The following full text is a publisher's version.

For additional information about this publication click this link.
http://hdl.handle.net/2066/75339

Please be advised that this information was generated on 2017-09-25 and may be subject to change.
Collected Size Semantics for Functional Programs over Polymorphic Nested Lists *

O. Shkaravska, M. van Eekelen, A. Tamalet
Institute for Computing and Information Sciences
Radboud University Nijmegen

Abstract. Size analysis is an important prerequisite for heap consumption analysis. This paper is a part of ongoing work about typing support for checking output-on-input size dependencies for function definitions in a strict functional language. A significant restriction for our earlier results is that inner data structures (e.g. in a list of lists) all must have the same size. Here, we make a big step forwards by overcoming this limitation via the introduction of higher-order size annotations such that variate sizes of inner data structures can be expressed.

1 Introduction

Bound on the resource consumption of programs can be used, and are often needed, to ensure correctness and security properties, in particular in devices with scarce resources as mobile phones and smart cards. Both the memory and the time consumption of a program often depend on the sizes of input and intermediate data. Here, we consider size analysis of strict functional programs over polymorphic lists. A size dependency of a program is a size function that maps the size of inputs onto the sizes of the corresponding output. For instance, the typical size dependency for a program append, that appends two lists of length \( n \) and \( m \), is the function \( \text{append}(n, m) = n + m \).

This paper is devoted to collecting size dependencies using multivalued size functions. Multivalued size functions can be defined by conditional multiple-choice rewriting rules [13]. These multivalued size functions are used to annotate types. They make it possible to express that there can be more than one possible output size (like e.g. in the case of inserting an element to a list if it is not there already: the result will either have the same size or it will be one element larger).

Consider e.g. the program insert : \((\alpha \times \alpha \rightarrow \text{Bool}) \times \alpha \times L_n(\alpha) \rightarrow L_{\text{insert}(n)}(\alpha)\) that inserts an element \( z \) of the type \( \alpha \) in a list \( l \), if this list does not contain an element \( z' \) such that the relation \( g(z, z') \) holds:

\[
\begin{align*}
\text{insert}(g, z, l) = \text{match } l \text{ with } & | \text{Nil} \Rightarrow \text{Cons}(z, \text{Nil}) \\
& | \text{Cons}(\text{hd}, \text{tl}) \Rightarrow \text{if } g(z, \text{hd}) \text{ then } l \\
& \quad \text{else } \text{Cons}(\text{hd}, \text{insert}(g, z, \text{tl}))
\end{align*}
\]

* This work is part of the AHA project [16] which is sponsored by the Netherlands Organisation for Scientific Research (NWO) under grant nr. 612.003.511.
Its size dependency \( \text{insert}(n) \) represents the length of the output corresponding to an input of the length \( n \). It is given by (where | separates alternative rewriting rules):

\[
\begin{align*}
\text{insert}(0) & \rightarrow 1 \\
\text{insert}(n) & \rightarrow n | \text{insert}(n-1) + 1
\end{align*}
\]

However, the type system from [13] only covers programs over ‘matrix-like’ structures, e.g. \( L_n(L_m(\alpha)) \) leaving no way to express variate sizes of internal lists. This substantially restricted application of the approach, since the case of programs over lists of lists with variate lengths is the most frequent one.

In this paper, we remove that restriction and generalise the approach to cover all polymorphic programs over lists for which the size(s) of an output depend only the size of first-order inputs. Below, we first introduce the approach using a concrete example. We use an ML-like strict language which is defined in Section 2. In Section 3 we define the type system which allows size variables of higher-order kinds, such that, e.g., a size variable \( M \) in the type \( L_n(L_M(\alpha)) \) represents the size \( M(pos) \) of an internal list depending on its position \( pos \) in the outer list, where \( 0 \leq pos \leq n - 1 \). Moreover, we extend (checking and inferring of) multivalued size functions allowing them to be defined with higher-order rewriting rules. We define soundness and sketch its proof. Section 4 gives a procedure for the generation of polynomial lower and upper bounds and a set of polynomials that covers the function defined by the higher-order rewriting rules. Section 5 relates our work to other resource analysis work.

Informal Sketch of the Approach Consider the function \( \text{concat} \), which given a list of lists appends all the inner lists:

\[
\text{concat}([\vdots]) = \text{match } l \text{ with } | \text{Nil} \Rightarrow \text{Nil} | \text{Cons}(\text{hd}, \text{tl}) \Rightarrow \text{append}(\text{hd}, \text{concat}(\text{tl}))
\]

The expected annotated type for \( \text{concat} \) is \( L_n(L_M(\alpha)) \rightarrow L_{\text{concat}(n,M)}(\alpha) \) where \( n \) and \( M \) are size variables of types \( N \) (naturals) and \( N \rightarrow N \), respectively and its size function \( \text{concat}(n, M) \) is defined by the following rewriting rules

\[
\begin{align*}
\text{concat}(0, M) & \rightarrow 0 & (1) \\
n \geq 1 & \Rightarrow \text{concat}(n, M) \rightarrow M(0) + \text{concat}(n-1, \lambda pos. M(pos + 1)) & (2)
\end{align*}
\]

where the first argument, \( n \), of \( \text{concat} \) is the length of a “master” list of lists and the second argument, \( M \), is a function that returns the size of an element at a given position \( pos \) in the master list. The head of a list is assumed to have position 0.

Consider the following expression: \( \text{concat} \left[ [1, 2, 3], [4, 5] \right] \). Here, \( n = 2 \) and \( M \) is instantiated with a concrete function \( M_0 \) defined in a tabular way: \( M_0(0) = 3, M_0(1) = 2 \) and \( M_0(pos) \) for \( pos \geq 2 \) is arbitrary. We are now interested in calculating the result size defined by \( \text{concat}(2, M_0) \):

\[
\begin{align*}
\text{concat}(2, M_0) & \rightarrow M_0(0) + \text{concat}(1, \lambda pos. M_0(pos + 1)) \\
& \rightarrow 3 + (\lambda pos. M_0(pos + 1))(0) + \\
& \text{concat}(1, 1, \lambda pos'. ((\lambda pos. M_0(pos + 1))(pos' + 1))) \\
& = 3 + M_0(0 + 1) + \text{concat}(0, \lambda pos'. M_0((pos' + 1) + 1)) \\
& = 3 + M_0(1) + \text{concat}(0, \lambda pos'. M_0(pos' + 2)) \\
& = 3 + M_0(1) + 0 = 3 + 2 + 0 = 5
\end{align*}
\]
However, a user often prefers to deal with closed-form size dependencies (i.e., without recursion) rather than with size functions given in the form of rewriting rules. We cannot always infer precise closed-forms but we will show that we can infer closed forms for polynomial lower and upper bounds of multivalued size functions. We focus on piecewise polynomial bounds, i.e., bounds that can be described by a finite number of polynomial families. Given a set of conditional multiple-choice rewriting rules, we show how to infer lower and upper bounds that define an indexed family of polynomials. Such a family fully covers the size function induced by the rewriting rules, in the sense that for each input, there is a polynomial in the family that describes the size of the output.

In order to generate such bounds for general nested lists we need a nontrivial extension of the method described in [13]. In that work, size variables in rewriting rules are instantiated with finite numbers, whereas in this work we need to instantiate size variables of higher kinds with finite multivalued maps.

Here, we extend this methodology by instantiating size variables like $M$ in $\text{concat}(n, M)$, of higher-order kinds, with finite multivalued maps. Consider how to infer size bounds for $\text{concat}$. Assume that the size of inner lists is at most $n'$. Then, the expected inferred result is $\{j\}_{0 \leq j \leq nn'}$ “covering” the range of $\text{concat}(n, M)$.

First, note that for fixed $n$ and $n'$ the map $M$ will be finite and is “covered” by a finite multivalued map $\phi$ that sends any position to $\{0,\ldots,n'\}$. For instance, on $n = 2$ and $n' = 3$ the finite-multivalued-map variable $\phi$ is instantiated to $\phi_0$, such that $\phi_0(0) = \phi(1) = \{0,1,2,3\}$ and $\phi_0$ is not defined on $\text{pos} \geq 2$. We will write finite multivalued maps as ordered sequences, so, e.g., $\phi_0$ is $\langle\{0,1,2,3\}, \{0,1,2,3\}\rangle$.

From this point of view, $\text{concat}$ in the “finite world” is presented by a function $\text{concat}_j$ over finite sets and finite multivalued maps. The rewriting rules for $\text{concat}_j$ are obtained by the obvious translation of the rewriting rules for $\text{concat}$.

\[
\text{init} : \text{concat}_0(0, \phi) \rightarrow 0 \\
\text{init} : \text{concat}_j(n, \phi) \rightarrow \phi(0) +\{\text{concat}_{j-1}(n-1, \phi_\downarrow)\}
\]

where $\phi_\downarrow := \lambda \text{pos}. \phi(\text{pos} + 1)$ is the 1-position-left shift for the finite sequence of sets presenting $\phi$, and $+$ is the elementwise addition of the elements of two sets. Note that for the sake of convenience $n$ and 1 represent the singletons $\{n\}$ and $\{1\}$ respectively.

Now we want to infer a lower bound $\text{concat}_l$ and an upper bound $\text{concat}_u$ such that the family $\{\text{concat}_l + j\}_{0 \leq j \leq \text{concat}_u - \text{concat}_l}$ approximates $\text{concat}$. As in [13], the inferred family may not be an approximation of the actual output size, for instance, because the actual degree of bounds is higher than the one we have chosen. For that reason, there is a repeated procedure that starts with degree zero, infers, checks and finishes if the inferred family also checks correctly. If not it increments the degree and repeats the procedure. Now for the sake of brevity, assume that the first two steps (degrees zero and one) of this procedure have already been performed and that we are in the third step assuming degree two.
Assume that $\text{concat}_i$ and $\text{concat}_o$ are polynomials with degree $d = 2$. A bound on the size of an output for $\text{concat}$ depends on two parameters, $n$ and $n'$. So, an upper bound is a polynomial of degree two of two variables: $\text{concat}_o(n, n') = \gamma_2 n^2 + \gamma_1 n n' + \gamma_0 n'^2 + \gamma_{10} n + \gamma_{01} n' + \gamma_{00}$. Hence, to find $\text{concat}_o$, one must know its value in 6 points. The same holds for $\text{concat}_i$. We evaluate the rewriting rules for $\text{concat}_i$ in 6 points. Let’s start with $n = n' = 1$. Then $\phi$ is instantiated to $\{0, 1\}$.

\begin{align*}
\text{concat}_o(1, 1) &\rightarrow \{0, 1\}(0) + \{1\} \text{concat}_o(0, \emptyset) = \{0, 1\} + \{1\} = \{0, 1\} \\
\text{concat}_i(1, 1) &\rightarrow \{0, 1\}(0, \emptyset) + \{1\} \text{concat}_i(0, \emptyset) = \{0, 1\} + \{1\} = \{0, 1\}
\end{align*}

So, $\text{concat}_o(1, 1) = \{0, 1\}$. Similarly, $\text{concat}_o(2, 1) = \{0, 1, 2\}$, $\text{concat}_o(3, 1) = \{0, 1, 2, 3\}$, $\text{concat}_i(1, 2) = \{0, 1\}$, $\text{concat}_i(2, 2) = \{0, 1, 2, 3, 4\}$ and finally $\text{concat}_i(1, 3) = \{0, 1, 2, 3\}$. Pick up the maximal values in these sets to define the right-hand side of the system of linear equations for the coefficients $\gamma_{ij}$:

\begin{align*}
720 + 702 + 711 + 710 + 701 + 700 &= 1 \\
720 + 9702 + 3711 + 710 + 3701 + 700 &= 3
\end{align*}

The solution is $(0, 0, 1, 0, 0, 0)$, so $\text{concat}_o(n, n') = n n'$. The similar system of $\text{concat}_i$ has all zeros on its right-hand side. So, the coefficients for $\text{concat}_i$ are all zeros. The inferred family is then $\{j'\}_0 \leq j' \leq mn'$.

Checking that the family obtained is indeed an approximation is done by checking the first-order predicate constructed in the following way. First, substitute in (1) and (2) the function applications for the corresponding approximations, the symbol $\rightarrow$ for $\geq$, and $+$ for $+$:

\begin{align*}
n &= 0 \quad \forall \{j'\}_0 \leq j' \leq mn' \\
n &\geq \forall \{j''\}_0 \leq j'' \leq (n-1)n \quad \forall \{j'\}_0 \leq j' \leq mn'
\end{align*}

Unfolding the definition of set inclusion gives the valid first-order predicates:

\begin{align*}
\forall n. \quad n &= 0 \quad \exists j'. \quad j' = 0 \land 0 \leq j' \leq mn' \\
\forall j'. \quad n \geq 1 \land 0 \leq j' \leq n' \land 0 \leq j' \leq (n-1)n \quad \exists j''. \quad j'' = j + j'' \land 0 \leq j' \leq mn'
\end{align*}

So, the inferred bounds of $\text{concat}_o$ are accepted by the type checker, the loop is finished at $d = 2$ and the informal sketch of our approach is finished.

