Typable Fragments of Polynomial Automatic Amortized Resource Analysis

Long Pham
Carnegie Mellon University, Pittsburgh, PA, USA
longp@andrew.cmu.edu

Jan Hoffmann
Carnegie Mellon University, Pittsburgh, PA, USA
janh@andrew.cmu.edu

Abstract
Being a fully automated technique for resource analysis, automatic amortized resource analysis (AARA) can fail in returning worst-case cost bounds of programs, fundamentally due to the undecidability of resource analysis. For programmers who are unfamiliar with the technical details of AARA, it is difficult to predict whether a program can be successfully analyzed in AARA. Motivated by this problem, this article identifies classes of programs that can be analyzed in type-based polynomial AARA. Firstly, it is shown that the set of functions that are typable in univariate polynomial AARA coincides with the complexity class \( \mathbf{PTime} \). Secondly, the article presents a sufficient condition for typability that axiomatically requires every sub-expression of a given program to be polynomial-time. It is proved that this condition implies typability in multivariate polynomial AARA under some syntactic restrictions.

2012 ACM Subject Classification Theory of computation → Type theory

Keywords and phrases Resource consumption, Quantitative analysis, Amortized analysis, Typability

Digital Object Identifier 10.4230/LIPIcs.CVIT.2016.23

Funding Long Pham: [funding]
Jan Hoffmann: [funding]

1 Introduction

There exists a wide range of effective techniques for automatically or semi-automatically analyzing the resource consumption of programs. These techniques derive symbolic bounds on the worst-case [25], best-case [10, 29], or expected [7, 30] resource consumption and are based on type systems [8, 33, 9, 27, 2, 6, 12], recurrence relations [34, 11, 1, 26, 24], relational reasoning [6, 31], and term rewriting [3, 5, 20].

State-of-the-art resource analyses can automatically derive complex bounds for large programs, and making analyses more practical by improving their efficiency and range is a main driving force in this area. However, resource analysis for Turing-complete languages is undecidable, and even for the most sophisticated tools there will remain programs that cannot be analyzed automatically. Diagnosing the cause and modifying the program so that the analysis can derive a bound often require in-depth knowledge of the implemented techniques. As a result, the usability of more sophisticated analysis tools is hampered by their complexity.

To improve the usability of automatic resource analysis for non-experts, this article develops easy-to-understand characterizations of the programs that can be analyzed with automatic amortized resource analysis (AARA). Such characterizations can serve as explanations for an unsuccessful resource analysis and guide program development without revealing technical details of the underlying analysis.
AARA is a type-based analysis that is based on the potential method of amortized analysis. It has been first introduced by Hofmann and Jost \cite{19} for deriving linear bounds heap-space bounds for a first-order language with lists. AARA has subsequently been extended to univariate polynomial bounds \cite{17,15}, and exponential bounds \cite{23}. Furthermore, AARA has been extended to other language features such as higher-order and polymorphic functions \cite{21,16}, lazy evaluation \cite{22}, and probabilistic programming \cite{30}. The analysis has been implemented in the programming language Resource-Aware ML (RaML) \cite{16}. An overview of polynomial AARA can be found in Section 2. We are not aware of previous work that studies the characterization of typable fragments of AARA.

Our first contribution (Section 3) is a characterization of the (mathematical) functions that can be implemented in AARA. We demonstrate that it is possible to embed every polynomial-time Turing machine in AARA, that is, for every such Turing machine, there exists a polynomial-time program that is equivalent to the Turing machine and is typable in polynomial AARA. This result shows that polynomial AARA corresponds to the complexity class $\text{PTime}$ and is in the tradition of implicit computational complexity (ICC) \cite{4,28,18}, which studies linguistic characterizations of complexity classes. For a user of RaML, this result means that an implementation of a $\text{PTime}$ function can always be rewritten so that a worst-case cost bound can be automatically derived. However, it does not provide guidance of how to rewrite an implementation.

An ideal resource analysis should automatically derive a cost bound for every program that has a polynomial bound. However, such an analysis does not exist, because the problem of deciding whether a given program runs in polynomial time is undecidable \cite{14}. Moreover, AARA is a type-based analysis that derives the bound of an expression from its sub-expressions. So we can only expect to derive a bound for an expression which is inherently polynomial time, that is, every subexpression is in $\text{PTime}$ if viewed as a function.

Our second contribution is an axiomatic definition of inherently polynomial time that implies typability in multivariate polynomial AARA for a Turing-complete first-order language with lists (see Section 2) under some restrictions: Programs can only use primitive recursion instead of general recursion, some variables are affine, and the use of nested lists is restricted. Although this characterization is far from being a necessary condition, we believe that it can be a valuable guide to users. A key concept is the notion of uniform resource annotations which is essential in the proof that inherently polynomial time is a sufficient condition for typability in multivariate polynomial AARA.

## 2 Automatic amortized resource analysis

Among approaches to resource analysis is automatic amortized resource analysis (AARA). Given a program $P$, consider its history of execution, that is, a sequence of transitioning program states. As in Sleator and Tarjan’s potential method in amortized analysis \cite{32}, we assign a certain (positive) amount of potential to the initial state of this sequence. If we can ensure that (i) the amount of potential never becomes negative throughout $P$’s run and (ii) the actual computational cost in each transition of $P$ is less than or equal to the change in the amount of potential, then we know that the total resource usage of $P$ is bounded above by the initial potential. This is essentially how AARA works.

More concretely, each sub-expression of $P$ is assigned a resource-annotated type: a conventional (i.e. simple) type augmented with an expression that indicates how much potential is stored. In polynomial AARA \cite{17,15}, we use polynomial functions to express potential.
Initially, AARA only assigns templates of resource-annotated types where coefficients of polynomials are left blank. AARA then collects constraints on these coefficients that respect the cost semantics of $P$. Finally, as these constraints are all linear, we can simply solve them using an off-the-shelf linear program solver, thereby inferring resource-annotated types. A worst-case cost bound of $P$ can be extracted from its resource-annotated type.

2.1 Resource-Aware ML

Resource-Aware ML (RaML) is a Turing-complete functional programming language used in the study of AARA [17].

The original version of RaML is first-order (i.e. no higher-order types or functions appear in RaML) and only offers a relatively small set of language features. Subsequent versions of RaML support more language features such as higher-order functions and polymorphic functions [16]. In this section, we describe a variant of RaML that only differs from the original version in a few minor details; e.g. the tick construct and the support for sum types.

The base types (denoted by $b$) and simple types (denoted by $\tau$) of RaML are formed by

\[
\begin{align*}
 b & ::= 1 & \text{unit type} \\
 b_1 + b_2 & \text{sum type} \\
 b_1 \times b_2 & \text{product type} \\
 L(b) & \text{list type.}
\end{align*}
\]

The set of all base types will be denoted by $B$.

Fix a set $V(\exists x)$ of variable symbols and a set $F(\exists f)$ of function symbols. The grammar of RaML is

\[
\begin{align*}
e & ::= x \quad \text{variable} \\
& \quad \langle \rangle \quad \text{unit element} \\
& \quad \ell \cdot x \mid r \cdot x \quad \text{sum} \\
& \quad \langle x_1, x_2 \rangle \quad \text{product} \\
& \quad [\ ] \mid x_1 :: x_2 \quad \text{list constructor} \\
\text{fun} & \quad f \ x \ e \quad \text{function definition} \\
& \quad x_1 \ x_2 \quad \text{function application} \\
\text{case} & \quad x \ \{ \ell \cdot y \mapsto e_\ell \mid r \cdot y \mapsto e_r \} \quad \text{case for the sum type} \\
\text{case} & \quad x \ \{ \langle x_1, x_2 \rangle \mapsto e \} \quad \text{case for the product type} \\
\text{case} & \quad x \ \{ [\ ] \mapsto e_0 \mid (x_1 :: x_2) \mapsto e_1 \} \quad \text{case for the list type} \\
\text{tick} & \quad q \quad \text{resource consumption; } q \in Q \\
\text{let} & \quad x = e_1 \ \text{in} \ e_2 \quad \text{let-binding} \\
\text{share} & \quad x \ \text{as} \ x_1, x_2 \ \text{in} \ e \quad \text{variable sharing.}
\end{align*}
\]

In a function definition, $e$ is allowed to mention $f$. Therefore, we can implement not only primitive recursion but also general recursion. As standard, we use the let-normal form, where we only permit function application of the form $x_1 \ x_2$ as opposed to $e_1 \ e_2$. For convenience in resource analysis, we require each variable symbol to be used in a affine manner (i.e. can only be used at most once). To use a variable symbol multiple times, we duplicate the symbol by the share construct.
RaML programs are evaluated using the call-by-value strategy. Computational costs accrue only when \( \text{tick} \) \( q \) is executed, and this cost metric is known as the tick metric. The general cost semantics of RaML can be found in [17]. In the case of the running time, which is a specific cost metric, of RaML, the judgment of the cost semantics has the form

\[
V \vdash e \Downarrow v \mid n,
\]

where \( V \) is an environment (i.e., a set of pairs of variable symbols and semantic values), \( v \) is a semantic value, and \( n \in \mathbb{N} \) is the running time of evaluating program \( e \) to \( v \). The running time is formally defined in Appendix B.

