an argument, case-frames ((x, y) → e), which account for the execution of a case-branch, and update frames of the form #(x, m), which take care of updating the heap when the active expression reduces to a value.

The first component of an update frame is a name of a variable to be updated, and the second one is its thunk cardinality.

Rule ELET allocates a new binding on the heap. The rules EB
E fires only if the cardinality annotation is non-zero; it de-references an Exp(e) binding and emits an update frame. Rules EB
E, EA
P, EP
A and EPRED are standard. Notice that EB
E also fires only if the λ’s multiplicity m is non-zero. Note that the analysis does not assign zero-annotations to lambdas, but we need them for the soundness result.

Rule ELKP
V de-references a binding for an already-evaluated expression [x ↦ Val(e)], and in a standard semantics would return e leaving the heap unaffected. In our counting semantics however,
we need to account for two things. First, we decrease the multiplicity
arity annotation on the binding (from \( m + 1 \) to \( m \)) in rule ELKPv.
Moreover, the value \( v \) can in the future be used both directly (since
it is now the active expression), and indirectly through a future
de-reference of \( x \).

We express this by non-deterministically splitting
the value \( v \), returning two values \( v_1 \) and \( v_2 \) whose top-level
\( \lambda \)-annotations sum up to the original (see split in Figure 5). Our
proof needs only ensure that among the non-deterministic choices there
exists a choice that simulates \( \mu \). Rule EUPD is similar except
that the heap gets updated by an update frame.

4.2 Checking well-annotated terms

We would like to prove that if we analyse a term \( e \), producing an
annotated term \( \tilde{e} \), then if \( e \) executes for a number of steps in the
standard semantics \( \Rightarrow \), then execution of \( \tilde{e} \) does not get stuck
in the instrumented semantics \( \Rightarrow \) of Figure 5. To do this we need to
do prove preservation and progress lemmas, showing that each step
takes a well-annotated term to a well-annotated term, and that well-
annotated terms do not get stuck.

Figure 5 says what it means to be “well-annotated”, using notation
from Figures 3 and 2. The rules look very similar to the analysis
rules of Figures 3 and 4, except that we check an annotated term,
rather than producing one. For example, rule TLAM checks that
the annotation on a \( \lambda \)-abstraction \( m \) is at least as large as the
call cardinality we press on this \( \lambda \)-abstraction \( m \). As evaluation
progresses the situation clarifies, so the annotations may become
more conservative than the checker requires, but that is fine.

A more substantial difference is that instead of holding concrete
demand transformers \( \rho \) as the analysis does (Figure 3), the environ-
ment \( P \) holds generalised demand transformers \( \rho \). A generalised
demand transformer is simply a monotone function from a demand
to a pair \( (\tau ; \varphi) \) of a type and a usage environment (Figure 2).
In the TLTDN rule, we clairvoyantly choose any such transformer \( \rho \),
which is sound for the RSH expression – denoted with \( P \upharpoonright e_1 \rho \).
We still check that \( e_1 \) can be type checked with some demand
\( d_1 \) that comes from type-checking the body of the \( \lambda \) (Figure 2).
In rule TVARDN we simply apply the transformer \( \rho \) to get a type
and fv-usage environment.

Rule WfTTRANS imposes two conditions necessary for the sound-
ness of the transformer. First, it has to be a monotone function on
the demand argument. Second, it has to soundly approximate any
type and usage environment that we can attribute to the expression.
One can easily confirm that the intensional representation used in
the analysis satisfies both properties for the \( \lambda \)-expressions bound
with LETDN.

Because these rules conjure up functions \( \rho \) out of thin air, and have
universally quantified premises (\( \text{WfTRANS} \)), they do not
constitute an algorithm. But for the very same reasons they are
convenient to reason about in the metatheory, and that is the only
reason we need them. In effect, Figure 6 constitutes an elaborate
invariant for the operational semantics.

4.3 Soundness of the analysis

The first result is almost trivial.

Lemma 4.1 (Analysis produces well-typed terms). If \( P \upharpoonright e \Downarrow d \Rightarrow (\tau ; \varphi) \sim e \) then \( P \upharpoonright e \Downarrow d \Rightarrow (\tau ; \varphi) \).

We would next like to show that well-typed terms do not get stuck.
To present the main result we need some notation first.

Definition 4.1 (Unannotated heaps and stacks and erasure). We use
\( H \) and \( S \) to refer to an un-instrumented heap and stack respectively.
We use \( e^\ast = e \) to mean that the erasure of all annotations from \( e \) is
\( e \), and we define \( S^\ast = S \) and \( H^\ast = H \) analogously.

We can show that annotated terms run for at least as many steps as
their erasures would run in the un-instrumented semantics:

Theorem 4.2 (Safety for annotated terms). If \( e \Downarrow e_1 \downarrow HU \Rightarrow (\tau ; \varphi) \) and \( e_1 = e^\ast_1 + (\epsilon ; \epsilon) ; e \) \( \Downarrow^k \) then there
exists \( H_2 \) and \( S \), such that \( (\epsilon ; e_1) ; e \Downarrow^k (H_2 ; S) \).

Unsurprisingly, to prove this theorem we need to generalise the
statement to talk about a single-step reduction of a configuration
with arbitrary (but well-annotated) heap and stack. Hence we intro-
duce a well-annotated configuration relation, denoted \( \Downarrow \) \( \langle H ; e ; S \rangle \),
that extends the well-annotation invariant of Figure 6 to configurations.
For reasons of space, we only give the statement of the
theorem below, and defer the details of the well-annotation relation
to Appendix A.

Lemma 4.3 (Single-step safety). Assume that \( \Downarrow \langle H_1 ; e_1 ; S_1 \rangle \).
If \( \langle H_1 ; e_1 S_1 \rangle \Downarrow \langle H_2 ; e_2 ; S_2 \rangle \) in the un-instrumented
semantics, then there exist \( H_2 \) and \( S_2 \), such that \( \langle H_1 ; e_1 ; S_1 \rangle \Downarrow \langle H_2 ; e_2 ; S_2 \rangle \).

Notice that the counting semantics is non-deterministic, so Lemma 4.3
simply ensures that there exists a possible transition in the counting
semantics that always results in a well-typed configuration.

Lemma 4.4 crucially relies on yet another property, below.
\[
\begin{align*}
P & ::= \epsilon \mid P, (x : g) \quad g \in d \Rightarrow \langle \tau ; \varphi \rangle \\
P \vdash e \downarrow d & \Rightarrow \langle \tau ; \varphi \rangle \quad \text{TVA RDN} \\
(x : g) \in P & \Rightarrow (x : g) = g(d) \quad \text{TVA UP} \\
P \vdash x \downarrow d & \Rightarrow \langle \tau ; \varphi \rangle & \text{ and } \text{dom}(P) \\
x \notin \text{dom}(P) & \Rightarrow \langle \tau ; \varphi \rangle \quad \text{TVA UP} \\
d \subseteq C^n(d_e) & \quad m \geq n \quad P \vdash e \downarrow d_e \Rightarrow \langle \tau ; \varphi \rangle \quad \text{T LAM} \\
P & \vdash \lambda^n x. e \downarrow d \Rightarrow \langle \varphi(x) \rightarrow \tau ; n*(\varphi') \rangle \quad \text{T LAM} \\
d \subseteq \text{HU} & \Rightarrow \langle \tau ; \varphi \rangle \quad \text{T LAM HU} \\
P \vdash e_1 \downarrow d_1 & \Rightarrow (\tau_1 ; \varphi_1) \quad \text{T L ET DN} \\
\tau_1 \leq d_1 & \Rightarrow \tau_2 \quad P \vdash y \downarrow d_2 \Rightarrow \varphi_2 \quad \text{T L ET UP} \\
P \vdash e_1 \downarrow d & \Rightarrow (\tau ; \varphi_1 \land \tau_2) \\
& \quad \text{case } e_1 \text{ of } (x, y) \rightarrow e_1 \downarrow d \Rightarrow (\tau ; \varphi_1 \land \varphi_2) \quad \text{T CASE} \\
m & \geq \rho(\varphi_2(x)) \quad \varphi_2(x) \subseteq n \times d_1 \\
P \vdash e_1 \downarrow d_1 & \Rightarrow (\tau_1 ; \varphi_1) \quad P \not\vdash e_1 ; \varphi \\
P \vdash (x : g) \uparrow \downarrow d & \Rightarrow \langle \tau ; \varphi \rangle \quad \text{T L ET UP A B S} \\
P \vdash e_2 \downarrow d & \Rightarrow (\tau ; \varphi_2) \quad A = \varphi_2(x) \\
P \vdash e_2 \downarrow d & \Rightarrow \langle \tau ; \varphi_2 \rangle \quad \text{T L E T UP A B S} \\
P \vdash e_1 \downarrow d & \Rightarrow (\tau ; \varphi_1 \land \varphi_2) \\
P \vdash x \downarrow d & \Rightarrow \varphi \quad \text{T A B S} \\
P \vdash x \downarrow d & \Rightarrow \langle \tau ; \varphi \rangle \quad \text{T M U L I} \\
P \vdash x \downarrow d & \Rightarrow \epsilon \quad \text{T A B S} \\
P \vdash x \downarrow d & \Rightarrow n \times \varphi \quad \text{T A B S} \\
\forall d_1, d_2, d \subseteq d_2 & \Rightarrow g(d_1) \subseteq g(d_2) \\
\forall d, \varphi, \tau, (P \vdash e \downarrow d \Rightarrow \langle \tau ; \varphi \rangle) & \Rightarrow (\tau ; \varphi) \subseteq g(d) \\
P \not\vdash e ; \varphi \\
\text{WFTRANS}
\end{align*}
\]

Figure 6: Well-annotated terms

**Lemma 4.4** (Value demand splitting). If \( P \vdash \epsilon \downarrow (d_1 \land d_2) \Rightarrow (\tau ; \varphi) \) then there exists a split \( (\epsilon, v_1) = (v_1, v_2) \) such that:

\( P \vdash v_1 \downarrow d_1 \Rightarrow (\tau_1 ; \varphi_1) \) and \( P \vdash v_2 \downarrow d_2 \Rightarrow (\tau_2 ; \varphi_2) \) and moreover \( \tau_1 \subseteq \tau, \tau_2 \subseteq \tau \) and \( \varphi_1 \land \varphi_2 \subseteq \varphi \).