2 Language

The type system is designed for a strict functional language over integers, booleans and (polymorphic) lists. Language expressions are defined by the grammar below where $c$ ranges over integer and boolean constants False and True, $x$ and $y$ denote program variables of integer and boolean types, $l$ ranges over lists, $z$ denotes a program variable of a zero-order type, $g$ ranges over higher-order program variables, unop is a unary operation, either $-$ or $-$, binop is one of the integer or boolean binary operations, and $f$ denotes a function name.

\begin{align*}
\text{Basic } b &::= c \mid \text{unop } x \mid x \mid \text{binop } y \mid \text{Nil} \mid \text{Cons}(x, l) \mid f(g_1, \ldots , g_i, z_1, \ldots , z_k) \\
\text{Expr } e &::= b \mid x \text{ if then } e_1 \text{ else } e_2 \mid \text{let } z = b \text{ in } e_1 \\
&\quad \mid \text{match } l \text{ with } z \Rightarrow e_1 \\
&\quad \mid \text{Cons}(z_1, l_0) \Rightarrow e_2 \\
&\quad \mid \text{letfun } f(g_1, \ldots , g_i, z_1, \ldots , z_k) = e_1 \text{ in } e_2
\end{align*}
The syntax distinguishes between zero-order let-binding of variables and higher-order letfun-binding of functions. We prohibit head-nested let-expressions and restrict subexpressions in function calls to variables to make type checking straightforward. Program expressions of a general form may be equivalently transformed into expressions of this form. We consider this language as an intermediate language where a general language like ML may be compiled into.

3 Type System

We consider a type system constituted from zero-order and higher-order types and typing rules for each program construct. Size annotations represent lengths of finite lists. Syntactically, size annotations are (higher-order) arithmetic expressions over constants, size variables and multivalued-function symbols. Let $R$ be a numerical ring used to express and solve the size equations. Constants and size variables are layered:

- The layer zero is empty. It corresponds to the unsized types int, bool and $\alpha$, where $\alpha$ is a type variable. Elements of these types have no size annotations.
- The first layer is the type $R^{(1)} = R$ of numerical zero-order constants (i.e. integers) and size variables, denoted by $a$ and $n$, respectively (possibly decorated with subscripts). They represent lengths of outermost lists. Examples are $L_5(a)$ with $a = 5$, or $L_n(L_5(\alpha))$.
- The second layer consists of numerical first-order constants and variables of type $R^{(2)} = R \times R$, denoted by $B$ and $M$, respectively. They represent lengths of nested lists in a list. For instance, in the typing $l : L_n(L_M(a))$ the function $\lambda pos.M(pos)$ represents the length of the $pos$-th list in the master list $l$. Indexes start at 0, so $M(0)$ is the length head of the master list, and $M(n - 1)$ is the length of its last element. Constants of the type $R \to R$ may be defined by an arithmetic expression or by a table. For instance, in $[[1, 2], [3, 4, 5], []]$ the length of the master list is $a = 3$ and $B$ is given by the table $B(0) = 2, B(1) = 3, B(2) = 0$. For $pos \geq 2$, $B(pos)$ may be any arbitrary number.
- In general, the $s$-th layer consists of numerical $(s-1)$-order constants and variables of type $R^{(s)} = R \to R^{(s-1)}$, denoted by $a^s$ and $n^s$. They represent lengths of lists of “nestedness” $s$. For instance in $l : L_n(...) L_n(...) (\alpha)$ the function $n^s(i_1) \ldots (i_{s-1})$ represents the length of the $i_{s-1}$-th list in the $i_{s-2}$-th list in ... in the $i_1$-th list of the master list $l$.

Let $R^*$ denote the union $\bigcup_{s=1}^{\infty} R^{(s)}$ and let $n^*$ range over size variables of $R^*$. Let $\vec{n}^*$ denote a vector of variables $(n_1^*, \ldots, n_k^*)$ for some $k \geq 0$.

Layering is extended to multivalued size functions, according to their return types (but not their parameter types):

- A function of the layer 1 is a function $f : (R^*)^k \to 2^R$ for some $k \geq 0$ that represents all possible sizes (depending on parameters from $(R^*)^k$) of outer
lists. For instance, if \( f(n) = \{n, n + 1\} \) in \( l : Lf(n)(\alpha) \), then the length of \( l \) is either \( n \) or \( n + 1 \). This annotation is given in the output type of the function \( \text{insert} : (\alpha \times \alpha \rightarrow \text{Bool}) \times \alpha \times L_{\alpha}(\alpha) \rightarrow L_{\text{insert}(n)}(\alpha) \). The function \( \text{insert} \), given a predicate \( g : \alpha \times \alpha \rightarrow \text{Bool} \), an element \( z : \alpha \) and a list \( l : L_{\alpha}(\alpha) \), inserts the element in the list if and only if there is no element in the list \( l \) related to \( z \) via \( g \). Another example has been given in the introduction: in the output type of the function \( \text{concat} : L_{n}(L_{\alpha}(\alpha)) \rightarrow L_{\text{concat}(n, M)}(\alpha) \), we have a function \( \text{concat} : \mathcal{R}(1) \times \mathcal{R}(2) \rightarrow 2^\mathcal{R} \). Here \( \text{concat}(0, M) = 0 \) and \( \text{concat}(n, M) = M(0) + M(n - 1, \lambda \text{pos. } M(\text{pos} + 1)) \) for \( n \geq 1 \).

A function of the layer \( s \) is a function of the type \((\mathcal{R}^s)^k \rightarrow (\mathcal{R} \rightarrow \ldots \rightarrow \mathcal{R} \rightarrow 2^\mathcal{R})\) that maps parameters from \((\mathcal{R}^s)^k\) to \( s - 1 \)-order multivalued functions of the type \( \mathcal{R} \rightarrow \ldots \rightarrow \mathcal{R} \rightarrow 2^\mathcal{R} \). Its value \( f(\overline{\text{pos}}_1) \ldots (\text{pos}_s) \) defines all possible sizes of the \( \text{pos}_{s - 1} \) list in the \( \text{pos}_{s - 2} \)-th list ... in the \( \text{pos}_1 \)-the list of the master list.

If a function is single-valued, we will omit the set brackets on its output. As an example, consider the function definition for \( \text{tails} : L_{\alpha}(\alpha) \rightarrow L_{\text{tails}_1(n)}(L_{\text{tails}_2(n)}(\alpha)) \) that creates the list of all non-empty tails of the input list:

\[
\text{tails}(l) = \text{match } l \text{ with } | \text{Nil } \Rightarrow \text{Nil } \\
| \text{Cons(hd, tl) } \Rightarrow \text{let } l' = \text{tails(tl)} \text{ in Cons(l, l')} 
\]

For instance, on \([1, 2, 3]\) it outputs \([[[1, 2, 3]], [[2, 3]], [[3]]]\). It is easy to see that \( \text{tails}_1 : \mathcal{R} \rightarrow 2^\mathcal{R} \) is the identity \( \text{tails}_1(n) = n \) and \( \text{tails}_2 : \mathcal{R} \rightarrow (\mathcal{R} \rightarrow 2^\mathcal{R}) \) for \( n \geq 1 \) is defined by \( \text{tails}_2(n)(\text{pos}) = n - \text{pos} \), if \( 0 \leq \text{pos} \leq n - 1 \).

\[
\text{tails}_2(n)(0) = n \\
\text{tails}_2(n)(1) = n - 1, \text{ if } n \geq 1 \\
\text{tails}_2(n)(\text{pos}) = n - \text{pos}, \text{ if } 0 \leq \text{pos} \leq n - 1 \\
\text{tails}_2(n)(\text{pos}) = \text{arbitrary if } \text{pos} > n
\]

A size expression \( p \) is constructed from size constants, variables, multivalued-function symbols and operations of all layers. We will denote functions of the first and second layers via \( f \) and \( g \), respectively. Admissible operations are arithmetic operations \(+, -, *, \lambda\)-abstraction and application. Layering is defined for size expressions as it has been defined for multivalued size functions. A size expression is of layer \( s \) if it returns a value of order \( s - 1 \) of type \( \mathcal{R} \rightarrow \ldots \rightarrow \mathcal{R} \rightarrow 2^\mathcal{R} \).

When necessary, we denote a size expression of the layer \( s \) via \( p^s \).

\[
p^1 := a | n, m | f(p_1, \ldots, p_k) \quad p^2(pos) \quad p^2(pos - 1) \quad p^2(0) \quad p^2(1) \quad p^2(1 + \ldots, * \ldots) \\
p^2 := B | M | g(p_1, \ldots, p_k) \quad p^3(pos) \quad p^3(pos - 1) \quad p^3(0) \quad p^3(1) \\
p^{s+1} := a^s | n^s | f^s(p_1, \ldots, p_k) \quad p^{s+1}(pos) \quad p^{s+1}(pos - 1) \quad p^{s+1}(0) \quad p^{s+1}(1)
\]

where \( \text{pos} \) is a special variable of type \( \mathcal{R} \) used to denote the position of an element in a list, and \( p_{s+1} \) abbreviates \( \lambda \text{pos. } p(\text{pos}) \). We also assume that constants (e.g. \( a \)) and size variables (e.g. \( n \)) represent singleton sets.

Zero-order annotated types are defined as follows:

\[
\tau^0 := \text{Int} | \text{Bool} | \alpha \\
\tau^{s'} := L_{\tau^{s'}}(L_{\tau^{s'+1}}(... L_{\tau^{s}}(\tau^0) ...)) \text{ for } 1 \leq s' \leq s \\
\tau^s := \tau^s, s
\]
where $\alpha$ is a type variable. It is easy to see that $\tau^s, s = L_{p^s}(\tau^s+1, s)$. The types $\tau^0$ and $\tau^s$ are types of program expressions, but $\tau^{s, s}$ are only used in definitions and proofs but not in function types.

Let $\tau$ ranges over zero-order types. The sets $TV(\tau)$ and $SV(\tau)$ of type and size variables of a type $\tau$ are defined inductively in the obvious way. All empty lists of the same underlying type represent the same data structure. So, $SV(L_0(\tau)) = 0$ for all $\tau$ and $L_0(L_m(\text{Int}))$ represents the same structure as $L_0(L_0(\text{Int}))$.

Zero-order types without type variables or size variables are ground types:

$$\text{GroundTypes } \quad \tau^* ::= \tau \text{ such that } SV(\tau) = 0 \land TV(\tau) = 0$$

The semantics of ground types is defined in Section 3.1. Here we give some examples: $L_2(\text{Bool})$, $L_2(L_B(\text{Bool}))$, and $L_{\text{concat}(2, B)}(\text{Bool})$, where $B(\text{pos}) = \text{pos}$ on $0 \leq \text{pos} \leq 1$. It is easy to see that $\text{concat}(2, B) = \{0\} + \{1\} = \{1\}$. Examples of their inhabitants are $[\text{True, True}, [], [\text{True}], ]$ and $[\text{True}]$, respectively. Examples of non-ground types are $\alpha$, $L_n(\text{Int})$, $L_n(L_M(\text{Bool}))$ and $L_{\text{concat}(n, M)}(\text{Bool})$ with unspecified $n$ and $M$.

Let $\tau^0$ denote a zero-order type where size expressions are all size variables or constants, like, e.g., $L_n(\alpha)$ and $L_n(L_M(\alpha))$. Function types are then defined inductively:

$$\text{FunctionTypes } \quad \tau^f ::= \tau^f_1 \times \ldots \times \tau^f_{k'} \times \tau^0 \rightarrow \tau_0 \quad \text{where } k' \text{ may be zero (i.e. the list } \tau^f_1, \ldots, \tau^f_{k'} \text{ is empty) and } SV(\tau_0) \text{ contains only size variables of } \tau^f_1, \ldots, \tau^f_{k'}.$$  

Multivalued size functions $f$ in the output types of function signatures in general are defined by conditional rewriting rules, as we have seen in the introduction. It is desirable to find closed forms for functions defined by such rewriting rules.

A context $\Gamma$ is a mapping from zero-order variables to zero-order types. A signature $\Sigma$ is a mapping from function names to function types. The definition of $SV(-)$ is straightforwardly extended to contexts:

$$SV(\Gamma) = \bigcup_{x \in \text{dom}(\Gamma)} SV(\Gamma(x))$$

### 3.1 Heap Semantics

In our semantic model, the purpose of the heap is to store lists. Therefore, a heap is a finite collection of locations $\ell$ that can store list elements. A location is the address of a cons-cell consisting of a head field $\text{hd}$, which stores a list element, and a tail field $\text{tl}$, which contains the location of the next cons-cell of the list, or the NULL address. Formally, a program value is either an integer or boolean constant, a location or the null-address, and a heap is a finite partial mapping from locations and fields into program values:
Address $adr ::= \ell | \text{NULL} \quad \ell \in \text{Loc}$
Val $v ::= c | adr \quad c \in \text{Int} \cup \text{Bool}$

Heap $h : \text{Loc} \rightarrow \{\text{hd}, \text{tl}\} \rightarrow \text{Val}$

We will write $h.\ell.\text{hd}$ and $h.\ell.\text{tl}$ for the results of applications $h.\ell$ $\text{hd}$ and $h.\ell$ $\text{tl}$, which denote the values stored in the heap $h$ at the location $\ell$ at its fields hd and tl, respectively. Let $h.\ell[hd := v_h, tl := v_t]$ denote the heap equal to $h$ everywhere but in $\ell$, which at the hd-field of $\ell$ gets the value $v_h$ and at the tl-field of $\ell$ gets the value $v_t$.