### 2.2 Univariate AARA

In univariate AARA, each list is annotated with a polynomial indicating the amount of the potential stored in the list. Univariate AARA does not let us mix potential of two lists, that is, multiply polynomials of two lists’ potential. This is why univariate AARA is called univariate.

Resource-annotated base types (denoted by \( b \)) and resource-annotated simple types (denoted by \( \tau \)) are formed by the following grammar:

\[
\begin{align*}
 b &::= 1 \quad \text{unit type} \\
 b_1 + b_2 &::= \langle b, q \rangle \quad q \in \mathbb{Q}_{\geq 0} \quad \text{sum type} \\
 b_1 \times b_2 &::= \langle b \rangle \quad \text{product type} \\
 L(b) &::= B_1 \rightarrow B_2 \quad \text{arrow type} \\
 L(\vec{q}(b)) &::= \langle L(b), 0 \rangle \quad \text{list type}.
\end{align*}
\]

Here, \( \vec{q} \) is a finite vector of \( \mathbb{Q}_{\geq 0} \).

Given a semantic value \( v : b \), where \( b \) is a resource-annotated base type, the potential stored in \( v \) is inductively defined as

\[
\begin{align*}
\Phi(v : 1) &= 0 \\
\Phi([] : L(\vec{q}(b))) &= 0 \\
\Phi(\ell \cdot v : b_1 + b_2) &= \Phi(v : b_1) + \Phi(v : b_2) \\
\Phi(r \cdot v : b_1 + b_2) &= \Phi(v : b_2),
\end{align*}
\]

where \( |\cdot| \) denotes the length of an input list. Given \( n \in \mathbb{N} \) and \( \vec{q} = (q_1, \ldots, q_k) \), \( \phi(n, \vec{q}) \) is defined as \( \phi(n, \vec{q}) := \sum_{i=1}^{k} q_i \binom{n}{i} \). If \( n < i \), then \( \binom{n}{i} = 0 \).

The typing judgment of univariate AARA has the form

\[
\Gamma_{\text{anno}}; p \vdash e : B,
\]

where \( \Gamma_{\text{anno}} \) is a resource-annotated typing context and \( p \in \mathbb{Q}_{\geq 0} \). We sometimes write \( \Sigma_{\text{anno}}; \Gamma_{\text{anno}}; p \vdash e : B \), where a resource-annotated typing context is split into \( \Gamma_{\text{anno}} \) for arrow-type variables and \( \Sigma_{\text{anno}} \) for base-type variables. The type system of univariate AARA is available in Appendix C.1.

To give examples of judgments in univariate AARA, consider two programs: (i) \textit{append} that appends the first input list to the second, and (ii) \textit{quicksort} that performs quicksort. The running time of \textit{append} is proportional to the size of the first input, and the running time of \textit{quicksort} is bounded by the square of the input size. For simplicity, we will not work out the exact coefficients of polynomial bounds—instead, we simply assume that the running time of \textit{append} and \textit{quicksort} can be bounded by \( n \rightarrow n \) and \( n \rightarrow n^2 \), respectively. It then makes sense that these two programs can be typed in univariate AARA as

\[
\begin{align*}
\text{append} : \langle L^1(b), L^0(b) \rangle, 0 \rightarrow \langle L^0(b), 0 \rangle \\
\text{quicksort} : \langle L^{(1,2)}(b), 0 \rangle \rightarrow \langle L^0(b), 0 \rangle.
\end{align*}
\]
The univariate resource annotation \((1, 2)\) of quicksort represents polynomial \(n \mapsto 1 \cdot \binom{n}{1} + 2 \cdot \binom{n}{2} = n^2\). The implementations of append and quicksort are given in Appendix C.2.

Univariate AARA is sound with respect to the cost semantics (specifically, the running time) of RaML:

**Theorem 1 (Soundness of univariate AARA [17]).** Given term \(e\), suppose \(\Gamma_{\text{anno}}; p \vdash e : \langle b_{\text{anno}}, q \rangle\) is derived in univariate AARA. Let \(V\) be an environment such that \(V \vdash e \Downarrow v \mid n\); that is, \(e\) runs in \(n\) units of time under \(V\). We then have

\[
n \leq p + \Phi(V : \Gamma_{\text{anno}}) - q - \Phi(v : b_{\text{anno}}),
\]

where \(\Phi(V : \Gamma_{\text{anno}}) = \sum_{x \in \text{dom}(\Gamma_{\text{anno}})} \Phi(V(x) : \Gamma_{\text{anno}}(x))\).

### 2.3 Multivariate AARA

In contrast to univariate AARA, multivariate AARA allows us to mix potential of different lists. For example, we can have \(|\ell_1| \cdot |\ell_2|\)'s worth of potential, where \(|\cdot|\) denotes the length of a list, in multivariate AARA. Due to this multivariate nature, multivariate AARA has a single global resource annotation represented by a multivariate polynomial over all size variables occurring in a given term. This global resource annotation is separate from individual types in a typing context.

Multivariate AARA is strictly more expressive than univariate one. This is surprising in light of the fact that multivariate polynomials can always be bounded by univariate polynomials; e.g. \(xy\) is bounded by \(x^2 + y^2\). Examples of programs that cannot be typed in univariate AARA but multivariate AARA are available in Section 4.1 and Section 5.

#### Resource-annotated types

Resource-annotated types in multivariate AARA are formed by

\[
\begin{align*}
&b ::= 1 \quad \text{unit type} & &B ::= \langle b, Q \rangle \quad \text{base type} \\
&b_1 + b_2 \quad \text{sum type} & &\tau ::= \langle b \rangle \quad \text{arrow type} \\
&b_1 \times b_2 \quad \text{product type} & &B_1 \rightarrow B_2 \\
&L(b) \quad \text{list type}.
\end{align*}
\]

In \(\langle b, Q \rangle\), \(Q\) is a multivariate resource annotation over the size variables inside \(b\). This will be formalized shortly.

Given a base type \(b \in \mathbb{B}\), its base polynomial is a function of type \([b] \mapsto \mathbb{N}\), where \([b]\) is the set of semantic values of type \(\tau\). The set of base polynomials associated with type \(b\), denoted by \(B(b)\), is inductively defined as follow:

\[
\begin{align*}
B(1) & := \{ \lambda v.1 \} \\
B(b_1 + b_2) & := \{ \lambda (\ell \cdot v). p(v) \mid p \in B(b_1) \} \cup \{ \lambda (r \cdot v). p(v) \mid p \in B(b_2) \} \\
B(b_1 \times b_2) & := \{ \lambda (v_1, v_2). p_1(v_1) \cdot p_2(v_2) \mid p_1 \in B(b_1) \} \\
B(L(b)) & := \{ \lambda [v_1, \ldots, v_n]. \sum_{1 \leq j_1 < \cdots < j_k \leq n} \prod_{1 \leq i \leq k} p_i(v_{j_i}) \mid k \in \mathbb{N}, p_i \in B(b) \}.
\end{align*}
\]

For \(b_1 + b_2\), we have a set of base polynomials for the \(\ell\)-tag and another set for the \(r\)-tag. If a base polynomial is applied to a value with a wrong tag, we assume that the output is 0. For instance, if we feed \(\lambda (r \cdot v).1\) to a value \(\ell \cdot \langle \rangle\), the output should be 0. In the definition of \(B(L(b))\), if \(n < k\), the function should return 0 since it is the identity of summation.
Given base type \( b \), a resource polynomial \( p : [b] \to \mathbb{Q}_{\geq 0} \) is a non-negative linear combination of finitely many base polynomials from \( \mathcal{B}(b) \). It is straightforward to prove that \( \mathcal{B}(b) \) for any \( b \) contains \( \lambda v.1 \). Therefore, a resource polynomial is always capable of expressing constant potential.

For convenience, it is desirable to have a succinct notation for base polynomials. This is achieved by introducing indexes of base polynomials:

\[
\begin{align*}
\mathcal{I}(1) & := \{ * \} \\
\mathcal{I}(b_1 + b_2) & := \{ \ell \cdot i \mid i \in \mathcal{I}(b_1) \} \cup \{ r \cdot i \mid i \in \mathcal{I}(b_2) \} \\
\mathcal{I}(b_1 \times b_2) & := \{ (i_1, i_2) \mid i_1 \in \mathcal{I}(b_1), i_2 \in \mathcal{I}(b_2) \} \\
\mathcal{I}(B(b)) & := \{ [i_1, \ldots, i_k] \mid k \in \mathbb{N}, i_j \in \mathcal{I}(b) \}.
\end{align*}
\]

An index is usually used as a subscript for a (meta)-variable representing a coefficient of a base polynomial. For instance, \( q_{(*, *)} \in \mathbb{Q}_{\geq 0} \) is a meta-variable representing a coefficient of base polynomial \( \lambda (v_1, v_2).1 \). For any base type \( b \), we will write \( 0_b \) for the index \( \lambda v.1 \).