Why is Lemma 4.4 important? Consider the following:

\[
\text{let } x = v \text{ in case } 3 \text{ of } (y, z) \rightarrow x 4
\]

Figure 7: Auxiliary simulation relation (heaps and stacks)

The demand exercised on \( x \) from the body of the \texttt{let-binding} will be \( C^1(U) \land C^1(U) = C^m(U) \) and hence the value \( v \) will be checked against this demand (using the \text{T LET UP} rule), unleashing an environment \( \varphi \). However, after substituting \( v \) in the body (which is ultimately what call-by-need will do) we will have checked it against \( C^1(U) \) and \( C^1(U) \) independently, unleashing \( \varphi_1 \) and \( \varphi_2 \) in each call site. Lemma 4.4 ensures that reduction never increases the demand on the free variables of the environment, and hence safety is not compromised. It is precisely the proof of Lemma 4.4 that requires demand transformers to be monotone in the demand arguments, ensured by \text{WFTRANS}.

**Theorem 4.5** (Safety of analysis). If \( \epsilon, e \downarrow H \) then there exist \( H \) and \( S \), such that \( \epsilon ; e_1 = e \rightarrow^k (H ; e_2 ; S) \) and \( \epsilon \rightarrow^k (H ; e_2 ; S) \), \( H^2 = H \) and \( S^2 = S \) and \( e_2 = e_2 \).

The proof is just a combination of Lemma 4.1 and Theorem 4.2.

5. Optimisations

We discuss next the two optimisations enabled by our analysis.

5.1 Optimised allocation for thunks

We show here that for 0-annotated bindings there is no need to allocate an entry in the heap, and for 1-annotated ones we don’t have to emit an update frame on the stack. Within the chosen operational model, this optimisation is of dynamic nature as we will see by providing a new, optimising small-step machine for the annotated expressions. The new semantics is defined in Figure 8. We will show that programs that can be evaluated via the counting semantics (Figure 6) can also be evaluated via the optimised semantics in a smaller or equal number of steps. The proof is a simulation proof, hence we define relations between heaps / optimised heaps, and stacks / optimised stacks that are preserved during evaluation.
Definition 5.1 (Auxiliary \(\infty\)-relations). We write \(e_1 \equiv e_2\) if \(e_1\) and \(e_2\) differ only on the \(\lambda\)-annotations. \(H_1 \equiv H_2\) and \(S_1 \equiv S_2\) are defined in Figure 7.

For this optimisation the annotations on \(\lambda\)-abstractions play no role, hence we relate any expressions that differ only on those.

Figure 7 tells us that a heap \(H\) is related with an optimised heap \(H_{opt}\) with the relation \(H \equiv H_{opt}\). As we have described, there are no \(\sim_\omega\) bindings in the optimised heap. Moreover notice that there are no bindings of the form \([x \mapsto \text{Val}(v)]\) in either the optimised or unoptimised heap. It is easy to see why: every heap binding starts life as \([x \mapsto \text{Exp}(e)]\). By the time \(\text{Exp}(e)\) has become a value \(\text{Val}(v)\), we have already used \(x\) once. Hence, if originally \(m = \omega\) then the value binding will also be \(\omega\) (in the optimised or unoptimised semantics). If it was \(m = 1\) then it can only be 0 in the un-optimised heap and non-existent in the optimised heap. If it was \(m = 0\) then no such bindings would have existed in the optimised heap anyway.

The relation between stacks is given with \(S \equiv S_{opt}\). Rule SSIM2 ensures that there are no frames \(\#(x, 0)\) in the optimised stack. In fact during evaluation it is easy to observe that there are not going to be any update frames \(\#(x, 0)\) in the original or optimised stack.

We can now state the optimisation simulation theorem.

Theorem 5.1 (Optimised semantics). If \(\langle H; e_1; S_1 \rangle \vdash (H_2; e_2; S_2)\) and \(\langle H_1; e_1; S_1 \rangle \rightarrow (H_1; e_1; S_1)\) then there exists \(k \in \{0, 1\}\) s.t. \(\langle H_2; e_2; S_2 \rangle \rightarrow^k (H_2; e_2; S_2)\) and \(\langle H_1; e_1; S_1 \rangle \rightarrow (H_1; e_1; S_1)\).

Notice that the counting semantics may not be able to take a transition at some point due to the wrong non-deterministic choice but in that case the statement of Theorem 5.1 holds trivially. Finally, we tie together Theorems 5.1 and 4.1 to get the following result.

Theorem 5.2 (Analysis is safe for optimised semantics). If \(\triangleright e_1 \parallel HU \Rightarrow \langle \tau; e \rangle \parallel e_1\) and \(\langle \epsilon; e_1; e \rangle \rightarrow^n (H; e_2; S)\) then \(\langle \epsilon; e_1; e \rangle \rightarrow^m (H; e_2; S)\). So \(e_2\) is in the reference semantics, then it also evaluates to the same (modulo annotation) in the optimised semantics in \(n\) steps or fewer; and the heaps and stacks are consistent. Moreover, the theorem has informative content on infinite sequences. For example it says that for any point in the evaluation in the reference semantics, we will have earlier reached a corresponding intermediate configuration in the optimised semantics with consistent heaps and stacks.

5.2 Let-in floating into one-shot lambdas

As discussed in Section 2, we are interested in the particular case of let-floating (Peyton Jones et al. 1996): moving the binder into the body of a lambda-expression. This transformation is trivially safe, given obvious syntactic side conditions (Moran and Sands 1999 §4.5), however, in general, it is not beneficial. Here we describe the conditions under which let-in floating makes things better in terms of the length of the program execution sequence.

We start by defining let-in floating in a form of syntactic rewriting:

Definition 5.2 (Let-in floating for one-shot lambdas).

\[
\begin{align*}
\text{let } z \equiv e_1 \text{ in } (\text{let } f \equiv \lambda x . e \text{ in } e_2) & \Rightarrow \text{let } f \equiv \lambda x . (\text{let } z \equiv e_1 \text{ in } e) \text{ in } e_2,
\end{align*}
\]

for any \(m_1, m_2\) and \(z \notin \text{FV}(e_2)\).

Next, we provide a number of definitions necessary to formulate the so called improvement result (Moran and Sands 1999). The improvement is formulated for closed, well-formed configurations. For a configuration \(\langle H; e; S \rangle\) to be closed, any free variables in \(H\), \(e\) and \(S\) must be contained in a union \(\text{dom}(H) \cup \text{dom}(S)\), where \(\text{dom}(H)\) is a set of variables bound by a heap \(H\), and \(\text{dom}(S)\) is a set of variables marked for update in a stack \(S\). A configuration is well-formed if \(\text{dom}(H)\) and \(\text{dom}(S)\) are disjoint.

Definition 5.3 (Convergence). For a closed configuration \(\langle H; e; S \rangle\):

\[
\langle H; e; S \rangle \uparrow N \equiv \exists H', v, N. \ (H; e; S) \longrightarrow^N (H'; v; e) \quad \langle H; e; S \rangle \uparrow M \equiv \exists M. \ (H; e; S) \uparrow M \quad \text{and} \ M \leq N
\]

The following theorem shows that local let-in floating into the body of a one-shot lambda does not make the execution longer.

Theorem 5.3 (Let-in float improvement). For any \(H\) and \(S\), if

\[
\langle H; \text{let } z \equiv e_1 \text{ in } (\text{let } f \equiv \lambda x . e \text{ in } e_2) ; S \rangle \uparrow N
\]

and \(z \notin \text{FV}(e_2)\), then

\[
\langle H; \text{let } f \equiv \lambda x . (\text{let } z \equiv e_1 \text{ in } e) \text{ in } e_2 ; S \rangle \uparrow N.
\]

Even though Theorem 5.3 gives a termination-dependent result, its proof (in Appendix B) goes via a simulation argument, hence it is possible to state the theorem in a more general way without requiring termination.

We also expect that the improvement result extends to arbitrary program contexts, but have not carried out the exercise.

Figure 8: Optimised counting semantics
6. Implementation

We have implemented the cardinality analyser by extending the demand analysis machinery of the Glasgow Haskell Compiler, available from its open-source repository. We briefly summarise some implementation specifics in this section.

6.1 Analysis

The implementation of the analysis was straightforward, because GHC’s existing strictness analyser is already cast as a backwards analysis, exactly like our new cardinality analysis. So the existing analyser worked unchanged; all that was required was to enrich the domains over which the analyser works. In total, the analyser increased from 900 lines of code to 1,140 lines, an extremely modest change.

We run the analysis twice, once in the middle of the optimisation pipeline, and once near the end. The purpose of the first run is to expose one-shot lambdas, which in turn enable a cascade of subsequent transformations (Section 6.3). The second analysis finds the single-entry thunks, which are exploited by the code generator. This second analysis is performed very late in the pipeline (a) so that it sees the result of all previous inlining and optimisation and (b) because the single-entry thunk information is not robust to certain other transformations (Section 6.4).