The semantics $w$ of a program value $v$ with respect to a specific heap $h$ and a ground type $\tau^*$ is a set-theoretic interpretation given via the four-place relation $v \models_{h, \tau^*} w$. Integer and boolean constants interpret themselves, and locations are interpreted as non-cyclic lists. Let $p^1(\overline{m_i})$ denote the set of values of some expression $p^1$ applied to some values $\overline{m_i}$. Then

\begin{align*}
c & \models_{\text{Int} \cup \text{Bool}} c \\
\text{NULL} & \models_{\text{null}} (\overline{m_i})(\ell^*) \quad \text{iff} \quad 0 \in p^1(\overline{m_i}) \\
\ell & \models_{\text{loc}} (\overline{m_i})(\ell^*) \quad \text{whd} :: \text{whd} \quad \text{iff} \quad h.\ell.\text{hd} \models_{\text{loc}} (\overline{m_i})_0 (\ell), \quad w_{\text{hd}}, \\
h.\ell.\text{tl} & \models_{\text{loc}} (\overline{m_i})_1 (\ell), \quad w_{\text{tl}}
\end{align*}

where $h|_{\text{dom}(h) \setminus \ell}$ denotes the heap equal to $h$ everywhere except in $\ell$, where it is undefined, $(\tau^{s+1})_p$ and $\tau^{s+1}$ are abbreviations for $\lambda \text{pos},. p^s(\text{pos} + 1)$ and $\lambda \text{pos}. \tau(\text{pos} + 1)$, respectively and the application of a type to a first-layer size expression $\tau(p^1)$ is defined as follows:

\begin{align*}
\tau^0(p^1) &= \tau^0 \\
\tau^{1,s}(p^1) &= \tau^{1,s} \\
(\text{length}(\overline{m_i}))(\ell^*) &:= \text{null}(\overline{m_i})(\text{length}(\overline{m_i})(\ell^*)), \text{for } s' \geq 2
\end{align*}

The length of a non-cyclic chain of cons-cells in a heap is defined by induction in a usual way: $\text{length}_h(\text{NULL}) = 0$ and $\text{length}_h(\ell) = 1 + \text{length}_h|_{\text{dom}(h) \setminus \ell}(h.\ell.\text{tl})$. Note that the function $\text{length}_h(\overline{m_i})$ does not take sharing into account, in the sense that the actual total size of allocated shared lists is less than the sum of their lengths. Thus, the sum of the lengths of the lists provides an upper bound on the amount of memory actually allocated.

Lemma 1 (Consistency of model relation). The relation $adr \models_{h} (\overline{m_i})(\ell^*)$ implies that $\text{length}_h(adr) \in p^1(\overline{m_i})$.

The proof is done by induction on the relation $\models$.

3.2 Operational semantics of program expressions

The operational semantics is standard. It extends the semantics from [14] with higher-order functions.

We introduce a frame store as a mapping from program variables to program values. This mapping is maintained when a function body is evaluated.
Before evaluation of the function body starts, the store contains only the actual
details of the function. During evaluation, the store is extended with the
variables introduced by pattern matching or let-constructs. These variables are
eventually bound to the actual parameters. Thus there is no access beyond the
current frame. Formally, a frame store $s$ is a finite partial map from variables to
values, $\text{Store } s : \text{ProgramVars} \to \text{Val}$.

Using a heap, a frame store and mapping $C$ (closures) from function names
to function bodies, the operational semantics of program expressions is defined
inductively in a standard way. The rules are as follows:

$$
\text{c} \in \text{Int} \cup \text{Bool} \quad \text{OSCONS} \quad \frac{s; h; C \vdash c \to c'; h}{s; h; C \vdash z \to s(z); h} \quad \text{OSVAR}
$$

$$
\frac{\text{NIL}}{s; h; C \vdash \text{NIL} \to \text{NULL}; h} \quad \text{OSNIL}
$$

$$
\frac{s(\text{hd}) = v_{\text{hd}} \quad s(\text{tl}) = v_{\text{tl}} \quad \ell \notin \text{dom}(h)}{s; h \vdash \text{Cons}(\text{hd}, \text{tl}) \to \ell; h[\ell.\text{hd} := v_{\text{hd}}, \ell.\text{tl} := v_{\text{tl}}]} \quad \text{OSCONS}
$$

$$
\frac{s(\text{x}) = \text{True}}{s; h; C \vdash \text{e}_1 \to v; h'} \quad \text{OSIfTrue}
$$

$$
\frac{s(\text{x}) = \text{False}}{s; h; C \vdash \text{e}_2 \to v; h'} \quad \text{OSIfFalse}
$$

$$
\frac{s; h; C \vdash \text{e}_1 \to v_1; h_1 \quad s[\text{z} := v_1]; h_1; C \vdash \text{e}_2 \to v}{s; h; C \vdash \text{let } \text{z} = \text{e}_1 \text{ in } \text{e}_2 \to v; h'} \quad \text{OSLET}
$$

$$
\frac{s(\text{l}) = \text{NULL}}{s; h; C \vdash \text{if } \text{x} \text{ then } \text{e}_1 \text{ else } \text{e}_2 \to v; h'} \quad \text{OSIf}
$$

$$
\frac{s; h; C \vdash \text{match } \text{l} \text{ with } | \text{Nil} \Rightarrow \text{e}_1 | \text{Cons}(\text{hd}, \text{tl}) \Rightarrow \text{e}_2}{s; h; C \vdash \text{match } \text{l} \text{ with } | \text{Nil} \Rightarrow \text{e}_1 \to v; h'} \quad \text{OSMatch-Nil}
$$

$$
\frac{h, s(\text{l}).\text{hd} = v_{\text{hd}} \quad h, s(\text{l}).\text{tl} = v_{\text{tl}}}{s[\text{hd} := v_{\text{hd}}, \text{tl} := v_{\text{tl}}]; h; C \vdash \text{e}_2 \to v; h'} \quad \text{OSMatch-Cons}
$$

$$
\frac{s; h; C \vdash \text{let} f = (g_1, \ldots, g_k, z_1, \ldots, z_k) \times e_1 \mid \text{e}_2 \to v; h'}{s; h; C \vdash \text{fun} f(g_1, \ldots, g_k, z_1, \ldots, z_k) = e_1 \text{ in } e_2 \to v; h'} \quad \text{OSLetFun}
$$

$$
\frac{s(\text{z}_i') = v_i \ldots s(\text{z}_k') = v_k \quad C(f) = (g_1, \ldots, g_k', z_1, \ldots, z_k) \times e_f \quad [z_1 := v_1, \ldots, z_k := v_k]; h; C \vdash e_f[g_1 := f_1, \ldots, g_k := f_k] \to v; h'}{s; h; C \vdash f(f_1, \ldots, f_k, z_1', \ldots, z_k') \to v; h'} \quad \text{OSFunApp}
$$
3.3 Typing rules

A typing judgement is a relation of the form \( D, \Gamma \vdash \Sigma : \tau \), i.e., given a set of constraints \( D \), a zero-order context \( \Gamma \) and a higher-order signature \( \Sigma \), an expression \( e \) has a type \( \tau \). The set \( D \) of disequations and memberships is relevant only when a rule for pattern-matching and constructors are applied. When the nil-branch is entered on a list \( Lp_1(n*)(a) \), then \( D \) is extended with \( 0 \leq p_1(n*) \). When the cons-branch is entered, then \( D \) is extended with \( m \geq 1, m \leq p(n*) \), where \( m \) is a fresh size variable in \( D \). When a constructor is applied, \( D \) is extended with position-delimiting disequations.

Given types \( \tau = Lp_1(n*)\ldots Lp_s(n*)(a) \ldots \) and \( \tau' = Lp_1'(n*)\ldots Lp_s'(n*)(a) \ldots \), let the entailment \( D \vdash \tau \rightarrow \tau' \) abbreviate the collection of rules that (conditionally) rewrite \( p_1(n*) \rightarrow p_1'(n*) \) etc.:

\[
D, m_1 \in p_1(n*), 0 \leq \text{pos} \leq m_1 - 1 \quad \vdash p^2(\text{pos}) \rightarrow p^2(\text{pos})
\]

\[
D, m_1 \in p_1(n*), 0 \leq \text{pos}_1 \leq m_1 - 1, \quad m_2 \in p_2(n*)\text{pos}_1) , 0 \leq \text{pos}_2 \leq m_2 - 1 \quad \vdash p^3(\text{pos}_1)\text{pos}_2)(\text{pos}_2)
\]

\[
D, m_1, \text{pos}_1, m_2, \text{pos}_2 \text{ are fresh for } D
\]

The typing judgement relation is defined by the following rules:

\[
\frac{D, \Gamma \vdash \iota : \text{Int}}{D, \Gamma \vdash \iota : \text{Int}} \quad \text{1Const}
\]

\[
\frac{D, \Gamma \vdash \text{b} : \text{Bool}}{D, \Gamma \vdash \text{b} : \text{Bool}} \quad \text{BConst}
\]

\[
\frac{D \vdash \tau' \rightarrow \tau}{D, \Gamma, \text{z} : \tau \vdash \text{z} : \tau'} \quad \text{VAR}
\]

\[
\frac{D \vdash \tau' \rightarrow L_0(\tau)}{D, \Gamma \vdash \text{Nil} : \tau'} \quad \text{NIL}
\]

\[
\frac{D \vdash \tau' \rightarrow L_{p_1(n*)+1}(\tau'')}{D, \Gamma \vdash \text{Cons}(\text{hd}, \text{tl}) : \tau'} \quad \text{CONS}
\]

where \( n \) is fresh in \( D, \Gamma, \tau_1, \tau_2 \). Note, that the obvious naive version of this rule, with the judgement \( D, \Gamma, \text{hd} : \tau, \text{tl} : L_{p_1(n*)}(\tau) \vdash \Sigma : \text{Cons}(\text{hd}, \text{tl}) : \tau' \) in the conclusion and the side condition \( D \vdash \tau' \rightarrow L_{p_1(n*)+1}(\tau) \), is less general. It does not allow the length of \( \text{hd} \), if it is a list, to differ from the length of the internal lists of \( \text{tl} \). For instance, the naive version is not applicable to the constructor over \( \text{hd} : L_5(\alpha) \) and \( \text{tl} : L_n(\alpha) \), whereas the presented rule accepts the type \( L_{n+1}(L_{\text{pos}}.g(\text{pos})(\alpha)) \), where \( g(0) = 5 \) and \( g(\text{pos}) = 6 \) for \( 1 \leq \text{pos} \leq n \).

Moreover, backward application of the \text{CONS}-rule to \( n \geq 1 ; l : L_n(\alpha), l' : L_{n-1}(\text{tl}_1(n-1)(\text{tl}_2(n-1)(\alpha)) \vdash \Sigma : \text{Cons}(l, l') : L_{n+1}(\alpha) \) allows to infer the
rewriting rules for the sizes of the inner lists of the output for tails:

\[
\begin{align*}
\text{if } n \geq 1, \text{ then } &\vdash \text{tails}_2(n)(0) \rightarrow n \\
\text{if } n \geq 1, 1 \leq \text{pos} \leq n &\vdash \text{tails}_2(n)(\text{pos}) \rightarrow \text{tails}_2(n-1)(\text{pos} - 1)
\end{align*}
\]

The IF-rule "collects" the size dependencies of both branches:

\[
\begin{align*}
\Gamma(x) = \text{Bool} & \quad \frac{D \vdash \Gamma \tau \rightarrow \tau_1 \mid \tau_2}{D, \Gamma \vdash \Sigma \text{ if } x \text{ then } \tau_1 \text{ else } \tau_2} & \text{IF} \\
\frac{\text{if } x \in \text{dom}(\Gamma) \quad D, \Gamma \vdash \Sigma \tau_1 \mid \tau_2}{\text{let } z = e_1 \text{ in } \tau_2} & \text{LET}
\end{align*}
\]

where \(n' \not\in SV(D)\). Note that if in the MATCH-rule \(p^1\) is single-valued, the statements in the nil and cons branches are \(p^1(\overline{n}^*) = 0\) and \(p^1(\overline{n}^*) \geq 1\), respectively.

\[
\begin{align*}
\Sigma(f) = \tau_1 \times \ldots \times \tau_k & \quad \frac{\text{letfun } f(g_1, \ldots, g_k, z_1, \ldots, z_k) = e_1 \text{ in } e_2 \vdash \tau'}{\text{FUNAPP}}
\end{align*}
\]

where \(\sigma\) is an instantiation of the formal size variables with the actual size expressions, and \(C\) consists of equations between size expressions that are constructed in the following way. If \(\tau^* = \Sigma(g_1)\) and \(\tau' = \Sigma(g_1')\), then \(\sigma(n^*) := p^1(\overline{n}^*)\). If \(\tau^* = \tau'^*\), then the corresponding size expressions are equal, that is \(C\) contains \(p^1(\overline{n}^*) = p^1(\overline{n}^*)\). Further, if \(\tau^* = \Sigma(g_1)\), then \(C\) contains \(p^1(\overline{n}^*) = a^*\). Eventually \(\sigma(q_0)\) for \(q_0 = \Sigma(g_1)\ldots\Sigma(g_k)\) is defined as \(\Sigma(g_1)\ldots\Sigma(g_k)\).