The degree of an index is defined by

\[
\begin{align*}
\deg(\ast) & := 0 \\
\deg((i_1, i_2)) & := \deg(i_1) + \deg(i_2) \\
\deg(\ell \cdot i) & := \deg(i) \\
\deg([i_1, \ldots, i_k]) & := k + \sum_{1 \leq j \leq k} \deg(i_j).
\end{align*}
\]

Because a resource polynomial can only have non-zero coefficients for finitely many base polynomials, any resource polynomial (or a finite set of resource polynomials) has a bounded degree. In practice, we ask a user of AARA to supply an upper bound on the degree of base polynomials.

**Resource annotations of typing contexts**

Given a base-type typing context \( \Gamma = \{ x_1 : b_1, \ldots, x_n : b_n \} \), its multivariate resource annotation is given by a resource polynomial of type \( b_1 \times \cdots \times b_n \). In other words, we treat a typing context as one big tuple and assign a single multivariate annotation to this tuple.

With regard to an arrow-type typing context \( \Sigma = \{ f_1 : b_{1,1} \to b_{1,2}, \ldots, f_m : b_{m,1} \to b_{m,2} \} \), its multivariate resource annotation has the form

\[
\Sigma_{\text{anno}} = \{ f_1 : B_{1,1} \to B_{1,2}, \ldots, f_m : B_{m,1} \to B_{m,2} \},
\]

where each \( B_{i,j} \) is a pair \( \langle h_{i,j}, Q \rangle \) such that \( Q \) is a multivariate resource annotation of \( h_{i,j} \).

**Typing judgment**

The typing judgment of multivariate AARA takes the form

\[
\Gamma ; P \vdash e : \langle b, Q \rangle,
\]

where \( \Gamma \) and \( b \) are free of resource annotations. \( P \) and \( Q \) are multivariate annotation over \( \Gamma \) and \( b \), respectively. The type system of multivariate AARA is available in Appendix D.2.

To give examples of judgments in multivariate AARA, consider append \( \ell_1 \), \( \ell_2 \), which appends \( \ell_1 \) to \( \ell_2 \). Suppose that the output must store \( n \to n^2 \) much potential. It is reasonable that the total potential required for this program is \( |\ell_1| + (|\ell_1| + |\ell_2|)^2 \), out of which \( |\ell_1| \) is used to account for the running time. This can be expressed by the judgment
exists a RaML program A (deterministic) Turing machine AARA and that simulates where

This amounts to $2 \cdot (\ell_1 + \ell_2) + 1 \cdot \ell_1$, which is equal to $|\ell_1| + (|\ell_1| + |\ell_2|)^2$ as desired.

The multivariate equivalent of the soundness theorem (Theorem 1) holds [15].

3 Embedding polynomial-time Turing machines in AARA

In this section, we show that every polynomial-time Turing machine can be expressed as a typable Resource-Aware ML (RaML) program while preserving the semantics and worst-case cost bounds. More formally, we have

> **Theorem 2** (Embedding of polynomial-time Turing machines in RaML). Let $M$ be a polynomial-time Turing machine that inputs and outputs bit strings from $\{0, 1\}^*$. There exists a RaML program $M'$ : $\{0, 1\}^* \rightarrow \{0, 1\}^*$ such that

- For every input $w \in \{0, 1\}^w$, we have $M(w) = M'(w)$;
- The computational cost of $M'$ (according to the tick metric) is larger than or equal to the running time of $M$;
- Univariate AARA can infer a polynomial upper bound of the computational cost of $M'$.

Theorem 2 only tells us the existence of a RaML program $M'$ that is typable in univariate AARA and that simulates $M$ faithfully. In our proof of the theorem, we assume that a polynomial bound on the running time of $M$ is known. Thus, if we do not have access to this polynomial bound, we cannot construct $M'$. In fact, the problem of determining whether a given Turing machine runs in polynomial time or not is undecidable [14].

It is fairly easy to prove that the cost of any program according to the tick metric is asymptotically bounded by its running time. Therefore, in the statement of Theorem 2, we can replace the “tick metric” with the “running time” of RaML.

A detailed proof of Theorem 2 is available in Appendix A.

3.1 Preliminaries

A (deterministic) Turing machine $M$ is specified by an 8-tuple $(Q, \Sigma, \Gamma, \vdash, \sqcup, \delta, q_0, q_{\text{final}})$, where

- $Q$ is a finite set of machine states.
- $\Sigma$ is a finite input alphabet. $\Gamma$ is a finite alphabet for symbols written on $M$’s tape. Since an input will be initially placed on the tape, every input symbol is also a tape symbol.
- $\vdash \in \Gamma \setminus \Sigma$ is the left end marker that demarcates the left end of a semi-infinite working tape, and $\sqcup \in \Gamma \setminus \Sigma$ is the blank symbol for the tape.
- $\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$ is the transition function.
- $q_0 \in Q$ is the initial state, and $q_{\text{final}} \in Q$ is the final state.

In the initial configuration of a Turing machine, an input string $w$ is placed immediately after the left end marker $\vdash$ on the tape. The state of the machine is initially $q_0$, and the read/write head is positioned on the first symbol of $w$. The rest of the tape is filled with $\sqcup$.

The Turing machine first (i) reads the content of the cell currently under the tape head and (ii) identifies the current state of the machine. The machine then overwrites the current cell (if necessary), updates the machine’s state, and moves the head to the left or right.
Typable Fragments of Polynomial Automatic Amortized Resource Analysis

where

3.2 Embedding

Fix a polynomial-time Turing machine $M = (Q, \Sigma, \Gamma, \vdash, \sqcup, \sqcap, \delta, q_0, q_{\text{final}})$. Assume that the running time of $M$ is bounded above by $p(n)$ for some polynomial $p : \mathbb{N} \to \mathbb{N}$. The target program of the translation will be denoted by $M'$, and this is what we are about to define. $M'$ works as described in Algorithm 1.

```
Procedure $M'(w)$

1. Create a list $\ell_1 : L(\text{Sym})$ containing $\vdash$
2. Create a list $\ell_2 : L(\text{Sym})$ of size $p(|w|)$ filled with $\sqcup$
3. Prepend $\ell_2$ with $w$
4. while $s \neq q_{\text{final}} \land ps \neq \text{nil}$ do
5. Use $\ell_2$ to simulate the transition function $\delta$
6. Update $s$ and $\ell_2[0]$ appropriately
7. Update the tape head’s position by moving the head of $\ell_1$ or $\ell_2$ to the other
8. $ps \leftarrow \text{tail } ps$
9. $ps \leftarrow \text{tail } ps$
10. $s \leftarrow q_0$
11. $s \leftarrow q_0$
12. return $\text{append}(\text{reverse } \ell_1, \ell_2)$
```

The list $\ell_1$ represents the region on $M$’s tape to the left of the tape head (in the reverse order and excluding the cell where the tape head is currently on), and $\ell_2$ represents the region to the right of the head (including the current cell). Since it is assumed that $p(|w|)$, where $|w|$ denotes the length of input list $w$, is an upper bound on $M$’s running time, we are assured that $M$ requires at most $p(|w|)$ many cells on the working tape. This is why $\ell_2$ initially has size $p(|w|)$. In fact, because we prepend $\ell_2$ with $w$ in line 4, we have $|w|$ more cells than necessary.

The list $ps$ acts as a reservoir of potential, storing constant potential in each element. As the head of $ps$ is removed in line 8, the potential stored in this element is freed and will be consumed in subsequent lines inside the loop’s body.

It is technically possible to store potential directly in $\ell_1$ and $\ell_2$, which together simulate $M$’s working tape. However, not all cells on the working tape of $M$ are accessed equally often—some cells are accessed more often than others, and the maximum number of accesses to a given cell may not be bounded by a constant. If we are to store potential in $\ell_1$ and $\ell_2$, each cell of $\ell_1$ and $\ell_2$ needs to store $p(n)$ units of potential at the beginning. As a result, the total amount of potential supplied to $M'$ is $p^2(n)$, which is a gross over-approximation of the
actual running time. Therefore, to have a tighter cost bound, a separate list, namely \( ps \), is employed as a reservoir of potential.