6.2 Absence

GHC exploits absence in the worker/wrapper split, as described in Section 2. Absent arguments are not passed from the wrapper to the worker.

6.3 One-shot lambdas

As shown in Section 5.2, there is no run-time payoff for one-shot lambdas. Rather, the information enables some important compile-time transformations. Specifically, consider

\[
\text{let } x = \text{costly } v \text{ in } \ldots (\lambda y \ldots x \ldots) \ldots
\]

If the \( \lambda y \) is a one-shot lambda, the binding for \( x \) can be floated inside the lambda, without risk of duplicating the computation of costly. Once the binding for \( x \) is inside the \( \lambda y \), several other improvements may happen:

- It may be inlined at \( x \)’s use site, perhaps entirely eliminating the allocation of a thunk for \( x \).
- It may enable a rewrite rule (eg foldr/build fusion) to fire.
- It may allow two lambdas to be replaced by one. For example

\[
\begin{align*}
\text{let } x &= \text{costly } v \text{ in } \lambda y \ldots x \ldots \\
\implies f &= \lambda v \cdot \text{let } x &= \text{costly } v \text{ in } \lambda y \ldots x \ldots
\end{align*}
\]

The latter produces one function with two arguments, rather than a curried function that returns a heap-allocated lambda (Marlow and Peyton Jones 2006).

6.4 Single-entry thunks

The code that GHC compiles for a thunk begins by pushing an update frame on the stack, which includes a pointer to the thunk. Then the code for the thunk is executed. When evaluation is complete, the value is returned, and the update frame overwrites the thunk with an indirection to the values (Peyton Jones 1992). It is easy to modify this mechanism to take advantage of single-entry thunks: we do not generate the push-update-frame code for single-entry thunks. There is a modest code size saving (fewer instructions generated) and a modest runtime saving (a few store instructions saved on thunk entry, and a few more when evaluation is complete).

Take care though! The single-entry property is not robust to program transformation. For example, common sub-expression elimination (CSE) can combine two single-entry thunks into one multiple-entry one, as can this sequence of transformations:

\[
\begin{align*}
\text{let } y &= e \text{ in } \text{let } x &= y + 0 \text{ in } x \\
\text{Identity of } + & \implies \text{let } y &= e \text{ in } \text{let } x &= y + x \\
\text{Inline } x & \implies \text{let } y &= y + y \text{ Wrong!}
\end{align*}
\]

This does not affect the formal results of the paper, but it is the reason that our second run of the cardinality analysis is immediately before code generation.

7. Evaluation

To measure the accuracy of the analysis, we counted the proportion of (a) one-shot lambdas and (b) single-entry thunks. In both cases, these percentages are of the syntactically occurring lambdas or thunks respectively, measured over the code of the benchmark program only, not library code. Table 1 shows the results reported by our analysis for programs from the nofib benchmark suite (Purcell 1993). The numbers are quite encouraging. One-shot lambdas account for 0-30% of all lambdas, while single-entry thunks are 0-23% of all thunks.

<table>
<thead>
<tr>
<th>Program</th>
<th>Synt. ( \lambda )</th>
<th>Synt. Thnk</th>
<th>RT Thnk</th>
</tr>
</thead>
<tbody>
<tr>
<td>anna</td>
<td>4.0%</td>
<td>7.2%</td>
<td>2.9%</td>
</tr>
<tr>
<td>bspt</td>
<td>5.0%</td>
<td>15.4%</td>
<td>1.5%</td>
</tr>
<tr>
<td>cacheprof</td>
<td>7.6%</td>
<td>11.9%</td>
<td>5.1%</td>
</tr>
<tr>
<td>calendar</td>
<td>5.7%</td>
<td>0.0%</td>
<td>0.2%</td>
</tr>
<tr>
<td>constraints</td>
<td>2.0%</td>
<td>3.2%</td>
<td>4.5%</td>
</tr>
<tr>
<td>cryptarithm2</td>
<td>0.6%</td>
<td>3.0%</td>
<td>74.0%</td>
</tr>
<tr>
<td>gcd</td>
<td>12.5%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>gen_regress</td>
<td>5.6%</td>
<td>0.0%</td>
<td>0.2%</td>
</tr>
<tr>
<td>hpg</td>
<td>5.2%</td>
<td>0.0%</td>
<td>4.1%</td>
</tr>
<tr>
<td>integer</td>
<td>8.3%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>life</td>
<td>3.2%</td>
<td>0.0%</td>
<td>1.8%</td>
</tr>
<tr>
<td>mkhprog</td>
<td>27.4%</td>
<td>20.8%</td>
<td>5.8%</td>
</tr>
<tr>
<td>nucleic2</td>
<td>3.5%</td>
<td>3.1%</td>
<td>3.2%</td>
</tr>
<tr>
<td>partstof</td>
<td>5.8%</td>
<td>10.7%</td>
<td>0.1%</td>
</tr>
<tr>
<td>sphere</td>
<td>7.8%</td>
<td>6.2%</td>
<td>20.0%</td>
</tr>
</tbody>
</table>

Table 1. Analysis results for nofib: ratios of syntactic one-shot lambdas (Synt. \( \lambda \)), syntactic used-once thunks (Synt. Thnk) and runtime entries into single-entry thunks (RT Thnk).

The static (syntactic) frequency of single-entry thunks may be very different to their dynamic frequency in a program execution, so we instrumented GHC to measure the latter. (We did not measure the dynamic frequency of one-shot lambdas, because they confer no direct performance benefit.) The “RT Thnk” column of Table 1 gives the dynamic frequency of single-entry thunks in the same nofib programs. Note that these statistics include single-entry thunks from libraries, as well as the benchmark program code. The results vary widely. Most programs do not appear to use single-entry thunks much, while a few use many, up to 74% for cryptarithm2.

7.1 Optimising nofib programs

In the end, of course, we seek improved runtimes, although the benefits are likely to be modest. One-shot lambdas do not confer
any performance benefits directly; rather, they remove potential obstacles from other compile-time transformations. Single-entry thunks, on the other hand give an immediate performance benefit, by omitting the push-update-frame code, but it is a small one.

Table 2 summarises the effect of cardinality analysis when running the nofib suite. “Allocs” is the change in how much heap was allocated when the program is run and “Runtime” is a change in the actual program execution time.

In Section 2.1 we mentioned a hack, used by Gill in GHC, in which he hard-coded the call-cardinality information for three particular functions: build, foldr and runST. Our analysis renders this hack redundant, as now the same results can be soundly inferred. We therefore report two sets of results: relative to an un-hacked baseline, and relative to a hacked baseline. In both cases binary size of the (statically) linked binaries falls slightly but consistently (2.0% average), which is welcome. This may be due to less push-update-frame code being generated.

Considering allocation, the numbers relative to the non-hacked baseline are quite encouraging, but relative to the hacked compiler the improvements are modest: the hack was very effective! Otherwise, only one program, nucleic2 shows a significant (11%) reduction in allocation, which turned out to be because a thunk was floated inside a one-shot lambda and ended up never being allocated, exactly as advertised.1

A shortcoming of nofib suite is that runtimes tend to be short and very noisy; even with the execution key slow only 18 programs from the suite run for longer than half second (with a maximum of 2.5 seconds for constraints). Among those long-runners the biggest performance improvement is 8.8% (for integer), with an average of 2.3%.

1One can notice that the new compiler sometimes performs worse than the cardinality-unaware versions in a very few benchmarks in nofib. In a highly optimising compiler with many passes it is very hard to ensure that every “optimisation” always makes the program run faster, and, even if a pass does improve the program per se, to ensure that every subsequent pass will carry out all the optimisations that it did before the earlier improvement was implemented. The data show that we do not always succeed. We leave for the future some detailed forensic work to find out exactly why.

For more realistic numbers, we measured the improvement in run-time, relative to the hacked compiler, for several programs from the Computer Language Benchmarks Game. The results are shown in Table 3. All programs were run with the official shootout settings (except spectral-norm, to which we gave a bigger input value of 7500) on a 2.7 GHz Intel Core i7 OS X machine with 8 Gb RAM. These are uncharacteristic Haskell programs, optimised to within an inch of their life by dedicated Haskell hackers. There is no easy meat to be had, and indeed the heap-allocation changes are so tiny (usually zero, and -0.2% at the most in the case of binary-trees) that we omit them from the table. However, we do get one joyful result: a solid speedup of 9.2% in binary-trees due to fewer thunk updates. As you can see, nearly half of its thunks entered at runtime are single-entry.