As an example of a case when \(C\) is needed, consider a call of a function \(\text{scalarprod} : L_m(\text{Int}) \times L_m(\text{Int}) \rightarrow \text{Int}\) on actual size arguments \(l_1 : L_{n+1}(\text{Int})\) and \(l_2 : L_{m-1}(\text{Int})\). Then \(C\) contains \(n+1 = m-1\). It will hold if \(D\) contains \(n = m-2\).

**Example 1: inferring rewriting rules for concat** In the introduction we have given the rewriting rules defining the type for concat : \(L_n((M,\overline{a})) \rightarrow L_{\text{concat}(n, M)}(\overline{a})\), where

\[
\begin{align*}
\text{if } n \geq 1 &\vdash \text{concat}(0, M) \rightarrow 0 \\
\text{if } n \geq 1 &\vdash \text{concat}(n, M) \rightarrow M(0) + \text{concat}(n - 1, \lambda \text{pos}. M(\text{pos} + 1))
\end{align*}
\]
Now we show how the typing rules are used to infer this rewriting system. We apply the rules as in a subgoal-directed backward-style proof.

1. The LetFun rule defines the main goal: \( \Gamma \vdash L_M(a) \vdash \Sigma \) \( \concats \) \( L_{\text{concat}(n,M)}(a) \), where \( \concats \) denotes the body of \( \text{concat} \).

2. Apply the MATCH-rule. In the nil-branch we obtain the subgoal 
\( n = 0 \vdash L_M(a) \vdash \Sigma \) \( \Nil \vdash L_{\text{concat}(n,M)}(a) \).

3. Continue with the nil-branch. Apply the Nil rule and obtain 
\( n = 0 \vdash L_{\text{concat}(n,M)}(a) \rightarrow L_0(\tau^\gamma) \).

4. Instantiate \( \tau^\gamma = \alpha \). Unfold the definition of type rewriting: 
\( n = 0 \vdash \text{concat}(n,M) \rightarrow 0 \).

5. Now, consider the cons-branch. The subgoal there is
\( n \geq 1; \text{hd}: L_M(0)(0), \text{tl}: L_{n-1}(L_M(\alpha+1) \vdash \text{append}(: \text{concat}(\text{tl})): L_{\text{concat}(n,M)}(\alpha)) \).

6. Unfold the definition of application of a type to a first-level expression and the definition for \((-)_+1:\)
\( n \geq 1; \text{hd}: L_{M(0)}(\alpha), \text{tl}: L_{n-1}(L_M(\alpha)) \vdash \text{append}(: \text{concat}(\text{tl})): L_{\text{concat}(n,M)}(\alpha)) \).

7. The expression in the judgement above is a sugared let-construct. So, we apply the LET-rule. In the binding we get the goal:
\( n \geq 1; \text{tl}: L_{n-1}(L_M(\alpha)) \vdash \text{concat}(\text{tl}) : L_{\text{concat}(n,M)}(\alpha) \).

8. Using FUNApp-rule we instantiate the type \( \tau^\gamma := L_{\text{concat}(n-1,M+1)}(\alpha) \).

9. Therefore, the subgoal for the let-body is 
\( n \geq 1; \text{hd}: L_{M(0)}(\alpha), \text{tl}: L_{n-1}(L_M(\alpha)) \vdash \text{append}(: \text{concat}(\text{tl})): L_{\text{concat}(n,M)}(\alpha)) \).

10. Unfold the definition of type rewriting and the definition of the operation \((-)_+1:\)
\( n \geq 1 \vdash \text{concat}(n,M) \rightarrow M(0) + \text{concat}(n-1,M+1)) \).

Example 2: inferring rewriting rules for tails

Now we want to infer the rewriting rules for the size annotations in the type \( \text{tails} : L_n(a) \vdash L_{\text{tails}(n)}(L_{\text{tails}(2)}(n)(a)) \). Recall, that the closed forms of the annotations are \( \text{tails}(n) = n \) and \( n \geq 1, 0 < \text{pos} \leq n - 1 \vdash \text{tails}(n)(\text{pos}) = n - \text{pos} \), respectively. In this example we show how output lists of lists are treated.

1. The LetFun rule defines the main goal: \( \Gamma \vdash L_n(a) \vdash L_{\text{tails}(n)}(L_{\text{tails}(2)}(n)(a)) \), where \( \text{tails} \) denotes the body of tails.

2. Apply the MATCH-rule. In the nil-branch we obtain the subgoal 
\( n = 0 \vdash L_n(a) \vdash \Sigma \) \( \Nil \vdash L_{\text{tails}(n)}(L_{\text{tails}(2)}(n)(a)) \).

3. Continue with the nil-branch. Apply the Nil rule and obtain 
\( n = 0 \vdash L_{\text{tails}(n)}(L_{\text{tails}(2)}(n)(a)) \rightarrow L_0(\tau^\gamma) \).

4. Trivially, instantiate \( \tau^\gamma := L_{\text{tails}(n)}(\alpha) \). Unfold the definition of the type rewriting: 
\( n = 0 \vdash \text{tails}(n) \rightarrow 0 \).

Note, that the rewriting rules for \( \text{tails}(n) \) in this branch are absent, since \( n_1 \in \{n = 0\}, 0 \leq \text{pos} \leq n_1 - 1 \) is an empty set.

5. Now, consider the cons-branch. The subgoal there is
\( n \geq 1; \text{hd}: L_n(a), \text{tl}: L_{n-1}(\alpha+1) \vdash \Sigma \) \( \text{Cons}(l, \text{tails}(\text{tl})): L_{\text{tails}(n)}(L_{\text{tails}(2)}(n)(\alpha)) \).

(Again, that in contexts we omit variables, on which the expression in the typing judgement under consideration does not depend.)
6. In the type of $\text{tl}$ unfold the definition of $(-)^{+1}$:
\[ n > 1; \text{tl}: (\text{Ln}(n-1)) \vdash \text{Cons}(\text{hd}, \text{tl}) : (\text{Ln}(n+1)). \]

7. The expression in the judgement above is a sugared let-construct. So, we apply the Let-rule. In the binding we have the subgoal:
\[ n > 1; \text{tl}: (\text{Ln}(n-1)) \vdash \text{tails}(\text{tl}) : \tau^2. \]

8. Using FUNApp-rule we instantiate the type $\tau^2 := (\text{Ln}(n+1)).$

9. Therefore, the subgoal for the let-body is:
\[ n > 1; \text{tl}: (\text{Ln}(n-1)) \vdash \text{Cons}(\text{hd}, \text{tl}) : (\text{Ln}(n+1)). \]

10. Apply the CONS-rule. We obtain the predicates:
\[ n > 1 ; \vdash \text{Ln}(n+1) \rightarrow (\text{Ln}(n+1)). \]

11. Trivially, instantiate $\tau^2 := (\text{Ln}(n+1)).$ We obtain:
\[ n > 1 ; \vdash \text{tail}(n) (\text{TAILS}(n+1)). \]

12. Unfold the definition of type-typewriting. For $\text{TAILS}_1$ we obtain $n > 1 ; \vdash \text{TAILS}_1(n) = \text{TAILS}_1(n+1),$ and for $\text{TAILS}_2,$ unfolding the definition of application of a type to a first-layer expression, we obtain:
\[ n > 1 ; \vdash \text{TAILS}_2(n)(0) \rightarrow n \]

It is easy to see that $\text{TAILS}_1(n) = n$ is a closed form for the obtained rewriting system for $f:$ $\text{TAILS}_1(n)(0) = 0$ and $\text{TAILS}_1(n) = \text{TAILS}_1(n+1) + 1$ with $n > 1.$ Further, $\text{TAILS}_2(n)(pos) = n - i$ for $0 \leq pos \leq n - 1$ solves the rewriting system for $g.$ Indeed, by induction on $n > 2,$ $\text{TAILS}_2(n)(pos) = \text{TAILS}_2(n-1)(pos - 1) = (n-1) - (pos - 1) = n - i$ for $i > 1,$ with the base $\text{TAILS}_2(1)(0) = 1,$ and having $\text{TAILS}_2(n)(pos) = n$ for $pos = 0.$

3.4 Semantics of typing judgements (soundness)

The set-theoretic semantics of typing judgements is formalised later in this section as the soundness theorem, which is defined by means of the following two predicates. One indicates if a program value is valid with respect to a certain heap and a ground type. The other does the same for sets of values and types, taken from a frame store and a ground context $\Gamma^*.$

\[ \text{Valid}_{\text{val}}(v, \tau^*, h) = \exists w : v \models^* w \]
\[ \text{Valid}_{\text{store}}(\text{vars}, \Gamma^*, \text{store}, h) = \forall x : \text{vars}. \text{Valid}_{\text{val}}(s(x), \Gamma^*(x), h) \]

Let a valuation $\varepsilon^*$ map size variables to constants of the layer $s,$ and let an instantiation $\eta$ map type variables to ground types:

\[ \text{Valuation} \quad \varepsilon^* : \text{SizeVariables}^{*} \rightarrow (\mathcal{R} \rightarrow \cdots \rightarrow \mathcal{R} \rightarrow \mathcal{R}) \]
\[ \text{Instantiation} \quad \eta^* : \text{TypeVariables}^{*} \rightarrow \tau^{**} \]

Let $\epsilon$ and $\eta$ be the direct sums of some $\epsilon^1, \ldots, \epsilon^k$ and $\eta^1, \ldots, \eta^k$ respectively. We will usually write the application of $\eta$ and $\epsilon$ as subscripts. For example, $\eta(\epsilon(\tau))$ becomes $\tau_{\eta\epsilon}$ and $\epsilon(D)$ becomes $D_{\epsilon}.$ Note that $D$ contains no type variables and hence $D_{\eta} = D.$ Valuations and instantiations distribute over size functions in the following way:
\[ (L_{\varepsilon}(\eta)^*(\tau)))_{\eta\epsilon} = L_{\varepsilon}(\eta)^*(\tau_{\eta\epsilon}) \]
Lemma 2 (Rewriting preserves model relation (i.e. implies set-theoretic inclusion of types)). Let \( D(\overline{n}) \vdash \tau \rightarrow \tau' \). Let a valuation \( \epsilon \) and a type instantiation \( \eta \) be such that \( v \models^{\overline{n} \eta} w \) and \( D \epsilon \) hold. Then \( v \models^{\overline{n} \eta} w \) holds as well.

Proof. Induction on \( \models \). The case where \( v \) is an integer or a boolean is straightforward since \( \tau' \) and \( \tau \) will be Int or \( \text{Bool} \), respectively.

Let \( \tau = L_{p^1(\overline{n} \eta)}(\tau'') \) and \( \tau' = L_{p^1(\overline{n} \eta)}(\tau'''') \) for some \( \tau'' \) and \( \tau''' \), and let \( c(\overline{n} \eta^*) = \overline{n_0} \).

Assume \( v = \text{NULL} \). Then \( 0 \in p_1'(\overline{n_0}) \) and \( w = [] \). Since \( p_1(\overline{n_0}) \rightarrow p_1'(\overline{n_0}) \), that is \( p_1'(\overline{n_0}) \subseteq p_1(\overline{n_0}) \), we have \( 0 \in p_1(\overline{n_0}) \) and \( v \models^{\overline{n} \eta} [] \).

Now assume that \( v = \ell \) and \( w = w_{hd} :: w_{dl} \), where \( h.\ell.\overline{l} \models^{\overline{n_0}} w_{hd} \) and \( h.\ell.\overline{l} \models^{\overline{n_0}(\overline{n_0}) \rightarrow (\tau'''')} w_{hd} \). Since there is \( n \in p_1(\overline{n_0}) \) with \( n \geq 1 \) (because we are in the non-empty case), we have \( D \vdash \tau'' \rightarrow \tau''' \), from which follows that \( D \vdash \tau'_{n+1} \rightarrow \tau'''_{n+1} \). Then, by induction, \( h.\ell.\overline{l} \models^{\overline{n_0}(\overline{n_0}) \rightarrow (\tau'''')} w_{hd} \). Since \( p_1(\overline{n_0}) \rightarrow p_1'(\overline{n_0}) \), we have that \( p_1(\overline{n_0}) - 1 \rightarrow p_1'(\overline{n_0}) - 1 \), and by induction \( h.\ell.\overline{l} \models^{\overline{n_0}(\overline{n_0} - 1)(\tau'''')} w_{ld} \).

This lemma may seem counterintuitive on a first sight because it looks like a type preservation lemma where the type \( \tau \) and \( \tau' \) are swapped. However, a rewriting rule is different from an evaluation step. The idea behind this lemma is that on a rewriting rule there are several choices on the left hand side (\( \tau \)) and one in particular is chosen to obtain the right hand side (\( \tau' \)). So, if a value has type \( \tau' \), it also has type \( \tau \).

Informally, the soundness theorem states that, assuming that the zero-order context variables are valid, i.e., that they indeed point to lists of the sizes mentioned in the input types, then the result in the heap will be valid, i.e., it will have the size indicated in the output type.