4 Inherently polynomial time

Section 3 investigates the expressive power of AARA from the viewpoint of programming language semantics, disregarding the issue of how to algorithmically turn an arbitrary Turing machine into a typable RaML program. By contrast, in this section, we aim to identify a typable fragment of AARA that is defined statically/axiomatically. The sufficient condition corresponding to the typable fragment that this section presents is named \textit{inherently polynomial time}.

A key requirement is that the typable fragment should not resemble AARA’s type system, which itself is also defined axiomatically. Otherwise, it would be trivial to prove that any term in this fragment is typable in AARA. Because we want users of AARA to benefit from our findings of the present work, another requirement is that the definition (or at least the informal definition) of inherently polynomial time should be easy to convey to users of AARA.

On the other hand, it is not our priority to find as large a typable fragment as we can. In the remaining of the article, we will focus on the running time as a cost metric of RaML, unless stated otherwise.

4.1 High-level design

By Theorem 1 (and its multivariate equivalent), AARA is sound: if a program is typable in AARA, its resource-annotated type is a correct upper bound on the running time. Hence, to be typable in AARA, the worst-case running time of a program must be polynomial. To ensure termination of programs, we first restrict recursion to primitive recursion.

Furthermore, the type system of AARA is compositional: if term \( e \) is typable, so is every sub-expression of \( e \). Hence, in order for \( e \) to be typable, not only \( e \) but also all of its sub-expressions must be polynomial-time. This suggests that we should define the sufficient condition inductively, hence the name \textit{inherently polynomial time}.

It is straightforward to determine whether each of the base cases of the inductive definition is typable or not. It remains to work out inductive cases in the inductively defined sufficient condition for typability. The most interesting case is primitive recursion. Consider

\[ e := \text{rec } x \{ [] \mapsto e_0 \mid (y :: ys) \with z \mapsto e_1 \}. \]

(4.1)

Although the actual running time of \( e \) is \( O(|x|) \) and hence is linear, \( e \) is untypable in polynomial AARA. The problem of (4.1) is that the stepping function doubles the input size. This makes AARA conclude that the worst-case total running time is \( O(2^{|z|}) \), and this cost bound is beyond the expressive power of AARA (exponential AARA [23], however, can handle exponential cost bounds).

To preclude the example (4.1), it is reasonable to require the running time of \( e_1 \) (i.e. a stepping function inside primitive recursion) to be constant in the size of \( z \) (i.e. the result of
a recursive call). More concretely, if $T(|y|, |ys|, |z|)$ is the running time of a stepping function, we demand $T(|y|, |ys|, |z|) \leq p(|y|, |ys|)$, where $p(|y|, |ys|)$ is a polynomial in $|y|$ and $|ys|$. We will adopt this idea in the formulation of inherently polynomial time.

Although this idea results in a fairly simple inductive definition of inherently polynomial time, a major drawback is that some realistic programs are not admitted by the current formulation of inherently polynomial time. For instance, consider multiply that, given input lists $\ell_1$ and $\ell_2$, produces a list of size $|\ell_1| \cdot |\ell_2|$:

$$multiply := \text{rec } \ell_1 \{ [], \ell_2, [], \} \text{ with } z \mapsto e_1,$$  \hspace{1cm} (4.2)

where the stepping function of primitive recursion is

$$e_1 \equiv \text{case } z \{(z_1, z_2) \mapsto \text{share } z_1 \text{ as } z_1, z_1, z_1 \text{ in } \langle z_1, 1, \text{append } \langle z_1, 1, z_2 \rangle \rangle \}.$$  

The first component of $z$ stores $\ell_2$, while the second component of $z$ acts as an accumulator. The running time of $e_1$ is polynomial in $|z_1|$ but constant in $|z_2|$. Therefore, $e_1$’s running time is only polynomial partially in $|z|$. This is why the overall time complexity of $e$ remains polynomial instead of becoming exponential. Nonetheless, (4.2) is not inherently polynomial time according to the current formulation, since the formulation does not allow $e_1$’s running time to have any dependence on $|z|$.

Furthermore, (4.2) can only be typed in multivariate AARA and not in univariate AARA. This means our formulation of inherently polynomial time fails to capture some of the realistic programs that are typable only in multivariate AARA. In view of this, one might wonder whether inherently polynomial time is completely encapsulated by univariate AARA; that is, every inherently polynomial-time RaML program is typable in univariate AARA. The answer is negative.

As a counterexample, consider the standard append defined as

$$append := \text{rec } \ell_1 \{ [], \ell_2 | (y :: ys) \text{ with } z \mapsto y :: z \}.$$  \hspace{1cm} (4.3)

Note that it is inherently polynomial time. append alone is typable in univariate AARA as well as multivariate AARA. However, if we require the output of append to carry quadratic potential (because it will be later fed to a function that demands quadratic potential from inputs; for example), then univariate AARA cannot type append—we need to resort to multivariate AARA to type it.

In summary, our formulation of inherently polynomial time goes beyond the remit of univariate AARA, but does not capture the full range of realistic programs that require multivariate potential.

### 4.2 Formulation of inherently polynomial time

#### Restricting the syntax of Resource-Aware ML

To ensure termination of programs, we require programs to use primitive recursion in place of general recursion. Hence, we will from now on work with a fragment of RaML wherein general recursion is replaced by primitive recursion. This fragment removes fun $f \ x = e$ from the original RaML (Section 2.1) and adds the following:

1. $\lambda(x : b). e$ for a lambda abstraction, where $b \in B$;
2. $\text{rec } x \{ [], e_0 | (y :: ys) \text{ with } z \mapsto e_1 \}$, where $z$ denotes the result of the recursive call.

In primitive recursion, $e_1$ is only allowed to mention $\{y, ys, z\}$. If $e_1$ needs access to a global variable $v$ (i.e. a variable from outside the primitive recursion), $v$ should be transferred to $e_1$ by placing $v$ inside $z$. 
The reason why we deny $e_1$ access to a global variable is that every variable symbol can only be accessed at most once in RaML. However, this is in fact already violated by $e_1$ having access to $ys$ (because this means some elements of the input $x$ are accessed multiple times during primitive recursion). Further, even if we let $e_1$ access global variables, AARA can be easily adapted. Also, it will result in a less strict formulation of inherently polynomial time that admits \textit{multiply} in (4.2). Nonetheless, for simplicity, this article assumes that $e_1$ can only mention $y$, $ys$, and $z$.

Primitive recursion can be encoded using general recursion as

$$
\text{fun } f \langle x, \Gamma \rangle = \text{case } x \{ [] \mapsto e_0 | y :: ys \mapsto \text{share } ys \text{ as } ys_1, ys_2 \text{ inlet } z = f \langle ys_1, \Gamma \rangle \text{ in } e_1 \}. 
$$

Here, $\Gamma$ is a set/sequence of those variables that do not appear in $e_1$, but $e_0$. Variable $ys_1$ is passed on to the recursive call, and $ys_2$ is used in $e_1$ (if $e_1$ mentions $ys$).

**Judgments**

The primary judgment of inherently polynomial time is

$$
\Delta; \Gamma \vdash e \text{ inhpoly}(V), \tag{4.4}
$$

where

- $\Gamma$ is a typing context containing both base-type and arrow-type variables such that $\Gamma \vdash e : b$ for base type $b$.
- $V \subseteq \text{dom}(\Gamma)$ is a set of variables.
- $\Delta$ is a set of $f \text{ time}$, where $f \in \text{dom}(\Gamma)$ is a arrow-type variable and $\text{time} \in \{ \text{const, poly} \}$.

Sometimes we split $\Gamma$ into $\Sigma$ for arrow-type variables and $\Gamma$ for base-type variables, writing the judgment as $\Delta; \Sigma; \Gamma \vdash e \text{ inhpoly}(V)$. (4.4) is only applicable to base-type expressions.

An informal interpretation of (4.4) is

- $f \text{ const}$ denotes that the running time of $f$ is constant with respect to the input size, and likewise, $f \text{ poly}$ denotes that $f$’s running time is \textit{strictly} polynomial in the input size (and hence is not constant in the input size).
- The running time of $e$ is (i) polynomial in the sizes of those variables in $V$ but (ii) constant in the sizes of $\text{dom}(\Gamma) \setminus V$.
- Every sub-expression of $e$ runs in polynomial time.

The judgments for an arrow-type expression $e$ are

$$
\Delta; \Gamma \vdash e \text{ const} \quad \Delta; \Gamma \vdash e \text{ poly}, \tag{4.5}
$$

$\Delta; \Gamma \vdash e \text{ const}$ means $e$ runs in constant time with respect to the input size, and $\Delta; \Gamma \vdash e \text{ poly}$ likewise means $e$’s running time is \textit{strictly} polynomial in the input size.

**Inference rules**

The most important inference rules defining (4.4) are displayed in Figure 1. Throughout these rules, $b$ denotes a base type, $\text{time}$ is drawn from $\{ \text{const, poly} \}$, and $V$ is a set of variables. The remaining rules are deferred to Appendix E.