### Table 2. Cardinality analysis-enabled optimisations for nofib

<table>
<thead>
<tr>
<th>Program</th>
<th>Allocs</th>
<th>Runtime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No hack</td>
<td>Hack</td>
</tr>
<tr>
<td></td>
<td>No hack</td>
<td>Hack</td>
</tr>
<tr>
<td>anna</td>
<td>-2.1%</td>
<td>+0.1%</td>
</tr>
<tr>
<td>bept</td>
<td>-2.2%</td>
<td>+0.0%</td>
</tr>
<tr>
<td>calendar</td>
<td>-7.9%</td>
<td>-0.0%</td>
</tr>
<tr>
<td>constraints</td>
<td>-0.9%</td>
<td>-1.2%</td>
</tr>
<tr>
<td>cryptarithm2</td>
<td>-0.3%</td>
<td>-2.3%</td>
</tr>
<tr>
<td>gcd</td>
<td>-15.5%</td>
<td>-0.0%</td>
</tr>
<tr>
<td>gen_regexps</td>
<td>-1.0%</td>
<td>-0.0%</td>
</tr>
<tr>
<td>hpg</td>
<td>-2.0%</td>
<td>-0.1%</td>
</tr>
<tr>
<td>integer</td>
<td>0.0%</td>
<td>-8.8%</td>
</tr>
<tr>
<td>life</td>
<td>-0.8%</td>
<td>-5.9%</td>
</tr>
<tr>
<td>mkhprog</td>
<td>-11.9%</td>
<td>+0.1%</td>
</tr>
<tr>
<td>nucleic2</td>
<td>-14.1%</td>
<td>+0.0%</td>
</tr>
<tr>
<td>partstof</td>
<td>-95.5%</td>
<td>-0.0%</td>
</tr>
<tr>
<td>sphere</td>
<td>-1.5%</td>
<td>+0.0%</td>
</tr>
</tbody>
</table>

... and 72 more programs

<table>
<thead>
<tr>
<th></th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-95.5%</td>
<td>-10.9%</td>
</tr>
<tr>
<td></td>
<td>-28.2%</td>
<td>-12.1%</td>
</tr>
<tr>
<td></td>
<td>+3.5%</td>
<td>+0.5%</td>
</tr>
<tr>
<td></td>
<td>+2.2%</td>
<td>+2.8%</td>
</tr>
<tr>
<td></td>
<td>-6.0%</td>
<td>-0.3%</td>
</tr>
<tr>
<td></td>
<td>-2.2%</td>
<td>-1.4%</td>
</tr>
</tbody>
</table>

#### Table 3. Optimisation of the programs from Benchmarks Game

<table>
<thead>
<tr>
<th>Library</th>
<th>λ1</th>
<th>Thnk1</th>
<th>Benchmark</th>
<th>Alloc Δ</th>
</tr>
</thead>
<tbody>
<tr>
<td>attoparsec</td>
<td>32.8%</td>
<td>19.3%</td>
<td>benchmarks</td>
<td>-7.1%</td>
</tr>
<tr>
<td>binary</td>
<td>16.8%</td>
<td>0.9%</td>
<td>build</td>
<td>-0.2%</td>
</tr>
<tr>
<td>bytestring</td>
<td>5.3%</td>
<td>4.3%</td>
<td>boundcheck</td>
<td>-6.6%</td>
</tr>
<tr>
<td>cassava</td>
<td>26.4%</td>
<td>9.8%</td>
<td>benchmarks</td>
<td>-0.7%</td>
</tr>
</tbody>
</table>

#### Table 4. Analysis and optimisation results for hackage libraries

<table>
<thead>
<tr>
<th>Program</th>
<th>LOC</th>
<th>GHC Alloc Δ</th>
<th>GHC RT Δ</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No hack</td>
<td>Hack</td>
<td>No hack</td>
</tr>
<tr>
<td>anna</td>
<td>5740</td>
<td>-1.6%</td>
<td>-1.5%</td>
</tr>
<tr>
<td>cacheprof</td>
<td>1600</td>
<td>-1.7%</td>
<td>-0.4%</td>
</tr>
<tr>
<td>fluid</td>
<td>1579</td>
<td>-1.9%</td>
<td>-1.9%</td>
</tr>
<tr>
<td>gamtet</td>
<td>1933</td>
<td>-0.5%</td>
<td>-0.1%</td>
</tr>
<tr>
<td>parser</td>
<td>2379</td>
<td>-0.7%</td>
<td>-0.2%</td>
</tr>
<tr>
<td>veritas</td>
<td>4674</td>
<td>-1.4%</td>
<td>-0.3%</td>
</tr>
</tbody>
</table>

#### Table 5. Compilation with optimised GHC


6 [http://benchmarksgame.alioth.debian.org/](http://benchmarksgame.alioth.debian.org/)


7.2 Real-world programs

To test our analysis and the cardinality-powered optimisations on some real-world programs, we chose four continuation-heavy libraries from the hackage repository attoparsec, a fast parser combinator library, binary, a lazy binary serialisation library, bytestring, a space-efficient implementation of byte-vectors, and cassava, a CSV parsing and encoding library.

These libraries come with accompanying benchmark suites, which we ran both for the baseline compiler and the cardinality-powered one. Table 4 contains the ratios of syntactic one-shot lambdas and used-once thunks for the libraries, as well relative improvement in memory allocation for particular benchmarks. Since we were interested only in the absolute improvement against the state of
the art, we made our comparison with respect to the contemporary version of (hacked) baseline GHC. The encouraging results for attoparce are explained by its relatively high ratio of one-shot lambdas, which is typical for parser combinator libraries.

GHC itself is a very large Haskell program, written in a variety of styles, so we compiled it with and without cardinality-powered optimisations, and measured the allocation and runtime improvement when using the two variants to compile several programs. The results are shown in Table 5. As in the other cases, we get modest but consistent improvements.

8. Related Work

8.1 Abstract interpretation for usage and absence

The goal of the traditional usage/absence analyses is to figure out which parts of the programs are used, and which are not (Peyton Jones and Partain 1994). This question was first studied in the late 80’s, when an elegant representation of the usage analysis — inferring the usage of free variables in a usage signature. Moreover our formal underpinning is quite different to their (denotational) approach, underpinning is quite different to their (denotational) approach, our approach deals very naturally with absence, and with product types such as pairs, which are ubiquitous. Type-based approaches do not do so well here.

In short, an analysis-based approach has proved much simpler intellectually than the type-based one, and far easier to implement. One might wonder if a clever type system might give better results intellectually than the type-based one, and far easier to implement. One might wonder if a clever type system might give better results than the type-based approach deals very naturally with absence, and with product types such as pairs, which are ubiquitous. Type-based approaches do not do so well here.

In short, an analysis-based approach has proved much simpler intellectually than the type-based approach. One might wonder if a clever type system might give better results than the type-based approach. One might wonder if a clever type system might give better results than the type-based approach.

8.2 Type-based approaches

The notion of “single-entry” thunks and “one-shot” lambdas is reminiscent of linear types (Girard 1995; Turner and Wadler 1999), a similarity that was noticed very early (Lauchbury et al. 1993). Linear types per se are far too restrictive (see, for example, Wansbrough and Peyton Jones 1999) but the idea of using a type system to express usage information inspired a series of “once upon a type” papers (Gustavsson 1998; Turner et al. 1995 Wansbrough 2002; Wansbrough and Peyton Jones 1999).

Alas, a promising idea turned out to lead, step by step, into a deep swamp. Firstly, subtyping proved to be essential, so that a function that used its argument once could have a type like Int → Int, but still be applied to an argument x that used many times and had type Intω (Wansbrough and Peyton Jones 1999). Then usage polymorphism proved essential to cope with currying: “[Using the monomorphic system] in the entirety of the standard libraries, just two thunks were annotated as used-once” (Wansbrough 2002 3.7). Gustavsson advocated bounded polymorphism to gain greater precision (Gustavsson and Svenningsson 2001), while Wansbrough extended usage polymorphism to data types, sometimes resulting in data types with many tens of usage parameters. The interaction of ordinary type polymorphism with all these usage-type features was far from straightforward. The inference algorithm for a polymorphic type system with bounds and subtyping is extremely complex. And so on. Burdened with these intellectual and implementation complexities, Wansbrough’s heroic prototype in GHC (around 2,580 LOC of brand-new code; plus pervasive changes to thousands of lines of code elsewhere) turned out to be unsustainable, and never made it into the main trunk.

Our system sidesteps these difficulties entirely by treating the problem as a backwards analysis like strictness analysis, rather than as a type system. This is what gives the simplicity to our approach, but also prevents it from giving “rich” demand signatures to third- and higher-order functions: our usage types can account uniformly only for the first- and second-order functions, thanks to call demands.

For example what type might we attribute to

\[ f \times g = g \times \]

The usage of x depends on the particular g in the call, so usage polymorphism would be called for. This is indeed more expressive but it is also more complicated. We deliberately limit precision for very higher-order programs, to gain simplicity.

At some level abstract interpretation and type inference can be seen as different sides of the same coin, but there are some interesting differences. For example, our LETDN and LETUP rules are explicit about information flow; in the former, information flows from the definition of a function to its uses, while in the latter the flow is reversed. Type systems use unification variables to allow much richer information flow — but at the cost of generating constraints involving subtyping and bounds that are tricky to solve.

Another intriguing difference is in the handling of free variables:

\[ \text{let } f = \lambda x. y + x \text{ in if } b \text{ then } f \ 1 \text{ else } y \]

How many times is the free variable y evaluated in this expression? Obviously just once, and LETDN discovers this, because we unleash the demand on y at f’s call site, and lub the two branches of the if. But type systems behave like LETUP: compute the demand on f (namely, called once) and from that compute the demand on y. Then combine the demand on y from the body of the let (used at most once), and from f’s right hand side (used at most once), yielding the result that y is used many times. We have lost the fact that the two uses come from different branches of the conditional. The fact that our usage signatures include the \( \varphi \) component makes them more expressive than mere types — unless we extend the system yet further with an polymorphic effect system (Hage et al. 2007) Holdemans and Hage 2010. Moreover, the analysis approach deals very naturally with absence, and with product types such as pairs, which are ubiquitous. Type-based approaches do not do so well here.

In short, an analysis-based approach has proved much simpler intellectually than the type-based one, and far easier to implement. One might wonder if a clever type system might give better results in practice, but Wansbrough’s results (mostly zero change to allocation: one program allocated 15% more, one 14% less (Wansbrough 2002)) were no more compelling than those we report. Our proof technique does however share much in common with Wansbrough and Gustavsson’s work, all three being based on an operational semantics with an explicit heap.