Theorem 1 (Soundness). For any store \( s \), heaps \( h \) and \( h' \), closure \( C \), expression \( e \), value \( v \), context \( \Gamma \), quantifier-free formula \( D \), signature \( \Sigma \), type \( \tau \), size valuation \( \epsilon \), and type instantiation \( \eta \) such that

\[- \text{dom}(s) = \text{dom}(\Gamma), \epsilon : SV(\Gamma) \cup SV(D) \rightarrow \mathcal{R} \text{ and } \eta : TV(\Gamma) \rightarrow \tau^* , \]
\[- D \epsilon, \eta \text{ holds,} \]
\[- s; h; C \models e \rightarrow v; h' \text{ and } D, \Gamma \models_{\Sigma} e : \tau, \]
\[- \text{Valid}_{\text{store}}(\text{dom}(s), \Gamma_{\eta e}, s, h), \]

then \( v \) is valid according to its return type \( \tau \) in \( h' \), i.e., \( \text{Valid}_{\text{val}}(v, \tau_{\eta e}, h') \).

Proof. The proof is done by induction on the size of the derivation tree for the operational-semantic judgement. This is possible because we assume that the evaluation of \( e \) terminates (with a value \( v \)). We have to show that \( \text{Valid}_{\text{val}}(v, \tau_{\eta e}, h') \), i.e., that there is a \( w \) such that \( v \models^{\tau_{\eta e}} w \). This is proved for each of the operational-semantic rules.
OSNull: In this case e = Nil, v = NULL and h' = h. From the NIL typing rule we have that D \vdash \tau \rightarrow L_0(\tau'). According to the definition of rewriting rule, \tau = L_{p(\tau')}(\tau'') for some p, \tau' and \tau'', where p(\tau') \rightarrow 0. But then p(\tau'') \rightarrow 0 and hence 0 \in p(\tau''). But then from the definition of model relation we get that NULL \models h'_{\tau(\tau'')} \text{ and thus NULL} \models h' \tau_{\tau''} \text{.}

OSVar: In this case e = z, v = s(z) and h' = h. Since dom(s) = dom(\Gamma), there is a \tau' such that \Gamma(z) = \tau', and because Val_{store}(dom(s), \Gamma_{\neq}, s, h), there is a w such that s(z) \models h'_{\tau_{\tau'w}} w. Now from the VAR typing rule, D \vdash \tau \rightarrow \tau'.

Since D holds, we can now apply the Lemma 2 to obtain v = h'_{\tau_{\tau'w}} w.

OSCons: In this case e = Cons(hd, tl), v = \ell for some location \ell \notin dom(h) and h' = h.f.[hd := s(hd), tl := s(tl)].

From the CONS typing rule we have that hd: \tau_1 and tl: L_{p(\tau')}(\tau_2), and the judgements D \vdash \tau' \rightarrow L_{p(\tau')} (\tau''_2), D \vdash \tau''_2(0) \rightarrow \tau_1 and n \in p(\tau''), 1 \leq pos \leq n, D \vdash \tau''_2(pos) \rightarrow \tau_2(pos - 1). Since Val_{store}(dom(s), \Gamma_{\neq}, s, h), there exist w_{hd} and w_{tl} such that s(hd) \models h'_{\tau_1w_{hd}} and s(tl) \models h'_{\tau_2w_{tl}}. Therefore, h'.ell.hd \models h'_{\tau_{\tau'w_{hd}}} and h'.ell.tl \models h'_{\tau_{\tau'w_{tl}}}.

It is easy to see that h = h'|_{dom(h')}(\ell), thus, h'.ell.hd \models h'|_{dom(h')}(\ell) s(hd) and h'.ell.tl \models h'|_{dom(h')}(\ell) s(tl). From the judgement D \vdash \tau''_2(0) \rightarrow \tau_1 and Lemma 2, h'.ell.hd \models \tau''_2(0) w_{hd}. Now we want to show that h'.ell.tl \models \tau''_2(0) w_{tl} and then by the definition of model relation we can obtain the desired result: \ell \models h'_{\tau_{\tau'w_{td}}}.

The judgement n \in p(\tau''), 1 \leq pos \leq n, D \vdash \tau''_2(pos) \rightarrow \tau_2(pos - 1), is equivalent to n \in p(\tau''), 1 \leq pos \leq n, D \vdash \tau''_2(pos + 1) \rightarrow \tau_2(pos). Recall that \tau_{\tau'+1} is defined as \lambda pos. \tau(pos + 1), thus we have the judgement n \in p(\tau''), 1 \leq pos \leq n, D \vdash \tau''_2(pos + 1) \rightarrow \tau_2(pos). Now by definition of rewriting rules, n \in p(\tau''), 1 \leq pos \leq n, D \vdash L_{p(\tau''_2)}(\tau''_2(pos + 1)) \rightarrow L_{p(\tau''_2)}(\tau_2(pos)).

Instantiating Lemma 2 with this judgement and h'.ell.tl \models \tau''_2(0) w_{tl}, we get h'.ell.tl \models \tau''_2(0) w_{tl}.

OSIfTrue: In this case e = if x then e_1 else e_2, with s(x) = True and s; h; C \vdash e_1 \models v_1; h_1 and s; h; C \vdash e_2 \models v; h'. From the IF typing rule we get that D, \Gamma \vdash \Sigma e_1 : \tau_1, D, \Gamma \vdash \Sigma e_2 : \tau_2 and D \vdash \tau \rightarrow \tau_1 \downarrow \tau_2. Since e_1 is evaluated in the same context as e (s; h; C), we can use the induction hypothesis to get Val_{store}(v, \tau_{\tau_1h_1h'}).

Since by definition of D \vdash \tau \rightarrow \tau_1 \downarrow \tau_2, D \vdash \tau \rightarrow \tau_1, using Lemma 2 we obtain Val_{store}(v, \tau_{\tau_1h_1h'}).

OSIfFalse: Similar to the true case.

OSLet: In this case e is let z = e_1 in e_2, with s(z) = True and s; h; C \vdash e_1 \models v_1; h_1 and s; h; C \vdash e_2 \models v; h'. From the LET typing rule we have that z \notin dom(\Gamma), D, \Gamma \vdash \Sigma e_1 : \tau_1 and D, \Gamma; z : \tau' \vdash \Sigma e_2 : \tau. Applying the induc-
tion hypothesis to the antecedents of the operational semantics, we get that $\text{Valid}_{\text{val}}(v_1, \tau_{\text{ne}}, h_1)$ and that if $\text{Valid}_{\text{store}}(s[z := v_1], \tau_{\text{ne}}, h_1)$, then $\text{Valid}_{\text{val}}(v_1, \tau_{\text{ne}}, h_1)$.

Fix some $z' \in \text{dom}(s[z := v_1])$. If $z' = z$, then $\text{Valid}_{\text{val}}(v_1, \tau_{\text{ne}}, h_1)$ implies $\text{Valid}_{\text{val}}(v_1, \tau_{\text{ne}}, h_1)$. If $z' \neq z$, then $s[z := v_1](z') = s(z')$. Sharing of data structures in the heap is benign (no destructive pattern matching and assignments), hence $h|_{\text{R}(h, s(z'))} = h|_{\text{R}(h, s(z'))}$. Thus, we have that $s(z') = s(z') = \text{Valid}_{\text{val}}(v_1, \tau_{\text{ne}}, h_1)$ and that if $s[z := v_1](z') = s(z')$.

So, $\text{Valid}_{\text{val}}(s[z := v_1], \tau_{\text{ne}}, h_1)$. Hence, $\text{Valid}_{\text{store}}(s[z := v_1], \tau_{\text{ne}}, h_1)$ and we can now apply the induction hypothesis.

**OSMatch-Nil:** In this case $e = \text{match } l \text{ with } | \text{Nil} \mapsto e_1 \mid \text{Cons}(hd, tl) \mapsto e_2$ where $s(l) = \text{NULL}$ and $s; h; C[l := e_1 \leadsto v; h']$. From the MATCH typing rule we have that $\Gamma = \Gamma' \cup \{ l : L_{\pi}(n)(\tau') \}$ and $D, 0 \in p^1(\tau_\ast)$. From $\text{Valid}_{\text{store}}(s(l), \tau_{\text{ne}}, s, h)$, we get $\text{Valid}_{\text{val}}(s(l), \tau_{\text{ne}}, s, h)$ and since $s(l) = \text{NULL}$, from the definition of model relation we get that $0 \in p^1(\tau_\ast)$.

Therefore, the typing judgement about $e_1$ reduces to $\Gamma, l : L_{\pi}(n)(\tau') \vdash \tau$, and $e_2$. The typing context has the form $\Gamma, l : L_{\pi}(n)(\tau') \vdash \tau$. From the operational semantics we know that $s(l) = \text{NULL}$, that is, $s(l) \neq \text{NULL}$. Due to the validity of $s(l)$ and Lemma 1, there exists $n_0 \geq 1$ in $p^1(\tau_\ast)$. From the validity $s(l) = \text{Valid}_{\text{val}}(s(l), \tau_{\text{ne}}, s, h)$ and the results above, we obtain that $\text{Valid}_{\text{store}}(s(l), \tau_{\text{ne}}, s, h)$ and the induction hypothesis yields $\text{Valid}_{\text{val}}(v_1, \tau_{\text{ne}}, h')$.

**OSMatch-Cons:** In this case $e = \text{match } l \text{ with } | \text{Nil} \mapsto e_1 \mid \text{Cons}(hd, tl) \mapsto e_2$. The typing context has the form $\Gamma, l : L_{\pi}(n)(\tau') \vdash \tau$. From the operational semantics we know that $h.s(l).hd = v_{hd}$ and $h.s(l).tl = v_{tl}$, that is, $s(l) = \text{NULL}$. Due to the validity of $s(l)$ and Lemma 1, there exists $n_0 \geq 1$ in $p^1(\tau_\ast)$. From the validity $s(l) = \text{Valid}_{\text{val}}(s(l), \tau_{\text{ne}}, s, h)$ and the results above, we obtain that $\text{Valid}_{\text{store}}(s(l), \tau_{\text{ne}}, s, h)$ and the induction hypothesis yields $\text{Valid}_{\text{val}}(v_1, \tau_{\text{ne}}, h')$.

**OSLetFun:** Here $e = \text{letfun } f(f_1, \ldots, f_k, z_1, \ldots, z_k) = e_1 \text{ in } e_2$, where $s; h; C[l := ((g_1, \ldots, g_k, z_1', \ldots, z_k') \times e_1)] \vdash \tau_\ast$. From the LETFUN typing rule we have that $\Gamma, \tau_\ast \vdash \tau$, and $e_2 \vdash \tau$. Applying the induction hypothesis to these judgements with the same $n$ and $e$, we obtain $\text{Valid}_{\text{val}}(v, \tau_{\text{ne}}, h')$.

**OSFunApp:** In this case $e = f(f_1, \ldots, f_k, z_1', \ldots, z_k')$, where $C[e := ((g_1, \ldots, g_k, z_1', \ldots, z_k') \times e_1)] \vdash \tau \vdash v; h'$. From the LETFUN typing rule we have that $\Gamma, \tau \vdash \tau$, and $e_2 \vdash \tau$. Applying the induction hypothesis to these judgements with the same $n$ and $e$, we obtain $\text{Valid}_{\text{val}}(v, \tau_{\text{ne}}, h')$.
\( n'(a) = n(Ta) \), where \( Ta \) is such that \( a \) is replaced by \( Ta \) in the instantiation \( \sigma \) of the signature in this application of the \( \text{FUNApp} \)-rule.

\( e'(nij) = e(fij) \), where \( nij \) is replaced by \( fij \) in the instantiation \( \sigma \) of the signature in this application of the \( \text{FUNApp} \)-rule.

True holds trivially on \( \epsilon' \). From the induction hypothesis we have that if \( \text{Valid}_{\text{store}}((y_1, \ldots, y_k), (y_1 : T_{e_1}, \ldots, y_k : T_{e_k}), [y_1 := v_1, \ldots, y_n := v_n], h) \) then \( \text{Valid}_{\text{call}}(v, \tau_{e_1}, h') \).

From \( \text{Valid}_{\text{store}}(\text{dom}(s), \Gamma_{\text{nc}}, s, h) \) we get the validity of the values of the actual parameters: \( v_i \vdash_{\text{c}}^{\tau_{\text{nc}(i)}} w_i \) for some \( w_i \), with \( 1 \leq i \leq k \). Since \( \Gamma_{\text{nc}(i)} = \tau_{e'_i} \), the left-hand side of the implication holds, and one obtains \( \text{Valid}_{\text{call}}(v, \tau_{e'_i}, h') \). It is easy to see that

\[
\sigma(\tau_0)) = \eta(\tau_0)[\ldots \alpha := \tau_0 \ldots][\ldots nij := fij \ldots] =
\tau_0[\ldots \alpha := \eta(\tau_0) \ldots][\ldots nij := e(fij) \ldots] = \tau_{e'_i}.
\]

Therefore, we obtain \( \text{Valid}_{\text{call}}(v, \sigma(\tau_{0pc}), h') \) and using the rule \( \text{D \vdash \tau \rightarrow } \sigma(\tau_0) \) we obtain \( \text{Valid}_{\text{call}}(v, \tau_{e'_i}, h') \) by Lemma 2.

\[\square\]

4 Inferring Families of Polynomials

Consider a multivalued size function \( f \) over variables \( \bar{n}^* \) given by (recursive) rewriting rules. Our aim is to obtain a closed form (i.e. a recursion-free form) of \( f \). It is clear that this is not always possible. In this section, we show how to obtain an approximation of the closed form of \( f \) by constructing a family (i.e. a set) that includes the range of \( f \).