In (IP:CASE-SUM), the notation $V[x \mapsto y]$ refers to the result of replacing $x$ in $V$ with $y$ (if $x \in V$); otherwise, $V$ remains intact. If the running time of case $x \{ \ell \cdot y \mapsto e_0 | r \cdot y \mapsto e_r \}$ in the rule’s conclusion is allowed to be polynomial in $|x|$ (i.e. $x \in V$), then $e_{i \in \{ \ell, r \}}$ in the two premises is allowed to run in polynomial time in $|y| = |x| - 1$. 

CVIT 2016
\[
\begin{align*}
\vdash & x : b \vdash \text{inhpoly}(\emptyset) & (\text{IP:BASE}) \\
\Delta = \{ f \text{ time} \} & \quad \vdash f : b_1 \to b_2 \vdash f \text{ time} & (\text{IP:ARROW}) \\
\vdash & \vdash \emptyset \vdash \text{inhpoly}(\emptyset) & (\text{IP:UNIT}) \\
\vdash & x : b \vdash \ell \cdot x \vdash \text{inhpoly}(\emptyset) & (\text{IP:SUML}) \\
\vdash & x : b \vdash r \cdot x \vdash \text{inhpoly}(\emptyset) & (\text{IP:SUMR}) \\
\vdash & x_1 : b_1 \vdash x_1 \vdash \text{inhpoly}(\emptyset) \\
\vdash & x_2 : b_2 \vdash x_2 \vdash \text{inhpoly}(\emptyset) & (\text{IP:PAIR}) \\
\vdash & x_1 : b_1, x_2 : b_2 \vdash (x_1, x_2) \vdash \text{inhpoly}(\emptyset) & (\text{IP:CONS}) \\
\vdash & x_1 : b \vdash x_1 \vdash \text{inhpoly}(\emptyset) \\
\vdash & x_2 : L(b) \vdash x_2 \vdash \text{inhpoly}(\emptyset) & (\text{IP:CONS}) \\
\Delta = \{ x_1 \text{ const} \} & \quad \vdash x_1 : b_1 \to b_2, x_2 : b_1 \vdash x_1 \cdot x_2 \vdash \text{inhpoly}(\emptyset) & (\text{IP:APP-CONST}) \\
\Delta = \{ x_1 \text{ poly} \} & \quad \vdash x_1 : b_1 \to b_2, x_2 : b_1 \vdash x_1 \cdot x_2 \vdash \text{inhpoly}(\emptyset) & (\text{IP:APP-POLY}) \\
\Delta; \Gamma, y : b_1 \vdash e_\ell \vdash \text{inhpoly}(V[x \to y]) & \quad \Delta; \Gamma, y : b_2 \vdash e_r \vdash \text{inhpoly}(V[x \to y]) & (\text{IP:CASE-SUM}) \\
\Delta; \Gamma, x : b_1 + b_2 \vdash \text{case } x \{ \ell \cdot y \mapsto e_\ell | r \cdot y \mapsto e_r \} \vdash \text{inhpoly}(V) & (\text{IP:CASE-PROD}) \\
\Delta; \Gamma, x : b_1 \times b_2 \vdash e \vdash \text{inhpoly}(V[x \to x_1, x_2]) & (\text{IP:CASE-LIST}) \\
\Delta; \Gamma, x : L(b) \vdash \text{case } x \{ (x_1, x_2) \mapsto e \} \vdash \text{inhpoly}(V) & (\text{IP:CASE-LIST}) \\
\Delta; \Gamma, y : b_1 \vdash e_0 \vdash \text{inhpoly}(V) & \quad \Delta; \Gamma, x : L(b) \vdash \text{rec } x \{ y \mapsto y \vdash \text{inhpoly}(V) \} & (\text{IP:REC}) \\
\Delta; \Gamma, x : L(b) \vdash \text{rec } x \{ y \mapsto y \vdash \text{inhpoly}(V) \} & (\text{IP:REC}) \\
\Delta; \Sigma_1 ; \Gamma, x : b \vdash e_1 \vdash \text{inhpoly}(V_1) & \quad \Delta; \Sigma_2 ; \Gamma, x : b \vdash e_2 \vdash \text{inhpoly}(V_2) & (\text{IP:LET-BASE}) \\
\Delta_1 \cup \Delta_2 ; \Sigma_1 \cup \Gamma_1 \cup \Gamma_2 \vdash \text{let } x = e_1 \in e_2 \vdash \text{inhpoly}(V_3) & (\text{IP:LET-BASE}) \\
\Delta; \Gamma, x_1 : b, x_2 : b \vdash e \vdash \text{inhpoly}(V[x \to x_1, x_2]) & (\text{IP:SHARE-BASE}) \\
\Delta; \Gamma, x : b \vdash \text{share } x \text{ as } x_1, x_2 \in e \vdash \text{inhpoly}(V) & (\text{IP:SHARE-BASE})
\end{align*}
\]

\(\textbf{Figure 1}\) Key inference rules of inherently polynomial time.
Similarly, in (IP:Case-Prod), \( V[x \mapsto x_1, x_2] \) means \((V \setminus \{x\}) \cup \{x_1, x_2\}\) if \(x \in V\); otherwise, \(V\) remains unchanged.

(IP:Rec) is the crux of the notion of inherently polynomial time. Observe that the stepping function \(e_1\) must be constant-time in \(|z|\).

In (IP:Let-Base), we use a finer-grained notation where the typing context of \(e_1\) is split into \(\Sigma_1\) for arrow-type variables and \(\Gamma_1\) for base-type variables. \(V_3\) is determined by

\[
V_3 := \begin{cases} 
\text{dom}(\Gamma_1) \cup (V_2 \setminus \{x\}) & \text{if } x \in V_2; \\
V_1 \cup V_2 & \text{otherwise}.
\end{cases}
\]

If \(x \in V_2\), it means that \(e_2\) runs in polynomial time in \(|x|\). In the worst case, only the running time of \(e_1\) but \(|e_1|\) (i.e. the output size of \(e_1\)) is polynomial in the sizes of those variables in \(V_1\). Hence, in the worst case, the overall running time of \(let \ x = e_1 \ in \ e_2\) is polynomial in \(\text{dom}(\Gamma_1)\), which contains all base-type variables appearing in \(e_1\), and \(V_2 \setminus \{x\}\).

Note that (IP:Let-Base) considers the worst case—if we had information about the output size, we might be able to derive a more precise judgment.

Finally, the judgment (4.5) is defined by the following inference rules:

\[
\Delta; x : b \vdash e \ \text{inhpoly}(\emptyset) \quad \text{(IP:Const)} \\
\Delta; \vdash \lambda (x : b). e \ \text{const} \quad \text{(IP:Rec)} \\
\Delta; x : b \vdash e \ \text{inhpoly}([x]) \quad \text{(IP:Poly)}
\]

In (IP:Const), because the conclusion indicates that the \(\lambda\)-abstraction’s running time is constant in the input size, the premise states that the running time of the body \(e\) can only be polynomial in \(\text{dom}(\Gamma)\), which excludes \(x\). By contrast, in the premise of (IP:Poly), the set of variables contains \(x\).

## 5 Typabe fragment of Resource-Aware ML

It is nontrivial to prove that inherently polynomial time (Section 4.2) implies typability in multivariate AARA. The chief challenge is to come up with a suitable statement of a typability theorem (i) that we can prove by induction and (ii) that satisfies the following two requirements. Firstly, because a term \(e\) may later be used as an input to a function, it must be possible to type \(e\) such that a user-specified amount of potential remains in \(e\)’s output.

Secondly, to type primitive recursion, we need to establish an invariant of resource annotations that is analogous to a loop invariant in Hoare logic. Specifically, given a primitive recursion \(\text{rec } x \ {[]} \mapsto e_0 | (y :: y) \) with \(z \mapsto e_1\), we must give an (almost) identical annotation to both \(z\), which is the result of a recursive call, and \(e_1\), which is a stepping function.

### Typability theorem

We have partially overcome this challenge, and this section presents the result that inherently polynomial time implies typability in multivariate AARA under some restrictions. Detailed proofs of Theorem 5 and Theorem 8 are available in Appendix E.

➤ **Definition 3** (Variables with zero potential). Let \(\Gamma \cup \{v : b\}\) be a base-type typing context and \(P\) be its multivariate annotation. Variable \(v\) is said to contain zero potential in \(P\) if and only if \(P(i, j) = 0\) for every \(i \in \mathcal{I}(\Gamma)\) and \(j \in \mathcal{I}([v : b])\) such that \(j \neq 0\).