One other prominent type-based usage system is Clean’s uniqueness types (Barends and Smetsers 1996). Clean’s notion of uniqueness is, however, fundamentally different to ours. In Clean a unique-typed argument places a restriction on the caller (to pass the only copy of the value), whereas for us a single-entry argument is a promise by callee (to evaluate the argument at most once).

8.3 Other related work

Call demands, introduced in this paper, appear to be related to the notion of applicativeness, employed in the recent work on relevance typing (Holdemans and Hage 2010). In particular, applicativeness means that an expression either “guaranteed to be applied to an argument” (S), or “may not be applied to an argument” (L). In this terminology S corresponds to a “strong” version of our demands \( C^\omega(d) \), which requires \( d \subseteq U \), and L is similar to our U. The seq-like evaluation of expressions corresponds to our demand HU. However, neither call- nor thunk-cardinality are captured by the concept of applicativeness.
Abstract counting or sharing analysis conservatively determines which parts of the program might be used by several components or accessed several times in the course of execution. Early work employed a forward abstract interpretation framework [Goldberg [1987], Hudak [1986]]. Since the forward abstract interpreter makes assumptions about arguments of a function it examines, the abstract interpretation can account for multiple combinations of those and may, therefore, be extremely expensive to compute.

Recent development on the systematic construction of abstract interpretation-based static analyses for higher-order programs, known as abstracted abstract machines (AAM), makes it straightforward to derive an analyser from an existing small-step operational semantics, rather than come up with an ad-hoc non-standard one [Van Horn and Might [2010]]. This approach also greatly simplifies integration of the counting abstract domain to account for sharing [Might and Shivers [2006]]. However, the abstract interpreters obtained this way are whole-program forward analysers, which makes them non-modular. It would be, however, an interesting future work to build a backwards analysis from AAM.

9. Conclusion
Cardinality analysis is simple to implement (it added 250 lines of code to a 140,000 line compiler), and it gives real improvements for serious programs, not just for toy benchmarks; for example, GHC itself (a very large Haskell program) runs 4% faster. In the context of a 20-year-old optimising compiler, a gain of this magnitude is a solid win.

Acknowledgements We are grateful to Johan Tibell for the suggestion to use benchmark-accompanied hackage libraries and the cabal bench utility for the experiments in Section 7.2. We also thank the POPL’14 reviewers for their useful feedback.

References


Optional Appendices

In the optional appendices we provide detailed proofs of key lemmas and theorems for the soundness of the cardinality analysis and optimisations it enables. Appendix A provides typing rules for stacks and heaps and proves the soundness of the analysis (Section 4). Appendix B contains a proof of Theorem 5.1 which connects the counting semantics \( \rightarrow \) (Figure 5) with the optimised semantics \( \Rightarrow \) (Figure 6). It also provides a proof sketch of the let-in float improvement (Theorem 5.3).

A. Soundness (Section 4)

A.1 Stack and heap typing for analysis safety

Definition A.1 (Configuration typing). We write \( P \vdash (H : e \in S) \) to mean that there exist \( d, \tau, \varphi_1, \) and \( \varphi_2 \) such that \( P \vdash e \downarrow d \Rightarrow (\tau : \varphi_1) \) and \( P \vdash S \downarrow (d, \tau) \Rightarrow \varphi_2 \) and \( P \vdash H \sim (\varphi_1 \& \varphi_2) \) according to the heap and stack typing rules of Figure 9.

Figure 9 explains how we type stacks and heaps. The judgement \( P \vdash S \downarrow (d, \tau) \Rightarrow \varphi \) intends to identify the \( \tau \)-usage environment of the stack \( S \), given that the argument that we intend to place in the hole of the stack has type \( \tau \) when being pressed with demand \( d \). Rule SHU deals with the case when we press no demand on the hole of the stack -- consequently the stack must be empty! Rule SARR deals with the case when the stack demands the application of the expression in the hole to an argument and hence the shape of the stack has to be \( (\bullet : y) : S \). The corresponding demand that this particular stack expresses is \( C^1(d) \) where \( d \) is the demand expressed by the rest of the stack. The following three rules (SUPDUP, SUPDUPABS, and SUPDDN) correspond to the flavors of LETDn that we encountered in the typing rules. If we encounter a stack \( \#(x, n) : S \) then what is the demand that is placed on \( x \)? In the continuation \( S \) the variable \( x \) will be immediately used with some demand \( d \) but it might be that the continuation induces further calls to \( x \) which end up pressing an additional \( m * d_n \). In total the demand that this stack presses on the hole is \( d \& m * d_n \) – and it must be the case that the multiplicity on the stack \( n \) be higher that the indirect multiplicity in \( S \ (m) \), plus \textit{one}, for the immediate pressure on the top of the stack. This is in-line with our intuition that the only way we can exercise more pressure than just a linear \( C^1(d) \) on a function is via the heap: in the continuation we could potentially be immediately calling the function but we might as well be calling it indirectly later on. Rule SUPDUPABS is of similar flavor, only simpler, since the indirect pressure on \( x \) is just \( A \).

The SUPDUP and SUPDUPABS rules deal with demand on \( x \) being gathered up from the continuation of the execution, but rule SUPDDN is rather different: If \( x \) is bound with a transformer in \( P \) then we -- in effect -- treat it as if the expression bound by \( x \) is inlined so we only gather the \( \varphi \) from the continuation and check that the multiplicity of \( x \) is sufficient.

Rule SCASE is interesting too. The stack has the shape of a case elimination branch. If there exists a demand \( d \), such that the rhs \( e \) can be typed with it, giving \( (\tau : \varphi_1) \) and the stack, when pressed with \( d \), can give \( \varphi_2 \), then we can simply return \( \varphi_1 \& \varphi_2 \). In this case the demand pressed on the hole of the stack can be any \( dp \subseteq U(\varphi_1(x), \varphi_1(y)) \).

The heap typing judgement \( P \vdash H \sim \varphi \) ensures that the heap \( H \) has enough multiplicity to withstand the pressure that \( \varphi \) will exercise. Rules HPVARABS and HPEMPTY are boring. However HPVARUP ensures that if \( \varphi \) needs to press \( m * d \) on \( x \) then \( i \) \( x \) must have enough multiplicity in the heap, but also that \( ii \) the expression or value bound by \( x \) can be checked at this demand yielding a new \( \varphi_1 \). Finally, \( iii \) the remaining heap must have enough multiplicity to withstand the newly unleashed demand from \( \varphi_1 \).

Rule HPVARDN is simpler: checks that (i) the multiplicity of \( x \) in the heap is high enough, (ii) the transformer is well-formed for the bound expression, and (iii) the expression can indeed be typechecked in the demand that \( \varphi \) presses.

With these definitions in place we can prove the generalised safety statement, Lemma 4.3 which is needed for the proof of Theorem 4.2.

A.2 Soundness theorems

The partial order \( \sqsubseteq \) and the least upper bound \( \sqcup \) are defined for usage types naturally:

\[
\tau_1 \sqsubseteq \tau_2 \iff (\tau_1 \sqcup \tau_2) = \tau_2
\]

For usage environments \( \varphi \) the partial order is defined as a pointwise lifting of partial order on multi-terms in their codomains (assuming each \( \varphi \) is predetermined with \( A \) by default).

Lemma A.1 (Monotonicity of usage typing). If the transformer environment \( P \) consists of monotone functions and \( P \vdash e \downarrow d \Rightarrow \)
\(\langle \tau ; \varphi \rangle\) and \(d' \subseteq d\) then \(P \vdash e \downarrow d' \Rightarrow \langle \tau' ; \varphi' \rangle\) and \(\tau' \subseteq \tau\) and \(\varphi' \subseteq \varphi\).

**Proof.** The intuition is that if we use an expression “less” than how it was originally typed, then the annotations in it are still adequate, and we get smaller types and environments out.

The proof goes by induction on the typing derivation.

- Case **TVARDN** follows by monotonicity of the transformer and monotonicity of the operations on usage environments.
- Case **TVARUP** is trivial.
- Case **TLAM** is easy application of the induction hypothesis, and then either **TLAM** or **TLAMHU**. Note that this relies on the non-deterministic choice of return type of **TLAMHU** which lets us choose the same type as the **TLAM** used for typing the \(\lambda\)-abstraction.
- Case **TLAMHU** is straightforward.
- Case **TPAIR** and **TCASE** are easy applications of the induction hypothesis.
- Case **TLTEN** goes by induction hypothesis for \(e_2\), noting that \(g\) is monotone by the assumption \(P \vdash e_1 : \rho\).
- Case **TLTUP** goes by induction hypothesis and then applying either **TLTEN** or **TLTEN**.
- Case **TLTABS** follows by induction hypothesis and **TLTEN**.

\[\square\]

**Lemma A.2** (Discrete usage signatures are well-formed). If

\[e = \lambda^{n_1} x_1 \ldots \lambda^{n_k} x_k . e_1 , n_1 , \ldots , n_k > 0\]

\[P \vdash e \downarrow U \Rightarrow \langle \tau_1 ; \varphi_1 \rangle\]

\[\langle \tau_0 ; \varphi_0 \rangle = \langle \varphi_1 (P) \rightarrow \tau_1 ; \varphi_1 \setminus \tau \rangle\]

\[\varphi = \lambda \delta . \text{transform}(\langle k ; \tau_0 ; \varphi_0 \rangle, d)\]

then \(P \vdash e : \varphi\).