Let \( \bar{n} \subseteq \bar{n}^* \) be the list of all first-layer variables of \( \bar{n}^* \). For any variable \( n^*_i \in \bar{n}^* \) of a layer \( s \geq 2 \), let its range be given in the form \( T(n^*_i) = \{p(n, n', i) \mid Q_i(n, n', i)\} \), which is a short cut for \( \{p(n_0, n_0', i) \mid Q_i(n_0, n_0', i)\} \). Here \( Q \) is a first-order arithmetic predicate and \( n_0' \) are fresh w.r.t. \( \bar{n} \). We introduce fresh size variables like \( n_0' \) and assumptions as the one above if we know nothing about \( n^*_i \), where \( s \geq 2 \). In general such default assumptions are of the form \( \text{range}(n_0') \subseteq \{i\}_{0 < i < n_2} \).

We will show how, given a conditional rewriting rule with the l.h.s \( D_1(\bar{n}, \bar{\bar{n}}) \land D_2(\bar{n}, \bar{\bar{n}}, \bar{\bar{\bar{n}}}), \) to obtain \( \{p(\bar{n}, \bar{n}', i) \mid Q(n, n', i)\} \) such that if for all higher-layer variables \( \text{range}(n^*_i) \subseteq T(n^*_i) \) and \( D_1(\bar{n}, \bar{\bar{n}}) \) holds then \( f(n^*_i) \subseteq \{p(\bar{n}, \bar{n}', i) \mid Q(n, n', i)\} \).

Sometimes it is convenient to consider more specific estimates, where positions are mentioned explicitly. For instance, \( \text{tail}_2(n)(\text{pos}) = n - \text{pos} \) for \( n \geq 1 \) and \( 0 < \text{pos} < n - 1 \). Such position-aware estimates may be used to obtain tight position-free bounds on the overall size of the output structure. This is done by summations over positions. In the example above we have that the overall length of the internal lists is \( \sum_{\text{pos}=0}^{n-1} \text{tail}_2(n - \text{pos}) = \sum_{\text{pos}=0}^{n-1} (n - \text{pos}) = n(n + 1) - \frac{n^2}{2} \). This is definitely more precise than the position-free estimate \( \text{tail}_2(n) \subseteq \{i\}_{0 < i < n} \). In general, position-aware estimates for bound of internal lists have the form \( \text{range}(n^*_i) \subseteq T(n^*_i) \land D(\bar{n}, \bar{n}', \bar{\bar{n}}) \implies f(n^*_i) \subseteq \{p(\bar{n}, \bar{n}', \bar{\bar{n}}, \text{pos}) \mid Q(n, n', \text{pos}, i) \} \land D(n, n', \text{pos}) \).
4.1 Generating a candidate family to cover the range of a size function

Our main assumption is that for any fixed $n_0, n_0'$ the sets $T(n^*_0)$ are finite. For instance, for $n' = 3$ the range of $M$ is included into the set $(T(M) = \{i\}_{0 \leq i < n'} = \{0, 1, 2, 3\})$. Moreover, for fixed $n$ and $n'$ the function $M$ is reduced to the finite multivalued map $\phi$ such that $\phi(pos)$ is the set of all possible lengths of the “inner” lists. E.g. with $n = 2$ and $n' = 3$ we have $\phi$ instantiated as $\phi(0) = \phi(1) = \{0, 1, 2, 3\}$.

With fixed $n$ and $n'$ the function $f$ is translated to an auxiliary function $\mathcal{f}_j$ over finite sets and maps. For instance, $\text{concat}(n, M)$ becomes $\mathcal{f}_j(n, \mathcal{f}(\mathcal{f}(\phi(0)) + \mathcal{f}(\phi(n - 1, \mu_{+1})))$. Now we show how to translate $f$ to the function $\mathcal{f}_j$, which will be used later to obtain a family of polynomials that possibly covers the range of $f$.

Rewriting rules for an auxiliary function over finite sets We are going to introduce auxiliary functions of type

\[(\text{FiniteSet}, \text{FiniteMMap})^* \rightarrow \text{FiniteSet}\]

where \((\text{FiniteSet}, \text{FiniteMMap})^*\) is a finite Cartesian product of finite sets and finite multivalued maps. Binary arithmetic operations are lifted to sets: if $\oplus$ is one of the arithmetic operations $\oplus, -, +$, then $\mu_1 \oplus \mu_2 := \{x \oplus y\}_{x \in \mu_1 \land y \in \mu_2}$.

A finite multivalued map is a mapping from positions to finite sets: $\text{FiniteMMap} : \text{Positions}_{\tilde{d}_1} \rightarrow \ldots \rightarrow \text{Positions}_{\tilde{d}_k} \rightarrow \text{FiniteSet}$

where \(\text{Positions}_{\tilde{d}_k} = \{0, \ldots, d_k - 1\}\). An example of finite multivalued maps is $\langle \{1, 2, 3\}, \{1\}\rangle$, which sends 0 to $\{1, 2, 3\}$ and 1 to $\{1\}$. We denote a multivalued map via $\phi$ and $\mu$ denotes either a finite map or set. There is an empty map denoted via ( ). The only operation over multivalued maps, which is relevant to our task, is left shift $\lbrack - \rbrack_k$ sending $\langle \mu_0, \ldots, \mu_{d - 1}\rangle$ to $\langle \mu_k, \ldots, \mu_{d - 1}\rangle$.

Symmetrically, to mirror constructor application we could have used concatenation operation on finite multivalued maps. However, we do not use concatenation here. The reason is that this operation is defined explicitly via the rewriting rules in the antecedent of the CONS-rule, so it is not a part of the syntax of size annotations. Therefore, here it will be not a part of the syntax of expressions over finite sets and multivalued maps, but will be defined within rewriting systems for functions over finite sets and multivalued maps, when necessary.

The straightforward translation $\mathcal{L} - \mathcal{J}$ that maps size expressions onto expressions over finite sets and finite multivalued maps is inductively defined on the structure of size expressions. We define the translation $\mathcal{L} - \mathcal{J} : \text{SizeExpressions} \rightarrow \text{FiniteMMapSetExpressions}$ as follows:

- first-layer constants represent themselves: $\mathcal{L}a := a$;
- higher-layer constants, $s \geq 2$ are translated into their restrictions: $\mathcal{L}a^s := a^s$; since we fix the sizes of lists, then e.g. for $s = 2$ the map $a^2$ represents the restriction of the map $a^2$ to the set $\{0, \ldots, \max \{p^1(\mu^0)\} - 1\}$, where the expression $p^1$ is given by the type $L_{p^1(\mu^0)}(L_{a^2}(\ldots))$;
for instance, $\alpha^2 = a^2$, where $a^2(0) = 0$ and $a^2(1) = \{0, 1\}$ and $a^2$ is taken from the type $L_{n+2}(L_{2(\ldots)})$ with $n := 0$.

- positions $\text{pos}$ and first-layer variables $n$ are translated to themselves: $\text{pos}_j := \text{pos}$ and $\text{n}_j := n$; they represent the corresponding singleton sets;
- for a higher-layer variable $n^s$ from the set of parameters $\overline{n}^s$; where $s \geq 2$, we introduce a fresh variable $\phi$; $\text{n}^s_j := \phi$;
- translation $\text{p}_1 \oplus \text{p}_2 \mapsto \text{p}_1 \oplus_1 \text{p}_2 \oplus_2$ is defined on first-layer size expressions;
- $\text{p}_{s+1} := \text{p}_{s+1}$, where $p'$ is a first-layer expression with no free occurrences of $\text{pos}$;
- $\text{p}_j := \text{p}_j$ if $\text{p}_j$ is defined on first-layer size expressions;
- $\text{p}_j := \text{p}_j$, where $\text{p}_j$ is a first-layer expression with no free occurrences of $\text{pos}$;
- $(\text{p})(\text{pos}_j) := \text{p}(\text{pos}_j),$
- $\text{g}(\text{p}_1, \ldots, \text{p}_{k}) := \text{g}(\text{p}_1_j, \ldots, \text{p}_{k_j})$.

Given a rewriting rule $f(n^1, \ldots, n^k)(\text{pos}_1, \ldots, \text{pos}_{s-1}) \rightarrow p$ for a numerical multivalued function $f$, we construct the corresponding rewriting rule for $\text{f}_j$ as $\text{f}_j(n^1_j, \ldots, n^k_j)(\text{pos}_1, \ldots, \text{pos}_{s-1}) \rightarrow \text{p}_j$. For instance, the rewriting rule $n \geq 1, 0 \leq \text{pos} \leq n - 1 \rightarrow \text{tails}_2(n)(\text{pos}) \rightarrow \text{tails}_2(n-1)(\text{pos} - 1)$ is translated to $n \geq 1, 0 \leq \text{pos} \leq n - 1 \rightarrow \text{tails}_2(n)(\text{pos}) \rightarrow \text{tails}_2(n-1)(\text{pos} - 1)$.

**Generating a family** Consider a branch of $f$, defined by the rule $D_1(\overline{n}, \overline{m}) \land D_2(\overline{m}, \text{pos}) \vdash f(\overline{n})(\text{pos}) \rightarrow p$. We will construct an estimate for the range of $f$ in the form $\{f_l(n, n')(\text{pos}) \leq f(n, n')(\text{pos}) \leq f_u(n, n')(\text{pos})\}$, where $\text{f}_l(n, n')(\text{pos}) \leq f(\overline{n})(\text{pos}) \leq f_u(n, n')(\text{pos})$. We show now how to compute candidates for bounds $f_l$ and $f_u$ if they are polynomial. First, we need to assume their degree(s) $d$.

1. Choose $(V + d)$ points $(n_0, n'_0, \text{pos}_0)$, for which there exists $m$ such that $D_1(n_0, m) \land D_2(m, \text{pos})$ holds, that uniquely define a polynomial of degree $d$ with $V = |n| + |n'| + |\text{pos}_0|$ variables. We have discussed how to choose such points in [17]. For instance, assuming $d = 2$ for $\text{concat}(n, M)$ we take the finite set of test points $(n_0, n'_0, \text{pos}_0) = \{(1, 1), (2, 1), (3, 1), (1, 2), (2, 2), (1, 3)\}$. For instance, assuming $d = 1$ for $\text{tails}_2(n)(\text{pos})$ and $\text{tails}_2(n)(\text{pos})$ we take the set of test points $(n_0, \text{pos}_0) = \{(2, 0), (2, 1), (3, 0)\}$.

2. For each $(n_0, n'_0, \text{pos}_0)$ from the set of test points do:
   (a) for any $n_i \in \overline{n}$ assign $\phi_i := \lambda \text{pos}'. (p_i(n_0, n'_0, \text{pos}'))$, which is a constant multivalued map; e.g. $\phi := \{(0, 1)\}$ for $M$ in $\text{concat}(n, M)$ with $n = 1$, $n' = 1$; for instance, for $\text{concat}(n, \overline{n})$, with $n = 2$ and $n' = 3$ we have $\phi(2, 3) = \{(2)\}$ and $\phi(2, 3) = \{(0, 1, 2, 3), (0, 1, 2, 3)\}$;
   (b) compute $\text{f}_j(n, \phi)(\text{pos})$ using the rewriting rules; e.g.
      
      $\text{concat}(n(2, 3), \phi(2, 3)) \rightarrow \phi(2, 3)(0) \oplus \text{concat}(n(2, 3) - 1, \phi(2, 3) + 1) = \{(0, 1, 2, 3)\}$;
      $\text{concat}(2 - 1, \{(0, 1, 2, 3)\}) \oplus \{(0, 1, 2, 3)\} = \{(0, 1, 2, 3)\}$;
      $\text{concat}(1, \{(0, 1, 2, 3)\}) \oplus \{(0, 1, 2, 3)\} = \{(0, 1, 2, 3)\}$;
      $\text{concat}(0) \oplus \{(0, 1, 2, 3)\} = \{(0, 1, 2, 3)\}$;
      $\text{concat}(0, \{(0, 1, 2, 3)\}) = \{(0, 1, 2, 3)\}$;
      $\text{concat}(0, 6) \oplus \{(0, 1, 2, 3)\} = \{(0, 1, 2, 3)\}$;
      yet another example is $\text{tails}_2(2)(1) \rightarrow \text{tails}_2(2 - 1)(1 - 1) = \text{tails}_2(1)(0) \rightarrow 1$.  

19
(c) assign \( f_{\text{min}}(\overline{n}, \overline{n}', \overline{pos}_0) := \min (f_i) \) and \( f_{\text{max}}(\overline{n}, \overline{n}', \overline{pos}_0) := \max (f_i) \); e.g. \( \text{concat}_{\text{min}}(1,3) := 0 \) and \( \text{concat}_{\text{max}}(1,3) := 3 \); also \( \text{tail2}_{\text{min}}(2,1) = \text{tail2}_{\text{max}}(2,1) = 1 \).

(d) add to the lists of equations w.r.t. the coefficients of \( f_i \) and \( f_u \) the equations with \( f_{\text{min}}(\overline{n}, \overline{n}', \overline{pos}_0) \) and \( f_{\text{max}}(\overline{n}, \overline{n}', \overline{pos}_0) \) on the r.h.s., respectively; e.g., \( \text{tail2}_u(2,0) \) defines \( 2a_{u,10} + a_{u,01} + a_{u,00} = \text{tail2}_{\text{max}}(2,1) = 1 \).