➤ **Assumption 4.** Suppose we are given \(\Delta; \Sigma; \Gamma \vdash e\ t\) for \(t \in \{\text{inhpoly}(V), \text{const}, \text{poly}\}\). For every sub-derivation \(\Delta; \Sigma; \Gamma \vdash e_a\ \text{inhpoly}(V_a)\) inside the derivation of \(\Delta; \Sigma; \Gamma \vdash e\ t\), we assume the following:
The next theorem establishes that inherently polynomial time implies typability in multivariate AARA under Assumption 4, which restricts variable sharing and pattern matching on nested lists.

**Theorem 5 (Inherently polynomial time implies typability).** Suppose we are given a term \( \Sigma; \Gamma \vdash e : b \) with \( b \in \mathbb{B} \), where \( \Delta; \Sigma; \Gamma \vdash e \) inhpoly(V) holds for some \( V \subseteq \text{dom}(\Gamma) \). Additionally, assume Assumption 4. There exist \( P \) and \( Q \) satisfying \( \Sigma; \Gamma; P \vdash e : \langle b, Q \rangle \) such that each \( v \in \text{dom}(\Gamma) \setminus V \) contains zero potential (Definition 3).

Consider an arrow-type term \( \Sigma; \tilde{\Gamma} \vdash e : b \rightarrow b_{2} \) and assume Assumption 4. There exist \( P \) and \( Q \) such that \( \Sigma; \tilde{\Gamma}; 1 \vdash e : \langle b, P \rangle \rightarrow \langle b_{2}, Q \rangle \). Additionally, if \( \Delta; \cdot; \Gamma \vdash e \) \text{const} is true, \( P \) contains constant potential; i.e., \( b_{1} \) stores zero potential in \( P \).

Given a base-type expression \( e \), if \( \Delta; \Sigma; \Gamma \vdash e \) inhpoly(V) holds, the running time of \( e \) is constant in the size of any \( v \in \text{dom}(\Gamma) \setminus V \). In other words, such \( v \) does not contribute to the computational cost of \( e \). Therefore, it intuitively makes sense that such \( v \) contains zero potential in Theorem 5.

However, Theorem 5 cannot be immediately proved by induction on inhpoly(V), since the statement of the theorem is not strong enough for an inductive proof to go through. Specifically, a problem arises in the inductive case for (IP:Let-Base). In a let-binding let \( x = e_{1} \) in \( e_{2} \), \( e_{1} \) must carry sufficient potential to be transferred to \( e_{2} \). However, Theorem 5 does not allow us to specify how much potential will remain available in the output of \( e \).

Prior to remedying this issue, we first introduce the notion of uniform resource annotations for multivariate AARA.

**Definition 6 (Uniform resource annotations for base types in multivariate AARA).** Given a base type \( b \in \mathbb{B} \), let \( P \) be a multivariate resource annotation of \( b \). \( P \) is said to be a uniform multivariate annotation with degree \( d \in \mathbb{N} \) and number \( n \in \mathbb{N} \) if and only if the following conditions hold

1. The maximum degree of \( P \) is at most \( d \);
2. \( P(i) = n \) for every \( i \in \mathcal{I}(b) \) such that \( \text{deg}(i) = d \).

In words, all coefficients of base polynomials with degree \( d \) (which should be the maximum degree) are equal to \( n \). This will be denoted by a judgment \( P \text{ uniform}(d, n) \).

**Definition 7 (Uniform annotations for typing contexts in multivariate AARA).** Consider a term \( \Sigma; \Gamma \vdash e : b \) of base type. Suppose that \( \Delta; \Sigma; \Gamma \vdash e \) inhpoly(V) holds. Let \( P \) be a multivariate annotation for the base-type typing context \( \Sigma \). We say that \( P \) is uniform with respect to degree \( d \in \mathbb{N} \), number \( n \in \mathbb{N} \), and set \( V \) of variables if and only if the following conditions hold:

1. For any base-type variable \( v \in \text{dom}(\Gamma) \setminus V \) of type \( b_{v} \), we have
   \[
   \forall i \in \mathcal{I}(\{v : b_{v}\}), j \in \mathcal{I}(\Gamma \setminus \{v : b_{v}\}).\text{deg}(i) > d \Rightarrow P(i, j) = 0.
   \]
   In other words, for any base polynomial with a non-zero coefficient in \( P \), its projection on \( v \) must have degree at most \( d \).
2. For any \( v \in \text{dom}(\Gamma) \setminus V \) of base type \( b_{v} \), we have
   \[
   \forall i \in \mathcal{I}(\{v : b_{v}\}), j \in \mathcal{I}(\Gamma \setminus \{v : b_{v}\}).(\text{deg}(i) = d \wedge j \neq 0) \Rightarrow P(i, j) = 0.
   \]
In words, if a base polynomial has a non-zero coefficient and its projection on \( v \) has degree \( d \), then the base polynomial is not allowed to involve size variables of any other base-type variables from \( \text{dom}(\Gamma) \).

3. For any \( v \in \text{dom}(\Gamma) \setminus V \) of base type \( b_v \), we have
\[
\forall i \in I\{v : b_v\}. P(i, 0) = n.
\]
That is, every base polynomial whose projection on \( v \) has degree \( d \) has coefficient \( n \).

If these conditions hold, we denote \( P \) being a uniform annotation by a judgment \( P \text{ uniform}(d, n, V) \).

Note that Definition 7 is a generalization of Definition 6. \( P \text{ uniform}(d, n) \) in Definition 6 is equivalent to \( P \text{ uniform}(d, n, 0) \) in Definition 7.

Now that we have the notion of uniform annotations in place, we next present Theorem 8 that allows us to specify the amount of potential remaining in the output of a program. The major difficulty of the proof lies in establishing an invariant for primitive recursion as explained at the start of Section 5. We employ the notion of uniform annotations to characterize this invariant.

**Theorem 8 (Existence of a multivariate annotation with arbitrary potential in the output).**
Given a term \( \Sigma; \Gamma \vdash e : b \) with \( b \in \mathbb{B} \), suppose that \( \Delta; \Sigma; \Gamma \vdash e \text{ inhpoly}(V) \) holds, where \( V \subseteq \text{dom}(\Gamma) \). Also, assume Assumption 4. Fix a multivariate annotation \( Q \) for the base type \( b \) such that \( Q \text{ uniform}(d, n) \). Then there exists a multivariate annotation \( P \) such that \( \Sigma; \Gamma; P \vdash e : (b, Q) \) under the cost-free metric. Furthermore, \( P \text{ uniform}(d, n, V) \) holds.

Consider an arrow-type term \( \Sigma; \vdash e : b_1 \rightarrow b_2 \) and assume Assumption 4. Fix a multivariate annotation \( Q \) for base type \( b_2 \) such that \( Q \text{ uniform}(d, n) \). Then there exists \( P \) such that \( \Sigma; \vdash 0 \vdash e : (b_1, P) \rightarrow (b_2, Q) \) under the cost-free metric. Furthermore, if \( \Delta; \Sigma; \vdash e \text{ const} \) is true, \( P \text{ uniform}(d, n) \) holds.

Theorem 8 assumes Assumption 4 as the proof of the theorem poses technical challenges in variable sharing and pattern matching on nested lists. We will now look at these challenges more closely.

**Variable sharing**

Theorem 8 is false if we impose no restrictions on variable sharing. To illustrate this, consider \( e \) defined as
\[
e := \text{iter } x \{[] \leftrightarrow (\ell, \ell) \mid (y :: _) \leftrightarrow e_1\},
\]
where the stepping function is \( e_1 \equiv \text{case } z \{\langle z_1, z_2 \rangle \leftrightarrow \text{share } z_1 \text{ as } z_{1,1}, z_{1,2} \text{ in } \langle z_{1,1}, z_{1,2}\rangle\} \).

This stepping function satisfies \( e_1 \text{ inhpoly}(\{y, ys\}) \). Hence, (5.1) is indeed inherently polynomial time. However, we have \( \text{share} \) on \( v \), which Assumption 4 forbids. The typing context of \( e \) in (5.1) is \( \Gamma = \{x : L(1), \ell : L(1)\} \).

Let \( (\ell_1, \ell_2) \) be the output of (5.1). Suppose that both \( \ell_1 \) and \( \ell_2 \) are to be annotated with \( L^1(1) \). To type (5.1) under the cost-free metric such that \( \ell_1, \ell_2 : L^1(1) \), the typing context \( \Gamma \) of \( e \) needs to be annotated with \( 2|\ell| + |x| + |\ell| \), where \( |\cdot| \) denotes the size of an input list. Observe that we need to use multivariate AARA rather than univariate AARA to type (5.1).

In the notation of univariate AARA, the stepping function of (5.1) can be typed as
\[
y : 1, ys : L^0(1), z : L^2(1) \times L^0(1); 0 \vdash e_1 : (L^1(1) \times L^1(1), 0).
\]
Here, the maximum degree is \( d = 1 \). It is impossible for both \( z \) and \( e_1 \) to have the same coefficient for all base polynomials of degree \( d = 1 \). Therefore, Theorem 8 is false for (5.1).