**Proof.** By the typing rule **WFTRANS**, we need to show that

\[\forall d_1 , d_2 , d_3 \subseteq d_3 \Rightarrow T_{\delta}^{d_1} \subseteq T_{\delta}^{d_2} \land \Phi_{\delta}^{d_1} \subseteq \Phi_{\delta}^{d_2}\]

\[\forall d , \varphi , \tau . \left( P \vdash e \downarrow d \Rightarrow \langle \tau ; \varphi \rangle \right) \Rightarrow \tau \subseteq T^{d} \land \varphi \subseteq \Phi^{d}\]

The proof of (5) is straightforward, since \(\varphi\) is a monotonic step-function.

For the second part, let us first define the threshold \(d_3\) as \(d_3 = C^{\lambda}(k - f o l d \ldots C^1(U) \ldots)\). We remark that, by consecutive applications of rule **TLAM**, we can obtain:

\[P \vdash e \downarrow d_3 \Rightarrow \langle \tau_0 ; \varphi_0 \rangle\]

Let us assume that \(P \vdash e \downarrow e \Rightarrow \langle \tau_d ; \varphi_d \rangle\). We show that \(\tau_d \subseteq \tau_0\) and \(\varphi_d \subseteq \varphi_0\) by induction on the number of \(\lambda\)s.\(^{3}\)

- If \(k = 0\) then it can only be that \(d \subseteq U\) and the result follows by monotonicity (**Lemma A.1**).
- If \(k = l + 1\) then we have several cases on the shape of \(d\).
  - \(d = U(d_1^l . d_1^r)\). This can only happen if \(d \subseteq HU\) and rule **TLAMHU** was used, otherwise the lambda is not typeable at all. But \(HU \not\subseteq d\) anyway so this case follows by monotonicity.
  - \(d = HU\). This is similar as above.
  - \(d = C^m(d_1)\). In this case we can invert the **TLAM** rule used to type \(e = \lambda^m . e_0\) with \(C^m(d_1)\), \(n \geq m\), and apply the induction hypothesis for the body \(e_0\). We get back a pair \(\langle \tau ; \varphi \rangle\). If \(m = 1\) then we are easily done by the induction hypothesis. If \(m = \omega\) then it is definitely the case that \(d \not\subseteq \tau\) and hence we multiply both transform results by \(\omega\) and we are done, using the induction hypothesis[^3].
  - \(d = U\). We observe that \(d \subseteq C^\omega(U)\) and hence the case follows as the previous one using inversion on **TLAM**.

\[\square\]

**Lemma A.3** (Analysis produces well-typed terms (**Lemma 4.1**)).

If \(P \vdash e \downarrow d \Rightarrow \langle \tau ; \varphi \rangle\) then \(P \vdash e \downarrow d \Rightarrow \langle \tau ; \varphi \rangle\).

**Proof.** The proof is by induction on the height of the derivation.

\[\square\]

Note that we can guarantee the same result by choosing a different more expressive transform that only infinitizes the previous types but not the current one, yielding tighter types, but we have not done that for simplicity.
• Case CASE. By induction hypothesis,
  \[ P \vdash e_d \Downarrow \Rightarrow \langle \tau ; \varphi_d \rangle \]
  \[ P \vdash e_u \Downarrow U(\varphi(x), \varphi(y)) \Rightarrow \langle \omega ; \varphi_u \rangle, \]
  so we can directly apply the typing rule TCASE.

• Case LETUP By the induction hypothesis, we have
  \[ P \vdash e_2 \Downarrow d \Rightarrow \langle \tau ; \varphi_2 \rangle \]
  \[ n + d_C = \varphi_2(x) \]
  \[ P \vdash e_1 \Downarrow d_s \Rightarrow \langle \omega ; \varphi_1 \rangle \]
  The proof for this case is completed by applying the typing rule TLETUP with \( m = n \).

• Case LETUPABS Straightforward by the rule TLETUPABS.

• Case LETDN. In this case we have that:
  \[ P \vdash \text{let } x = \lambda \gamma^{l:k}. e_1 \text{ in } e_2 \Downarrow d \Rightarrow \langle \tau ; (\varphi_2(x)) \rangle \]

Let us call the resulting RHS term \( \epsilon = \lambda \gamma^{l_1} \ldots \lambda \gamma^{l_n} \cdot e_1 \). By inversion we have that:
  \[ P \vdash e_1 \Downarrow U \Rightarrow \langle \tau_1 ; \varphi_1 \rangle \]
  \[ P \vdash e_2 \Downarrow d \Rightarrow \langle \tau ; \varphi_2 \rangle \]
  Hence it is easy to show by induction and monotonicity that
  \[ P \vdash \epsilon \Downarrow (C^n(\tau_1 \ldots )) \Rightarrow \langle \omega ; \varphi \rangle. \]
  Moreover we know that \( n \geq \mu(\varphi_2(x)) \).

• Case LETDNABS. Similar to the case LETDN.

\[ \square \]

Lemma A.4 (Value splitting (Lemma 4.4)). If \( P \vdash \nu \Downarrow (d_1 \& d_2) \Rightarrow \langle \tau ; \varphi \rangle \) then there exists a split \( \nu' \) such that:
  \[ P \vdash \nu_1 \Downarrow d_1 \Rightarrow \langle \tau_1 ; \varphi_1 \rangle \]
  \[ P \vdash \nu_2 \Downarrow d_2 \Rightarrow \langle \tau_2 ; \varphi_2 \rangle \]
  and moreover \( \tau_1 \subseteq \tau \) and \( \varphi_1 \subseteq \varphi \).

Proof. This is an extremely important property. It says that for a value (and only for values!) the unleashed environment is additive with respect to the placed demands. This allows one to use a variable directly (by dereferencing a variable and using it with a particular continuation) and indirectly in the continuation! Here is the proof, by case analysis on the shape of the value \( \nu \):

• Case \( \nu = (x, y) \). In this case without loss of generality assume that:
  \( d_1 = U(d_1', d_2') \) and \( d_2 = U(d_1', d_2') \).
  If one of them is a call demand then their \& is not defined, and if one of them is a \( U \) or \( \nu \) then that is equivalent to some \( U(d_1', d_2') \) in terms of how the result will be typed. The result can follow by monotonicity of the \& operation and Lemma A.5 (see below).

• Case \( \nu = \lambda x. \epsilon \). In this case, if one of \( d_1 \) or \( d_2 \) is less or equal to \( \nu \), assume \( d_1 \), then the split is by choosing \( n_1 = 0 \) and \( n_2 = n \). The \( n_1 = 0 \) split uses the TLAMHU rule assigning the same type as the other split assigns. The other split merely uses the typing rule that was originally used to type \( \nu \). If on the other hand \( n_1 \) nor \( n_2 \) is less or equal to \( \nu \) then they cannot be used demands either (because their \& would not be defined). Assume then without loss of generality that:
  \( d_1 = C^n(\nu_1) \) and \( d_2 = C^n(\nu_2) \), where \( \nu_1 \) and \( \nu_2 \) are the results of typing \( \nu \) with \( d_1 \) and \( d_2 \). Let us use the split induced by \( d_1 \) and \( d_2 \), that is \( n = n_1 + n_2 \). From typing the body \( e \) with \( d_1 \) we will get:
  \[ \langle \varphi_1(x) \rightarrow \tau_1 ; n_1 \& \varphi_1 \rangle \]
  and similarly:
  \[ \langle \varphi_2(x) \rightarrow \tau_2 ; n_2 \& \varphi_2 \rangle \]
  as required. Moreover we need to show that:
  \[ \nu_1 \& \varphi_1 \& \nu_2 \& \varphi_2 \]
  By monotonicity it suffices to show that:
  \[ \nu_1 \& \varphi_1 \& \nu_2 \& \varphi_2 \]

Lemma A.5 (Variable demand splitting). Assume that the transformer environment \( P \) is monotone. If \( P \vdash x \Downarrow (d_1 \& d_2) \Rightarrow \langle \tau ; \varphi \rangle \) then \( P \vdash x \Downarrow d_1 \Rightarrow \langle \tau_1 ; \varphi_1 \rangle \) and \( P \vdash x \Downarrow d_2 \Rightarrow \langle \tau_2 ; \varphi_2 \rangle \) and \( \varphi_1 \& \varphi_2 \subseteq \varphi \).

Proof. If \( x \not\in \text{dom}(P) \) then the result is trivial. If \( x \in \text{dom}(P) \) then there is a transformer \( (x, \epsilon) \in P \). First of all let us examine the case where either \( d_1 \) or \( d_2 \) is \( A \). Without loss of generality assume \( d_1 = A \). In this case the result is trivial since \( \varphi_2 = \epsilon \) and \( \varphi = \varphi_1 \). Assume instead that \( d_1 = n_1 \& d_1 \) and \( d_2 = n_2 \& d_2 \). In this case it suffices to show that:
  \[ n_1 \& \varphi_1 \& n_2 \& \varphi_2 \subseteq (n_1 + n_2) \& \varphi_1 \& \varphi_2 \subseteq \varphi \]
  However by monotonicity we know that:
  \[ n_1 \& \varphi_1 \& n_2 \& \varphi_2 \subseteq n_1 \& \varphi_1 \& n_2 \& \varphi_2 \subseteq n_1 \& \varphi_1 \& n_2 \& \varphi_2 \subseteq d_1 \]

Lemma A.6 (Single-step safety (Lemma 4.3)). Assume that \( P \vdash H \Rightarrow \langle H_1 ; e_1 \& S_1 \rangle \).

Proof. By induction on the height of the derivation \( P \vdash H \Rightarrow \langle H_1 ; e_1 \& S_1 \rangle \). We proceed by case analysis on the rule used for \( \Rightarrow \) in the uninstrumented semantics.

• Case ELET. We have three cases to consider, depending on whether rule TLETUP, TLETUPABS, or TLETDN is used.