3. Solve the linear systems for the coefficients \( f_i \) and \( f_u \). For instance, solving the system for \( \text{concat}(n, n') \) and \( \text{concat}_u(n, n') \) gives \( \text{concat}(n, n') = 0 \) and \( \text{concat}_u(n, n') = nn' \); for \( \text{tail}2 \) we obtain \( \text{tail2}_i(n, pos) = \text{tail2}_u(n, pos) = n - pos \). Thus, we have obtained polynomial lower and upper bounds for the size function \( f \).

4. On the previous step we have obtained the bounds for the size function \( f \), from which construct a family of polynomials in the form given in the begin of this subsection.

If the size function is of the first layer, we output the family as it is. For instance, for \( \text{concat} \) we return \( \{i\}_{0 \leq i \leq m} \).

If \( f \) is of the layer \( s \geq 2 \), then the bounds depend on positions \( \overline{pos} \). In this case, replace \( \overline{pos} \) with new indices \( \overline{j} \) to obtain \( \{f_i(\overline{n}, \overline{n}', \overline{j}) + i \}_{0 \leq i \leq Q(\overline{n}, \overline{n}', \overline{j})} \) where \( Q' \) abbreviates \( 0 \leq i \leq f_i(\overline{n}, \overline{n}', \overline{j}) - f_i(\overline{n}, \overline{n}', \overline{j}) \) \( D_2(\overline{n}, \overline{j}) \) consists of disequations of the form \( 0 \leq j \leq m - 1 \) or \( 1 \leq j \leq m \). Replace \( m \) that belongs to the set \( p(\overline{n}')(\overline{pos}_1) \ldots (\overline{pos}_{s-1}) \) with the already derived upper bound for this set. For instance, for \( \text{tail2}_i(n) \) we obtain \( \{n - j\}_{1 \leq j \leq n - 1} \) on \( n \geq 1 \). The family is completed to \( \{n - j\}_{0 \leq j \leq n - 1} \) by \( \text{tail2}_i(n)(0) = n \).

The return family needs to be checked. The checking is done by reducing rewriting rules to set inclusions and, eventually, to first-order predicates. The reduction has been sketched in the introduction. For more detail, see 4.2.

If a type-checker accepts the family then the job is done. Otherwise we need to analyse the failure. Rejection may happen if either the program’s size bounds are not polynomial, or we have chosen wrong parameter \( d \) and/or the set of test points. We may repeat the procedure for a larger \( d \) and/or other test points (see [17] for a discussion on how to choose test points for such procedures).

4.2 Checking if a given family covers the range of a function

To give a sufficient condition for a given family of polynomials to cover the range of the function \( f \) we first need to fill-in the specification table \( T \) for functions \( g \) that occur in the rewriting rules for \( f \) and their variables (formal parameters).

Informally, the problem of checking if a family of polynomials \( T(f(\overline{n}')) \) “covers” a given multivalued function \( f \) amounts to checking if for any computation path for \( f(\overline{n}')(\overline{pos}) \) the result will be in \( (T(f(\overline{n}')) \). In other words, for any rewriting rule \( D \vdash f(\overline{n}')(\overline{pos}) \rightarrow p \) the following inclusion holds: \( D \vdash T(f(\overline{n}')) \supseteq \text{range}(p) \), given that the range each higher-layer size variable \( n^s \in \overline{n}^s \) is \( T(n^s) \).

Let \( \overline{n}_g \) be the list of the formal size parameters of \( g \) and \( \overline{n}_g \subseteq \overline{n}_g \) are first-layer variables. The table is constructed as follows.
- if $n_i^* \in \overline{n}_g$, where $s \geq 2$, then $T(n_i^*)$ is given in the form $\{p(\overline{n}_g, \overline{n}_g, i)\}_{Q(\overline{n}_g, \overline{n}_g, i)}$, where $\overline{n}_g$ are fresh first-layer size variables, and a polynomial $p(\overline{n}_g, \overline{n}_g, i)$ and a predicate $Q(\overline{n}_g, \overline{n}_g, i)$ are
  - either given by a user,
  - or are set by default to $\{i\}_{0 \leq i \leq n_1}$ or $\{i\}_{n_2 \leq i \leq n_2}$;
- $T(g(\overline{n}_g))$ has the form $\{p(\overline{n}_g, \overline{n}_g, i)\}_{Q(\overline{n}_g, \overline{n}_g, i)}$. Note, that we treat higher-layer constants as functions, that is their specifications must be present in the table as well, in the form $T(a) = \{p(\overline{n})\}_{Q(\overline{n})}$. In principle, the range of $a$ may be generated automatically and then there is no need to add it to the table $T$. To avoid technical overhead we do not consider this optimisation in the presented work and leave it for the future.

For instance, the table $T$, which is used to check the family $\{i\}_{0 \leq i \leq n'}$ for $\text{concat}$, contains $T(+, n_1, n_2) = n_1 + n_2$, $T(M) = \{i\}_{0 \leq i \leq n'}$, $T(\text{concat}, n, n') = \{i\}_{0 \leq i \leq n'}$.

Let $\overline{n}$ be the set of the free size variables of $f$. Let $\text{rhs}(f)$ denote the conditions from the rewriting rules defining $f$. The set $\text{rhs}(f)$ consists of memberships like $m \in p(\overline{n})$, position restrictions like $0 \leq \text{pos} \leq m - 1$ (from the definition of type rewriting) or $1 \leq \text{pos} \leq m$ (a side condition of the cons-rule) and disequations $m > 1$ (a side condition of the constructor-rule and of cons-branch in the match-rule).

**Definition 1.** The specification $T(f(\overline{n}^*))$ is valid if and only if given that the specifications of all functions $g \neq f$ used in its definition are valid, if $\overline{n}$, $\text{pos}$ are s.t. $f(\overline{n})(\text{pos})$ terminates, then $\forall n^* \in \mathbb{R}^*, s \geq 2$ $n^*(\text{pos}) \subseteq T(n^*)$ implies $f(\overline{n}^*)(\text{pos}) \subseteq T(f(\overline{n}^*))$.

Let $p_{\overline{n}^*, \text{pos}}$ denote a size expression with free size variables $\overline{n}$ and free position variables $\text{pos}$. The result of its application to some values $x^*, \text{pos}^*$ is denoted via $p_{\overline{n}^*, \text{pos}}(x^*, \text{pos}^*)$.

Next, we define a range map $\lbrack \cdot \rbrack : \text{SizeExpression} \rightarrow \text{IndexedPolynomial} \times \text{1stOrderPredicate}$, where the first-order predicate in the image delimits the indices of the polynomial. Let $\lbrack p \rbrack_1$ and $\lbrack p \rbrack_2$ stay for the first projection (the polynomial) and the second projection (the predicate that bounds the indices) of $\lbrack p \rbrack$, resp. A correct range map $\lbrack p \rbrack$ is defined by induction over the structure of its argument $p$, which is an expression with free size variables $\overline{n}$:

- for a first-layer constant $a$ the range map is defined obviously as $\lbrack a \rbrack := \{a\}$;
- $\lbrack a^s \rbrack := T(a^s)$, where $s \geq 2$;
- for a first-layer variable $n$ from the set of parameters $\overline{n}$ the range map is defined as $\lbrack n \rbrack := \{n\}$,
- for a higher-layer variable $n^s$ from the set of parameters $\overline{n}$, where $s \geq 2$, the range map is defined by the spec. table, $\lbrack n^s \rbrack := T(n^s)$;
- if $\circ$ is one of the arithmetic operations $+$, $-$, $*$, then $\lbrack p_1 \circ p_2 \rbrack := \lbrack p_1 \rbrack \circ_1 \lbrack p_2 \rbrack$;
- $\lbrack p(0) \rbrack := \lbrack p \rbrack$.
\[ (p(p_{pos})) := (p); \]
\[ (p(p_{pos} - 1)) := (p); \]
\[ (p_{-1}) := (p); \]

In a function call \( g(p_1, \ldots, p_k, p'_1, \ldots, p'_{k'}) \) we match the actual parameters with the formal parameters \( \overline{n}_g, \overline{n}'_g \) of the specification

\[
T(g(\overline{n}_g)) = \{ p(n_{g1}, \ldots, n_{gk}, \overline{n}_{p_j}, j) \} Q(n, n', i, j)
\]

First, note that since the function call terminates, then there must be a rewriting rule \( D_g \vdash g(\overline{n}_g) \rightarrow p_g \) applicable for this call. From what follows that if we replace in \( D_g \) the formal parameters \( \overline{n}_g \) with the corresponding actual size expressions, then the result of the replacement \( D'_g \) should be valid on the actual size expressions.

Now continue as follows:
1. we first (inductively) compute the range sets \( \{ p_l \} \) of the first-layer actual parameters \( p_l \), where \( 1 \leq l \leq k; \)
2. after that we (inductively) compute the range sets \( \{ p'_{l'} \} \) of the higher-layer actual parameters \( p'_{l'} \), where \( 1 \leq l' \leq k' \);
3. after that the most difficult part of the matching “formal vs. actual parameters” is to be done: finding a substitution \( \sigma : \text{FreshSizeVar} \rightarrow \text{IndexedPolynomial} \times \text{1stOrderPredicate}, \) such that for all formal \( n_g^\theta \), with \( T(n_g^\theta) = \{ p''_1(\overline{n}_g, \overline{n}_{p_j}, j) \} Q''(n, n', i, j) \), the following inclusion must be provable from \( D'_g \):

\[
\{ p'_{l'} \} \subseteq \{ p''_1((p_1)_{1, \ldots, (p_k)_k}, \sigma_1(\overline{n}_{p_j}), j') \} Q''((p_1)_{1, \ldots, (p_k)_k}, \sigma_1(\overline{n}_{p_j}), j') \land \\
\bigwedge_{l=1}^k (p_l'_{l})_2 \land \\
\bigwedge_{l=1}^{k'} \sigma_2(n_{p_j}^\theta)
\]

For the sake of convenience we denote the last set via \( \{ p'_{l'} \} \).

Finding a substitution \( \sigma \) is the most difficult part of the procedure. It is a source of undecidability of inference in general, since it amounts to the instantiation of existential quantifiers in Peano arithmetic. However, in some cases (e.g. for linear predicates) finding a substitution may be done automatically.

Eventually

\[
\{ g(p_1, \ldots, p_k, p'_1, \ldots, p'_{k'}) \} := \\
\{ p((p_1)_{1, \ldots, (p_k)_k}, \sigma_1(\overline{n}_{p_j}), j) \} Q((p_1)_{1, \ldots, (p_k)_k}, \sigma_1(\overline{n}_{p_j}), j) \land \\
\bigwedge_{l=1}^k (p_l'_{l})_2 \land \bigwedge_{l=1}^{k'} \sigma_2(n_{p_j}^\theta)
\]

Sometimes, for the sake of convenience, the polynomial \( p \) and the delimiting predicate \( Q \) form the specification \( T(program(\overline{n})) = \{ p(\overline{n}, n', i) \} Q(\overline{n}, n', \text{abbar}) \) are denoted via \( \{ program \}_1 \) and \( \{ program \}_2 \) respectively.
As an instance, consider the r.h.s. of the rewriting rule $n \geq 1 \vdash \text{concat}(n, M) \rightarrow M(0) + \text{concat}(n - 1, M + 1)$.

$$\begin{align*}
\text{concat}(n, M) &= M(0) + \text{concat}(n - 1, M + 1), \\
\text{concat}(n - 1, M + i) &= \text{concat}(n + 1, M + i), \quad \text{for } 0 \leq i < n.
\end{align*}$$

where $\sigma(n') = \{n'\}$. Note that the scope of an index limited to the set it is “attached” to.

Another example shows that substitutions for fresh size variables $\bar{n}_g$ are not always identities as in the example above. Consider the composition $\text{concat}(\text{tails}(l))$ with $l$ be of the type $L_n(a)$. We want to check the rough but still sound estimate $\text{concat} \circ \text{tails}(n) \subseteq \{i\}_{0 \leq i < n}$, where $\text{tails}(l)$ is defined as.

We already know that $T(\text{concat}(n, M)) = \{i\}_{0 \leq i < n}$ for $T(M) = \{i\}_{0 \leq i < n}$. Now we need to match $T(M)$ with the annotation of the actual parameter $L_{\text{tails}(n)}(\alpha)$. We know that $T(\text{tails}(n)) = \{i\}_{0 \leq i < n}$, so we assume $\sigma(n') = \{n\}$. Indeed, $\{\text{tails}(l)\} = \{i\}_{0 \leq i < n} \subseteq \sigma(T(M)) = \{i\}_{0 \leq i < n'}$, thus $\sigma$ is a valid substitution.

**Lemma 3 (Consistency of range map: basic).** Given an expression $p_{\bar{n}, \bar{\rho}, \bar{\varphi}}$, if the specifications $T(g(\bar{n}))$ of all the functions $g$ that occur in it are valid, then for all $\bar{n}', \bar{\rho}, \bar{\varphi}$, such that $\bigwedge_{m \geq n'} n^*(\bar{\rho}, \bar{\varphi}) \subseteq T(n')$ and $p_{\bar{n}, \bar{\rho}, \bar{\varphi}}(\bar{n}', \bar{\rho}, \bar{\varphi})$ terminates, the inclusion $p_{\bar{n}, \bar{\rho}, \bar{\varphi}}(\bar{n}', \bar{\rho}, \bar{\varphi}) \subseteq (p_{\bar{n}, \bar{\rho}, \bar{\varphi}})$ holds.