To accommodate the multivariate annotation of (5.1), it is necessary to relax the notion of uniform resource annotations, but this will make the typability proof more challenging.
Nested lists in pattern matching

Theorem 8 is false for pattern matching on nested lists. For example, consider \( e \) defined as

\[
e := \text{case } x \{ [ ] \rightarrow \_ | (y :: ys) \rightarrow \langle y, ys \rangle \},
\]

where the first branch is unimportant in the present discussion. The typing context of \( e \) is \( \Gamma = \{ x : L(L(1)) \} \). Assume that we consider multivariate annotations of degree up to \( d = 2 \). Let \( P \) denote a multivariate annotation of \( \Gamma \). The multivariate annotation for context \( \{ y : L(1), ys : L(L(1)) \} \) as a result of pattern matching on \( x : L(L(1)) \) is given by the additive shift of \( P \), denoted by \( \ll(P) \). It is defined as

\[
\ll(P)(i,j) := \begin{cases} 
P(0_{L(1)} :: j) + P(j) & \text{if } i = 0_{L(1)}; \\
P(i :: j) & \text{otherwise,} 
\end{cases}
\]

where \( i \in I(\{ y : L(1) \}) \) and \( j \in I(\{ ys : L(L(1)) \}) \). The problem is that the base polynomial \( (i,j) \) on the left hand side of (5.2) has degree \( \deg(i) + \deg(j) \), while in the second branch of the right hand side has degree \( 1 + \deg(i) + \deg(j) \). As a consequence, if \( 1 + \deg(i) + \deg(j) = 2 \), \( P(i :: j) \) is required to be equal to \( n \) because Theorem 8 requires \( P \) uniform \((d, n)\) to be true. This means \( \ll(P)(i, j) = n \) must hold as well. But \( \ll(P)(i, j) = n \) is not necessarily the case, since Theorem 8 imposes no requirements on the coefficients of lower-degree base polynomials.

6 Conclusion

In this work, we have shown that polynomial-time Turing machines can be embedded in a typable fragment of Resource-Aware ML (RaML) in such a way that the semantics and worst-case cost bounds are preserved. Moreover, we have proved that if a first-order program \( P \) satisfies the following conditions, it is guaranteed to be typable in multivariate polynomial AARA:

1. \( P \) uses primitive recursion instead of general recursion;
2. \( P \) is (axiomatically) inherently polynomial-time;
3. No variable sharing is applied to \( v \), where \( P \)'s running time is (axiomatically) constant in \( v \);
4. No pattern matching is applied to a nested list.

We have neither found a counterexample to the full typability theorem (i.e. Theorem 5 without Assumption 4) nor proved it. As future work, we are looking to investigate how to prove or disprove the full typability theorem. To lift the restriction on nested lists, we expect that it suffices to modify the statement of the theorem such that we can keep track of the largest coefficient. However, lifting the restriction on variable sharing will be more challenging because it certainly requires a drastically different inductive hypothesis.

References


Supplementary results for the embedding of polynomial-time Turing machines in AARA

A.1 Standard-form polynomials in AARA

In conventional mathematics taught at school, (univariate) polynomials are expressed in the standard form of \( a_nx^n + \cdots + a_0x^0 \), where \( x \) is a variable and \( a_i \)'s are coefficients. On the other hand, in AARA, polynomials are encoded as linear combinations of binomial coefficients \( \binom{x}{d} \), where \( x \) is a variable and \( a \) is a constant. The following proposition establishes that these two representations of univariate polynomials are interchangeable.

Lemma 9. For any \( d \in \mathbb{N} \), the polynomial function \( n^d \) can be expressed as \( \sum_{i=0}^{d} q_i \binom{n}{i} \), where \( q_i \in \mathbb{Q}^{\geq 0} \) for all \( 0 \leq i \leq d \).

Proof. The proof goes by induction on \( d \). The claim clearly holds when \( d = 0 \).

For the inductive case, by way of example, we will first illustrate how to prove the lemma for \( d = 4 \), given that the claim holds when \( d = 3 \). For simplicity, we will use the basis of \( i! \cdot \binom{n}{i} \) rather than \( \binom{n}{i} \) in this example. Suppose we have

\[
n^3 = p_1n + p_2n(n-1) + p_3n(n-1)(n-2).
\]

This yields

\[
n^4 = n \cdot (p_1n + p_2n(n-1) + p_3n(n-1)(n-2))
= p_1n^2 + p_2n^2(n-1) + p_3n^2(n-1)(n-2)
= p_1n(n-1) + p_2n(n-1)((n-2) + p_3n(n-1)(n-2) + p_3n(n-1)(n-2) + p_3n(n-1)(n-2) + p_3n(n-1)(n-2),
\]

where all coefficients are non-negative, provided that each \( p_i \) is non-negative as well. Generalizing this, we learn that \( n^k = \sum_{i=0}^{k} p_i \cdot n(n-1) \cdots (n-i+1) \) gives

\[
n^{k+1} = p_k \cdot n(n-1) \cdots (n-k) + \sum_{i=1}^{k} (p_{i-1} + i \cdot p_i) \cdot n(n-1) \cdots (n-i+1).
\]

If the coefficients \( p_i \) for \( n^k \) are non-negative, so are the coefficients for \( n^{k+1} \).

Finally, to switch from the new basis to the original basis of binomial coefficients, we use the identity \( p_i = \frac{q_i}{i!} \). This gives

\[
n^{k+1} = \frac{q_k}{k!} \cdot n(n-1) \cdots (n-k) + \sum_{i=1}^{k} \left( \frac{q_{i-1}}{(i-1)!} + i \cdot \frac{q_i}{i!} \right) \cdot n(n-1) \cdots (n-i+1)
= q_k \cdot \binom{n}{k+1} + \sum_{i=1}^{k} i(q_{i-1} + q_i) \binom{n}{i}.
\]

This concludes the proof.

A.2 Generating lists of polynomial size

We will explain how to generate in Resource-Aware ML (RaML) a list of polynomial size \( p(n) \) with constant potential stored in each cell. To this end, it suffices to show how to generate a list of size \( \binom{n}{d} \) for a fixed \( d \in \mathbb{N} \) because \( n^k \) for any \( k \in \mathbb{N} \) can be expressed as a non-negative linear combination of \( \binom{n}{0}, \ldots, \binom{n}{d} \). This has formally been established by Proposition 9.
Without loss of generality, we assume that the output is a list of blank symbols (as required in line 3 of Algorithm 1). Let \( \text{amp}_d : L(\text{Sym}) \to L(\text{Sym}) \) denote a RaML function that (i) generates a list of size \( \binom{n}{d} \) in which each cell stores one unit of potential and (ii) appends it to an accumulator, which is assumed to already contain one unit of potential in each cell. Here, \( \text{amp} \) stands for amplification.

\( \text{amp}_0 \) is defined as

\[
\text{fun } \text{amp}_0 \ w \ \text{acc} = \sqcup :: \text{acc}.
\]  

(A.2)

For \( i \geq 0 \), \( \text{amp}_{i+1} \) is inductively defined as

\[
\text{fun } \text{amp}_{i+1} \ w \ \text{acc} = \text{case } w \{ \text{nil} \mapsto \text{acc} \\
\mid x :: xs \leftrightarrow \text{share } xs \text{ as } xs_1, xs_2 \text{ in} \\
\qquad \text{let } _\_ = \text{tick } 1 \text{ in} \\
\qquad \text{let acc'} = \text{amp}_i \ xs_1 \ \text{acc} \text{ in} \\
\qquad \text{amp}_{i+1} \ xs_2 \ \text{acc'} \}
\]  

(A.3)

We use \text{tick} to account for only the cost of function application but not costs of other operations such as the list constructor. This is why (A.2) does not generate any costs. Although the syntax of RaML presented in Section 2.1 only permits uncurried functions, I will use curried functions throughout Section A without loss of generality.

This implementation is analogous to the example given in Section 7.1 of [17], where given a list \( \ell \), all subsets of \( \ell \) with a fixed size are computed. However, our implementation in (A.3) differs from the implementation in [17] in that ours uses an accumulator, while the one in [17] explicitly uses the \text{append} function. The use of an accumulator allows us to embed both generation of elements and their concatenation in the implementation of \( \text{amp}_d \), saving us the need to explicitly reason about the computational cost of \text{append}. Hence, using an accumulator can simplify the cost analysis of \( \text{amp}_d \), although admittedly \( \text{amp}_d \) with an accumulator is not the most natural implementation from the perspective of programmers.