• Case LETUP. In this case we have that:
  \[ P \vdash \text{let } x \equiv e_1 \text{ in } e_2 \Downarrow d \Rightarrow \langle \tau ; \varphi_1 \& \varphi_2 \rangle \]
  \[ n \leq m \]

• Case LETDNABS. Similar to the case LETDN.

This is easy to show using the fact that \( \omega \& d \equiv d \& d \equiv d \& d \).

The rule ELET fires in the uninstrumented semantics as well, giving us a new heap \( H; [x \Rightarrow \text{Exp}(e_1)] \). By using HP-VARUP we can conclude:
  \[ P \vdash H; [x \Rightarrow \text{Exp}(e_1)] \Rightarrow \varphi_2, \tau \& \varphi \& \varphi_S \]
from (17), (19), (21). Hence, from (18), (22), and (20) we conclude that the resulting configuration is well-typed.

- Case TLETUAbS. Similar but simpler than the case for TLETU.

- Case TLETDN. In this case we have that:
  \[ P \vdash \text{let } x \equiv e_1; e_2 \downarrow d \Rightarrow (\tau; \phi_2) \]
  \( n \leq m \quad (23) \)
  \[ P \vdash e_1 \downarrow d_1 \Rightarrow (\tau; \phi_1) \]
  \[ P \vdash e_1 : \phi_1 \quad (24) \]
  \[ P, (x : \theta) \vdash e_2 \downarrow d \Rightarrow (\tau; \phi_2; (x:d_1)) \]
  \[ d_1 \subseteq n + d_1 \quad (25) \]

  Moreover:
  \[ P \not\vdash S \downarrow (d, \tau) \Rightarrow \varphi_S \quad (26) \]
  \[ P \vdash H \sim \varphi_2 \& \varphi_S \quad (27) \]

  The rule ELET fires in the instrumented semantics as well, giving us a new heap \( H, [x \mapsto \text{Exp}(e_1)] \). We need to use HPVARDN to deduce that:
  \[ P, (x : \rho) \vdash H, [x \mapsto \text{Exp}(e_1)] \sim (\varphi_2; (x : d_1) \& \varphi_S) \quad (28) \]

  which follows from \( (29), (26), (24), (25) \). Moreover, from \( (29) \) and the observation that \( x \not\in \text{fv}(S) \) it is easy to deduce that \( P, (x : \rho) \not\vdash S \downarrow (d, \tau) \Rightarrow \varphi_S \) (simple inductive weakening proof). From this, and (27) and (28) we get that the resulting configuration is well-typed.

- Case ELKPE. In this case we have two cases depending on how the variable was typed.

  - Case TVARUp. In this case we have:
    \[ P \vdash x \downarrow d \Rightarrow (\bullet ; (x : 1 \ast d)) \quad (30) \]
    where \( x \not\in \text{dom}(P) \). Moreover:
    \[ P \not\vdash S \downarrow (d, \bullet) \Rightarrow \varphi_S \quad (31) \]
    \[ P \vdash H, [x \mapsto \text{Exp}(e)] \sim (\varphi_S)_{\setminus x}, (x : 1 \ast d \& \varphi_S(x)) \quad (32) \]

    We have two cases: if \( \varphi_S(x) = A \) then we only press \( 1 \ast d \) on \( x \). If \( \varphi_S(x) = m \ast d_1 \) then we press \( (1 + m) \ast (d \& d_1) \) on \( x \). Let us work with the latter case first:
    \[ P \vdash H, [x \mapsto \text{Exp}(e)] \sim (\varphi_S)_{\setminus x}, (x : (1 + m) \ast (d \& d_1)) \quad (33) \]

    By inverting HPLETUP, it must be then:
    \[ n \geq m + 1 \quad (34) \]
    \[ P \vdash e_1 \downarrow (d \& d_1) \Rightarrow (\tau ; \varphi_1) \quad (35) \]

    To finish the case by SUpdUP we need to show that:
    \[ P \not\vdash (\#(x, n) : S) \downarrow (d \& d_1, \tau_1) \Rightarrow \varphi_S \quad (36) \]

    which will be the case if we show that:
    \[ P \vdash S \downarrow (d, \bullet) \Rightarrow (\varphi_S)_{\setminus x}, (x : m \ast d_1) \]

    and also: \( n \geq 1 + m \). The first is exactly (33) and the second is just (36).

    If it was the case that \( \varphi_S(x) = A \) then we could similarly use SUpdUPABBS.

  - Case TVARDN. In this case we have that:
    \[ P \vdash x \downarrow d \Rightarrow (T^d ; \Phi^d \& (x : 1 \ast d)) \quad (37) \]

Let us assume that bindings are not recursive so \( x \not\in \text{dom}(\Phi^d) \). Moreover:

\[ P \not\vdash S \downarrow (d, T^d) \Rightarrow \varphi_S \quad (38) \]
\[ P \vdash H, [x \mapsto \text{Exp}(e)] \sim (\Phi^d \& (\varphi_S)_{\setminus x}, (x : 1 \ast d \& \varphi_S(x))) \quad (39) \]

Let us assume that \( \varphi_S(x) = m \ast d_1 \) (the case where \( \varphi_S(x) = A \) is easier). By rule HPLETDN this also means that:

\[ P \vdash H \sim \Phi^d \& (\varphi_S)_{\setminus x} \]

and moreover \( P \vdash e \downarrow (d \& d_1) \Rightarrow (\tau_1 ; \varphi_1) \) – hence by monotonicity it is also the case that \( P \vdash e \downarrow d \Rightarrow (\tau_2 ; \varphi_2) \), and in fact such that \( \varphi_1 \subseteq \Phi^d \) and \( \tau_2 \subseteq T^d \).

Now for the right hand side the environment from the expression is \( \varphi_1 \) (we press the demand \( d \)). The environment for the stack-typing is the one we get from: \( P \not\vdash S \downarrow (d, T^d) \Rightarrow \Phi^d \). Hence we need to show that: \( P \vdash H \sim \varphi_1 \& \varphi_2 \& (\varphi_S)_{\setminus x} \) and the result follows from monotonicity.

- Case ELKPV. Again we have two cases depending on how the variable is typed.

  - Case TVARUp. In this case we have:
    \[ P \vdash x \downarrow d \Rightarrow (\bullet ; (x : 1 \ast d)) \quad (40) \]

    where \( x \not\in \text{dom}(P) \). Moreover:
    \[ P \not\vdash S \downarrow (d, \bullet) \Rightarrow \varphi_S \quad (41) \]
    \[ P \vdash H, [x \mapsto \text{Val}(v)] \sim (\varphi_S)_{\setminus x}, (x : 1 \ast d \& \varphi_S(x)) \quad (42) \]

    Again we have two cases depending on \( \varphi_S(x) \):

    - Case \( \varphi_S(x) = m \ast d_1 \). We know that \( m \geq 1 + m \) and hence the expression can take a step in the counting semantics. From (43) we get that:
      \[ P \vdash H \sim (\varphi_S)_{\setminus x} \& \varphi_v \quad (44) \]

      where \( P \vdash v \downarrow (d \& d_1) \Rightarrow (\tau ; \varphi_v) \). Hence it must be that:
      \[ P \vdash H \sim (\varphi_S)_{\setminus x} \& \varphi_v \quad (45) \]

      By Lemma [A.4] we get that: \( P \vdash v_1 \downarrow d \Rightarrow (\tau_1 ; \varphi_1) \) and \( P \vdash v_2 \downarrow d_1 \Rightarrow (\tau_2 ; \varphi_2) \) such that \( \varphi_1 \& \varphi_2 \subseteq \varphi_v \), \( \tau_1 \subseteq \tau \) and \( \tau_2 \subseteq \tau \) for some \( v_1 \) and \( v_2 \) with \( \text{split}(v) = (v_1, v_2) \). To finish the case we need to show that:
      \[ H \sim \varphi_1 \& \varphi_2 \& (\varphi_S)_{\setminus x} \]

      which follows from (45) and strengthening (Lemma [A.7]).

    - Case \( \varphi_S(x) = A \). This case is easy as it induces a trivial split for \( v_1 \) and \( v_2 \) where \( v_1 \) gets a 0 counter if it is a lambda. This reflects the fact that this is never used indirectly in the continuation but only directly in the stack \( S \).

- Case TVARDN. In this case we have:
  \[ P \vdash x \downarrow d \Rightarrow (T^d ; \Phi^d \& (x : 1 \ast d)) \quad (46) \]

  where \( (x : \rho) \in P \). Moreover:
  \[ P \not\vdash S \downarrow (d, T^d) \Rightarrow \varphi_S \quad (47) \]

  and
  \[ P \vdash H, [x \mapsto \text{Val}(v)] \sim (\Phi^d \& (\varphi_S)_{\setminus x}, (x : 1 \ast d \& \varphi_S(x))) \quad (48) \]

  Let us deal with the case when \( \varphi_S(x) = m \ast d_1 \) (the case where \( \varphi_S(x) = A \) is easier).
By inverting rule \( \text{H}_{\text{LETDN}} \) we get:

\[
P \vdash H \sim (\varphi_S)_{\varphi} \land \Phi^d_v
\]

and moreover \( P \vdash \nu \downarrow (d \land d_\nu) \Rightarrow \langle \nu ; \varphi_v \rangle \) (i.e. the \( \nu \) is sufficiently annotated). So the configuration can indeed step and for the right-hand side, by the splitting lemma, we must have: \( P \vdash v_2 \downarrow d \Rightarrow (\tau_2 ; \varphi_2) \) and we must also have \( P \vdash S \downarrow (d, \tau_2) \Rightarrow \varphi_S \). By the well-formedness of the transformer it must be \( \tau_2 \subseteq \tau_\nu^d \) and it also must be \( \varphi_2 \subseteq \Phi^d_v \). Hence by monotonicity \( \varphi_S \subseteq \varphi_2 \) as well. To finish the case we need to show that:

\[
P \vdash H, [x \overset{\nu}{\rightarrow} \text{Val}(v_1)] \sim (\varphi_S)_{\varphi} \land \varphi_2, (x ; \varphi_S(x))
\]

By rule \( \text{H}_{\text{LETDN}} \) it suffices to show two things: First, that \( P \vdash H \sim (\varphi_S)_{\varphi} \land \varphi_2 \) this follows by \( (\cdot) \) and monotonicity. Second, that if \( \varphi_2(x) = d^1 \), \( v_1 \) is still typeable under that \( d^1 \). However by the splitting lemma we know that: \( P \vdash v_1 \downarrow d_\nu \Rightarrow \langle \nu ; \varphi_1 \rangle \) and the result follows by monotonicity since it must be the case that \( d^1 \subseteq \mu m \cdot d_\nu \).