**Proof.** Fix $\bar{n}', \bar{\rho}, \bar{\varphi}$, such that $p_{\bar{n}', \bar{\rho}, \bar{\varphi}}$ terminates on them. The proof is done by induction on the structure of $p_{\bar{n}', \bar{\rho}, \bar{\varphi}}$.

- The statement of the lemma for the base cases (constants and variables) follows directly from the definition of $\{\ldots\}$ and the validity of the specifications for the higher-layer variables and constants.

- Let $p_{\bar{n}', \bar{\rho}, \bar{\varphi}} = p_1 \bar{n'}, \bar{\rho}, \bar{\varphi} \circ p_2 \bar{n'}, \bar{\rho}, \bar{\varphi}$. By induction assumption, $p_1 \bar{n'}, \bar{\rho}, \bar{\varphi}(\bar{n}', \bar{\rho}, \bar{\varphi}) \subseteq (p_{\bar{n}, \bar{\rho}, \bar{\varphi}})$, where $l = 1, 2$. From the definition $p_{\bar{n}, \bar{\rho}, \bar{\varphi}}(\bar{n}, \bar{\rho}) := p_1 \bar{n}, \bar{\rho}(\bar{n}, \bar{\rho}) \circ p_2 \bar{n}, \bar{\rho}(\bar{n}, \bar{\rho})$ it follows that $p_{\bar{n}, \bar{\rho}, \bar{\varphi}}(\bar{n}, \bar{\rho}) = (p_{\bar{n}, \bar{\rho}, \bar{\varphi}}(\bar{n}, \bar{\rho}) \circ \{1\} \cdot p_{\bar{p}, \bar{\rho}, \bar{\varphi}} := (p_{\bar{n}, \bar{\rho}, \bar{\varphi}})$.

- Let $p_{\bar{n}, \bar{\rho}, \bar{\varphi}} = p_1 \bar{n}, \bar{\rho}(\bar{n}, \bar{\rho})$. By induction assumption, $p_1 \bar{n}, \bar{\rho}(\bar{n}, \bar{\rho}, \bar{\varphi}) \subseteq (p_{\bar{n}, \bar{\rho}, \bar{\varphi}})$, where $l = 1, 2$. From the definition $p_{\bar{n}, \bar{\rho}, \bar{\varphi}}(\bar{n}, \bar{\rho}) := p_1 \bar{n}, \bar{\rho}(\bar{n}, \bar{\rho}) \circ p_2 \bar{n}, \bar{\rho}(\bar{n}, \bar{\rho})$ it follows that $p_{\bar{n}, \bar{\rho}, \bar{\varphi}}(\bar{n}, \bar{\rho}) = (p_{\bar{n}, \bar{\rho}, \bar{\varphi}}(\bar{n}, \bar{\rho}) \circ \{1\} \cdot p_{\bar{p}, \bar{\rho}, \bar{\varphi}} := (p_{\bar{n}, \bar{\rho}, \bar{\varphi}})$.

- The other cases, where $p$ is an application of another size expression to a position, are treated similarly.

- Let $p_{\bar{n}, \bar{\rho}, \bar{\varphi}} \equiv p_{\bar{n}, \bar{\rho}, \bar{\varphi}}^p + 1$ for some $p^p$, where $\bar{\rho}^p = \{\bar{\rho}, \bar{\rho}^p\}$. Therefore, $p_{\bar{n}, \bar{\rho}, \bar{\varphi}}(\bar{n}, \bar{\rho}) = p_{\bar{n}, \bar{\rho}, \bar{\varphi}}(\bar{n}, \bar{\rho}^p, \bar{\varphi})$. According to the induction assumption, $p_{\bar{n}, \bar{\rho}, \bar{\varphi}}(\bar{n}, \bar{\rho}, \bar{\varphi}) \subseteq (p_{\bar{n}, \bar{\rho}, \bar{\varphi}})$. According to the definition of $\{\ldots\}$, the last set is equal to $\{p_{\bar{n}, \bar{\rho}, \bar{\varphi}}\}$, which is exactly $p_{\bar{n}, \bar{\rho}, \bar{\varphi}}$. 23
Consider the function call
\[
g(p_1, \ldots, p_k, p_1', \ldots, p_k') = g(p_1, p_2, \ldots, p_k, p_1', \ldots, p_k')
\]
According to the actual-parameter listing, a formal parameter \(n^*_f\) of \(g\) is instantiated with the actual parameter expressed by \(p_1^*\). The similar holds for the first-layer formal and corresponding actual parameters. Now we want to apply the validity of \(T(g(n^*_g))\). Instantiate \(n^*_g\) with \(\sigma(n^*_g)\) from the definition of \(\langle - \rangle\) for the function call under consideration. Further, according to the induction assumption for the actual parameters \(p_1^* = p_1\) and the definition of \(\sigma\) we obtain
\[
p_1^*(n^*, \text{pos}) \subseteq \{p_1^*(p_1), \ldots, p_k^*(p_k), \sigma_1(n^*_g), \sigma_2(n^*_g)\} \conj \prod_{i=1}^k p_i^* \sigma(w_i^*), \sigma(w_i^*) \prod_{i=1}^k p_i^*
\]
This is exactly means, that the actual parameters satisfy the specifications for the corresponding higher-layer variables of \(g\). Therefore, we are allowed to apply the validity of \(T(g)\) and obtain:
\[
\langle g(p_1, \ldots, p_k, p_1', \ldots, p_k') \rangle (n^*, \text{pos}) \subseteq \{p_1, \ldots, p_k, p_1', \ldots, p_k'\} \cap \prod_{i=1}^k p_i^* \sigma(w_i^*), \sigma(w_i^*) \prod_{i=1}^k p_i^*
\]
where the last set is exactly \(\langle g(p_1, \ldots, p_k, p_1', \ldots, p_k') \rangle\) according to the definition of \(\langle - \rangle\).

Given a collection of a right-hand side conditions \(D\) or its instances by actual parameters, let \(\langle D \rangle\) denote the result of substituting of size expressions \(p\), which occurs in \(D\), for the corresponding sets \(\langle p \rangle\).

**Lemma 4 (Consistency of range map).** Given an expression \(p_{n^*, \text{pos}}\), let the specifications \(T(g(n^*_g))\) of all the functions \(g\) that occur in it be valid, except may be the specification \(T(f(n^*_f))\) for \(f\), for which we do not know if it is valid or not. Let for each rewriting rule \(D \vdash f(n^*_f) \rightarrow p_f\) the inclusion \(\langle D \rangle \vdash T(f(n^*_f)) \subseteq \langle p_f \rangle\) holds. Then for all \(n^*, \text{pos}\), such that \(\prod_{n^*} n^*_f \text{pos} \subseteq T(n^*)\) and \(p_{n^*, \text{pos}}\) terminates, the inclusion \(p_{n^*, \text{pos}}(n^*, \text{pos}) \subseteq \langle p_{n^*, \text{pos}} \rangle\) holds.

**Proof.** It is done by induction on the deepness of the recursion in the calls of \(f\) occurring in \(p_{n^*, \text{pos}}(n^*, \text{pos})\).

- If the deepness \(d = 0\), then \(f\) does not occur in \(p\). Hence, we apply Lemma 3 directly.
- Let the deepness \(d \geq 1\). Run the inductive proof on the structure of \(p\).
  - If \(p\) is NOT a call of \(f\), then the proof schema is the same as for the corresponding clause of Lemma 3.
Consider a function call
\[
[f(p_1, \ldots, p'_k, p_{k+1}, \ldots, p_{k+t})(n, \text{pos}) :=
\]
\[
f(p_1(n, \text{pos}), \ldots, p_{k-1}(n, \text{pos}), p'_k(n, \text{pos}), \ldots, p_{k+t}(n, \text{pos}))
\]
Since this call terminates, there must be a rule \( D \vdash T(f(n)) \rightarrow p_f \) applicable for the actual parameters of the call. According to the actual-parameter listing, a formal parameter \( n_S \) is instantiated with the actual parameter expressed by \( p_j(n^*) \). The similar holds for the first-layer formal and corresponding actual parameters and the corresponding instance of \( D \) should hold, allowing us to use the rewriting rule. Applying the rewriting rule we obtain
\[
[f(p_1, \ldots, p'_k)(n^*, \text{pos}) :=
\]
\[
f(p_1(n^*, \text{pos}), \ldots, p'_k(n^*, \text{pos})) =
\]
\[
p_f(p_1(n^*, \text{pos}), \ldots, p'_k(n^*, \text{pos}))
\]
We may apply induction-on-the-deepness assumption, since the deepness of the recursive calls of \( f \) in \( p_f \) is one less then in \( p \). Therefore,
\[
p_f(p_1(n^*, \text{pos}), \ldots, p'_k(n^*, \text{pos})) \subseteq \|p_f(p_1, \ldots, p_{k'})\|
\]
Now, as we have pointed out above, \( D \) implies \( \{D\} \). Therefore we may apply the inclusion \( \{D\} \vdash T(f(n^*)) \supseteq \{p\} \), more precisely, its instantiation with the first-layer actual parameters and \( \sigma(n^*) \) for the fresh size variables, taken from the definition of \( \{\_\} \) for function calls. Thus, we obtain that
\[
p_f(p_1(n^*, \text{pos}), \ldots, p'_k(n^*, \text{pos})) \subseteq
\]
\[
\|p_f(p_1, \ldots, p_{k'})\| \subseteq \|p_f(p_1, \ldots, p_{k'})\| \subseteq T(f(n^*))_{\sigma} = \text{definition} \|p_{n^*}, \text{pos}\|
\]

**Theorem 2 (Checking).** If all called in the definition of \( f \) functions \( g \neq f \) have valid specifications \( T(g(n^*_g)) \), and for each rule \( D \vdash f(n) \rightarrow p_f \), the inclusion \( \{D\} \vdash T(f(n)) \supseteq \|p\| \) holds then the specification \( T(f(n^*)) \) is also valid.

**Proof.** Fix some \( n^*, \text{pos} \) such that the function \( f \) is defined on them. It means that there must be a rewriting rule applicable to these parameters, say, \( D \vdash f(n^*)(\text{pos}) \rightarrow p \). Since this rule is used as the first rule to compute \( f(n^*)(\text{pos}) \) we obtain that \( f(n^*)(\text{pos}) = p \). Form Lemma 4 we obtain \( f(n^*)(\text{pos}) \subseteq \|p\| \). From the condition of the lemma we have \( f(n^*)(\text{pos}) \subseteq T(f(n^*)) \).

### 5 Related Work

This research extends our work [14, 17, 15] about shapely function definitions that have a single-valued, exact input-output polynomial size functions. Our non-monotonic framework resembles [2] in which the authors describe monotonic resource consumption for Java bytecode by means of Cost Equation Systems (CESs), which are similar to, but more general than recurrence equations. CESs
express the cost of a program in terms of the size of its input data. In a further step, a closed-form solution or upper bound can sometimes be found by using existing Computer Algebra Systems, such as Mathematica. This work is continued by the authors in [1], where mechanisms for solving and upper bounding CESs are studied. However, they do not consider non-monotonic size functions.

Our approach is related to size analysis with polynomial quasi-interpretations [6, 3]. There, a program is interpreted as a monotonic polynomial extended with the max operation. To our knowledge, non-monotonic quasi-interpretations have not been studied for size analysis, but only for proving termination [10]. In this work, one considers some unspecified algorithmically decidable classes of non-negative and negative polynomials and introduces abstract variables for the rest.

Hoffman and Jost have presented a heap space analysis [11] to infer linear space bound of functional programs with explicit memory deallocation. It uses type annotations and an amortisation analysis that assign a potential, i.e. hypothetical free space, to data structures. The type system ensures that the potential to the input is an upper bound on the total memory required to satisfy all allocations. They have extended their analysis to object-oriented programs [12], although without an inference procedure. Brian Campbell extended this approach to infer bounds on stack space usage in terms of the total size of the input [7], and recently as max-plus expressions on the depth of data structures [8]. Again, the main difference with our work is that we not require linear size functions.

The EmBounded project aims to identify and certify resource-bounded code in Hume, a domain-specific high-level programming language for real-time embedded systems. In his thesis, Pedro Vasconcelos [18] uses abstract interpretation to automatically infer linear approximations of the sizes of recursive data types and the stack and heap of recursive functions written in a subset of Hume.

Several papers have studied programming languages with implicit computational complexity properties [9, 5]. This line of research is motivated both by the perspective of automated complexity analysis and providing natural characterisations of complexity classes like PTIME or PSPACE. Resource analysis may also be performed within a Proof Carrying Code framework. In [4] the authors introduce resource policies for mobile code to be run on smart devices and certify resource bounds in a Proof Carrying Code system.

6 Conclusions and Future Work

We have presented a system that combines lower/upper bounds and higher-order size annotations to express, type check and infer reasonable approximations for polynomial size dependencies for strict functional programs using general lists.

Future work will include research on adding algebraic data types, making a prototype possibly using dependent types, applying the prototype for larger programs and transferring the results to an imperative object-oriented language.
References