- Case EUPD. Similar to \( \text{ELKPv} \) case.
- Case EBETA. Using the substitution lemma (Lemma \[A.8]\).
- Case EAAPP. Trivial.
- Case EPAIR. Trivial.
- Case EPRED. Using the substitution lemma (Lemma \[A.8]\).

**Lemma A.7** (Heap-typing strengthening). If \( P \vdash H \sim \varphi_1 \) and \( \varphi_2 \subseteq \varphi_1 \) then \( P \vdash H \sim \varphi_2 \).

**Proof.** Easy induction, appealing to the monotonicity of typing lemma.

**Lemma A.8** (Substitution). Assume that \( P \) is monotone and \( P \vdash e \downarrow d \Rightarrow \langle \tau ; \varphi_1 \rangle \) and \( x \notin \text{dom}(P) \). If \( P \vdash y \downarrow \varphi_1(x) \Rightarrow \varphi_2 \) then \( P \vdash e[y/x] \downarrow d \Rightarrow \langle \tau_c ; \varphi_v \rangle \) such that \( \varphi_v \subseteq \varphi_1 \) and \( \varphi_2 \) and \( \tau_c \subseteq \tau \).

**Proof.** By induction on the derivation \( P \vdash e \downarrow d \Rightarrow \langle \tau ; \varphi_1 \rangle \).

- First of all, if \( y \notin \text{dom}(P) \) either, then the result follows easily by a renaming. So we will only be concerned with the case when \( y \in \text{dom}(P) \), in particular \( (y:b) \in P \).
- Case TVARDN. In this case we know that we exercise pressure on is not \( x \) and therefore the result follows trivially (\( y \) is absent).
- Case TVARUP. If the variable is not \( x \) then the result follows trivially (\( y \) is absent). If it is then we have that the pressure on \( x \) is \( (x:1 \cdot d) \). Then \( \varphi_2 = \Phi^d_v \land \Phi^d_y \). For the substituted expression we get that: \( \varphi_v = \varphi_2 \) and \( \tau_c = T^d_v \). Clearly \( T^d_v \subseteq \tau \) and moreover \( \varphi_2 \subseteq \tau \varphi_2 \) as required.
- The rest of the cases are straightforward but somewhat tedious applications of the induction hypothesis and monotonicity of typing. They rely on the following property: If \( \varphi_1(x) = n_1 \cdot d_1 \) and \( \varphi_2(x) = n_2 \cdot d_2 \) then

\[
n_1 \cdot \Phi^d_1 \land n_2 \cdot \Phi^d_2 \subseteq (n_1 + n_2) \cdot \Phi^d_1 + d_2
\]

which follows by the monotonicity of the transformer of \( \varphi_0 \).

### B. Optimisation (Section \[5\])

**Theorem B.1** (Optimised semantics (Theorem \[5.1\])). If \( (H_1; e_1; \sigma) \approx (H_2; e_2; \sigma_2) \) and \( (H_1; e_1; \sigma_1) \rightarrow (H_1; e'_1; \sigma'_1) \) then there exists \( k \in \{0, 1\} \) s.t. \( (H_2; e'_2; \sigma'_2) \Rightarrow^k (H_2; e'_2; \sigma'_2) \) and \( (H_1; e'_1; \sigma'_1) \approx (H_2; e'_2; \sigma'_2) \).

**Proof.** The proof is by case analysis on the \( \Rightarrow \) relation:

- Case ELET. We have two cases to consider. If \( n \geq 1 \) then obvious. If \( n = 0 \) then \( H'_1 = H_1, [x \overset{\nu}{\rightarrow} \text{Exp}(e_1)] \) and \( H'_2 = H_2 \) and \( H'_2 \approx H_2 \) as required.
- Case ELKPE. In this case we have that:

\[
(H_1, [x \overset{\nu}{\rightarrow} \text{Exp}(e_1)] ; x ; \sigma_1) \rightarrow (H_1 ; e ; \#(x, n) ; \sigma_1)
\]

given that \( n \geq 1 \). Then either \( \text{OPT-ELKP} \) or \( \text{OPT-ELKPEO} \) will fire:

- If \( n = \omega \) the result follows trivially.
- If \( n = 1 \) then \( S'_1 = \#(x, 1) ; S_1 \) and \( S'_2 = S_2 \) and by rule \( \text{SSIM2} \) we are done.
- Case ELKPV. By the side condition \( n = m + 1 \) it can only be that \( n = 1 \) or \( n = \omega \). By the heap invariant for \( H_1 \) and an easy induction it has to be that \( n = \omega \). The corresponding rule that can fire in the optimised semantics is \( \text{OPT-ELKPv} \) and the result is trivial.

- Case EUPD. We have that:

\[
(H_1 ; v ; \#(x, n) ; \sigma_1) \rightarrow (H_1, [x \overset{\nu}{\rightarrow} \text{Val}(v_1)] ; v_2 ; \sigma_1)
\]

where \( n = m + 1 \) and \( \text{split}(v) = (v_1, v_2) \). By this last condition it has to be the case that \( n = \omega \) or \( n = 1 \).

- If \( n = \omega \) then rule \( \text{OPT-EUPD} \) gives the result.
- If \( n = 1 \). Then, assume that \( (H_1 ; v ; \#(x, n) ; \sigma_1) \approx (H_2 ; v ; \sigma_2) \) which will happen if \( S_1 \approx S_2 \). However, in this case, \( m = 0 \), which means that it also must be the case that \( (H_1, [x \overset{\nu}{\rightarrow} \text{Val}(v_1)] ; v_2 ; \sigma_2) \approx (H_2 ; v_2 ; \sigma_2) \) so we are done in 0 steps (hence we have \( \Rightarrow \) and not just \( \Rightarrow \) in the statement of the theorem).
- Case EBETA follow directly from rule \( \text{OPT-EBETA} \).
- Case EAAPP follows by \( \text{OPT-EAPP} \).
- Case EPRED and EPREDB and EPAIR follow from rules \( \text{OPT-EPRED} \) and \( \text{OPT-EPAIR} \).

**Theorem B.2** (Let-in float improvement (Theorem \[5.3\])). For any \( H \) and \( S \), if

\[
(H; \text{let } z \equiv e_1 \text{ in } (\text{let } f \equiv \lambda x . e_2) ; S) \Downarrow^N
\]

and \( z \notin \text{FV}(e_2) \), then

\[
(H; \text{let } f \equiv \lambda x . (\text{let } z \equiv e_1 \text{ in } e_2) ; S) \Downarrow^{\leq N}
\]

**Proof sketch:** Let us refer to the first configuration as \( q \) and the second as \( q' \). The proof goes in four stages.

1. It is the case that \( q \) evaluates in two steps to some \( q_1 = (H_1; e_2; S) \) and \( q' \) steps to some \( q_2 = (H_2; e_2; S) \) such that \( H_1 \) and \( H_2 \) are related, written \( H_1 \approx H_2 \). We define \( H_1 \approx H_2 \) iff

\[
H_1 = H_0, [z \overset{\nu}{\rightarrow} e_1], [f_{k_1}^m \lambda x . e], \ldots, [f_{k_2}^m \lambda x . e] \quad H_2 = H_0, [f_{k_1}^m \lambda x . e], \ldots, [f_{k_2}^m \lambda x . e, e_z]
\]

for some \( H_0 \) and \( k \), where \( e_z = (\text{let } z \equiv e_1 \text{ in } e) \); and \( e, e_1 \) and \( z \) are from the statement of the theorem, and
$\sum_{i=1}^{k} n_i = 1$\footnote{\text{The Val(·)/Exp(·) distinction does not affect the core of the proof.}} Now we need to show that $q_2$ will make at most one step more than $q_1$ before they both terminate.

2. Taking $(H_1 \cong H_2)$ and the stacks and expressions being the same for both configurations as an invariant, we show that both configurations will make a step simultaneously, so the invariant is preserved until some $f_k$ is in the configuration focus. Then we pass to the next stage.

3. If $f_k$ is in the focus of both configurations, we consider the stack. If $S = \epsilon$ the case is done. (And so is if $S$ contains a case alternative because both computations will be stuck.) If $S = \#(x, n) : S'$ then we update the heap in both branches in a $\sim$-preserving way, so we are back to stage (2). If $S = (\bullet y) : S'$ then the “optimised” program makes one additional step to allocate $z$, and we pass to the last stage of the proof.

4. For the rest of the execution we can show that the programs will execute in lockstep with a simulation argument taking the invariant almost as in stage (2), but now with $\sum_{i=1}^{k} n_i = 0$ and $z$ being allocated in the second heap too.

$\square$