We consider the generation of lists of size \( \binom{n}{d} \) instead of \( n^d \) for a similar reason. Due to the identity \( \binom{n+1}{d+1} = \binom{n}{d+1} + \binom{n}{d} \), we do not need to appeal to any auxiliary function in (A.3). On the other hand, to recursively create a list of size \( n^d \), one needs to use an iterator function, and this will complicate the analysis of total costs since we will need to account for the cost of invoking the iterator function.

The next proposition establishes the correctness of the above implementation and provides an upper bound on the evaluation cost.

\[\text{Lemma 10 (Correctness of } \text{amp}_d). \text{ The function } \text{amp}_d \text{ defined in (A.2) and (A.3) produces a list of size } \binom{\vert w \vert}{d} + \vert \text{acc} \vert, \text{ where } \binom{n}{k} = 0 \text{ for } n < k. \text{ Also, assuming that each cell in the output list is required to contain one unit of potential, the cost of evaluating } \text{amp}_d \ w \ \text{acc} \text{ is bounded above by } 2\vert w \vert^d.\]

\[\text{Proof.} \text{ The proof goes by nested induction: outer induction on } d \text{ and inner induction on } \vert w \vert. \text{ For the base case where } d = 0, \text{ the output size is indeed } \binom{n}{0} = 1. \text{ With regard to the evaluation cost, we need one unit of potential to execute (A.2) since the new cell requires one unit of potential. As } 2n^0 = 2 \text{ for every } n \in \mathbb{N}, 2n^d \text{ is a correct upper bound in this case. Here, we adopt the convention of } 0^0 = 1. \text{ For the inductive case, suppose that the claim holds when } d = k \text{ for some } k \geq 0. \text{ The proof proceeds by (inner) induction on } \vert w \vert. \text{ When } \vert w \vert = 0, \text{ we have}
\]

\[|\text{amp}_{k+1} \ w \ \text{acc}| = 0 + |\text{acc}|\]
according to the first branch of pattern matching in (A.3). Also, the evaluation cost is 0. Hence, the claim holds when \( w \) is empty.

Conversely, if \( w = x :: xs \), we have
\[
|\text{amp}_{k+1} w \text{ acc}| = \left( \frac{|xs|}{k+1} \right) + \left( \frac{|xs|}{k} \right) + |\text{acc}|
\]
by the inductive hypothesis
\[
= \left( \frac{|w| - 1}{k+1} \right) + \left( \frac{|w| - 1}{k} \right) + |\text{acc}|
\]
because \( w = x :: xs \)
\[
= \left( \frac{|w|}{k+1} \right) + |\text{acc}|
\]

Regarding the evaluation cost, we write \( \text{cost}(\text{amp}_{k+1} w \text{ acc}) \) for the evaluation cost of \( \text{amp}_{k+1} w \text{ acc} \). If \( k \geq 1 \), we have
\[
\text{cost}(\text{amp}_{k+1} w \text{ acc}) = 1 + \text{cost}(\text{amp}_k w \text{ acc}) + \text{amp}_{k+1} w \text{ acc}'
\]
by (A.3)
\[
\leq 1 + 2|xs|^k + 2|xs|^{k+1}
\]
by the inductive hypothesis
\[
\leq 2(1 + |xs|^k) + 2|xs|^{k+1}
\]
because \( k \geq 1 \)
\[
\leq 2(1 + |xs|^k) + 2|xs| \cdot (1 + |xs|^k)
\]
\[
= 2(1 + |xs|^{k+1})
\]
\[
= 2(|w|)^{k+1}
\]

If \( k = 0 \), we have
\[
\text{cost}(\text{amp}_1 w \text{ acc}) = 1 + \text{cost}(\text{amp}_0 w \text{ acc}) + \text{amp}_k w \text{ acc}'
\]
by (A.3)
\[
\leq 1 + 1 + 2|xs|
\]
by the inductive hypothesis
\[
= 2(|w|),
\]
where in the second line, we use the tight bound \( \text{cost}(\text{amp}_0 w \text{ acc}) = 1 \). Therefore, the claim is true regardless of whether \( k = 0 \) or \( k \geq 1 \). This concludes the proof. ▷

\( 2n^d \) is a tight cost bound of \( \text{amp}_d \) when \( d = 1 \). However, \( 2n^d \) is not a tight bound anymore when \( d > 1 \), and the general tight bound is probably complicated to express.

The next proposition claims that AARA can infer that \( 2n^d \) is an upper bound on the evaluation cost.

**Lemma 11 (Typability of \( \text{amp}_d \)).** AARA can infer the resource-annotated type
\[
\text{amp}_d : L^{2^n} (\text{Sym}) \xrightarrow{0/0} L^1 (\text{Sym}) \xrightarrow{0/0} L^1 (\text{Sym}),
\]
(A.4)
where vector \( \vec{q}_d \in \mathbb{Q}_{\geq 0}^d \) represents the function \( n \mapsto n^d \). To be more precise, since vectors from \( \mathbb{Q}_{\geq 0}^d \) cannot express constants, when \( d = 0 \), the resource-annotated type should be written as
\[
\text{amp}_d : L^0 (\text{Sym}) \xrightarrow{2/0} L^1 (\text{Sym}) \xrightarrow{0/0} \langle L^1 (\text{Sym}), 0 \rangle.
\]
(A.5)

Keep in mind that the resource annotation that AARA returns in reality can be a more accurate bound than (A.4).

**Proof.** To prove the claim, it is sufficient to show that (A.4) is a valid resource annotation that satisfies all relevant typing rules of AARA. The proof goes by induction on \( d \). For the base case of \( d = 0 \), the claim holds since \( \text{amp}_d \) requires exactly 1 potential unit.
We now turn to the inductive case. We can assign resource-annotated types to some variables appearing in (A.3) as

\[ w : L(\langle \text{Sym}, 2\tilde{q}_d \rangle) \quad xs_1 : L(\langle \triangleright 2\tilde{q}_d \rangle - 2\tilde{q}_d) \quad xs_2 : L(\langle \text{Sym}, 2\tilde{q}_d \rangle). \]

We will now argue that this annotation correctly accounts for the evaluation cost in every recursive call.

Firstly, from (A.1), we can derive that the first component of vector \( \tilde{q}_d \) for any \( d \geq 1 \) is 1. This means that 2 units of potential is available in each recursive call. Hence, we use this constant potential to account for tick 1 in the definition of \( \text{amp}_d \).

After deducting 2 units from the potential stored in \( w \), we have \( \triangleright 2\tilde{q}_d \) units of potential remaining, and this represents \( 2n^d - 2 \). We need to split it between \( xs_1 \) and \( xs_2 \) in such a way that we can pay for the costs of \( \text{amp}_{d-1} \) \( xs_1 \) acc and \( \text{amp}_d \) \( xs_2 \) acc'. For the former, the inductive hypothesis suggests \( \text{amp}_{d-1} : L^{2\tilde{q}_{d-1}}(\text{Sym}) \xrightarrow{0/0} L^1(\text{Sym}) \xrightarrow{0/0} L^1(\text{Sym}) \), provided that \( d \geq 2 \). If \( d = 1 \), we need to conduct separate analysis since the type of \( \text{amp}_0 \) in (A.5) is distinct from the type for \( \text{amp}_d \) for \( d \geq 1 \). Nonetheless, we will assume \( d \geq 2 \) in the present proof as it is straightforward to adapt this proof to the case of \( d = 1 \). For the recursive call \( \text{amp}_d \) \( xs_2 \) acc', ideally, we would like to reuse the resource-annotated type of \( \text{amp}_d \); otherwise, resource-polymorphic recursion would arise, complicating the proof. As a consequence, our goal is to show

\[ 2\tilde{q}_{d-1} + 2\tilde{q}_d \leq \triangleright 2\tilde{q}_d, \]

where + and \( \leq \) are applied component-wise. This is equivalent to \( \tilde{q}_{d-1} + \tilde{q}_d \leq \triangleright \tilde{q}_d \) because \( \triangleright \) is linear and hence \( \triangleright 2\tilde{q}_d = 2 \triangleright \tilde{q}_d \).

If \( \tilde{q}_{d-1} = (q_1, q_2, \ldots, q_{d-1}) \), it follows from (A.1) that

\[ \tilde{q}_d = (q_1, 2(q_1 + q_2), 3(q_2 + q_3), \ldots, (d - 1)(q_{d-2} + q_{d-1}), (d - 1)q_d). \]

This yields

\[ \tilde{q}_{d-1} + \tilde{q}_d = (2q_1, 2q_1 + 3q_2, \ldots, (d - 1)q_{d-2} + dq_{d-1}, (d - 1)q_{d-1}), \]

which is smaller than \( \triangleright \tilde{q}_d \) component-wise. Therefore, \( \tilde{q}_{d-1} + \tilde{q}_d \leq \triangleright \tilde{q}_d \) indeed holds. \( \blacksquare \)

### A.3 Target RaML programs

The target program \( M' \) can be expressed as

```plaintext
fun M' w = share w as w1, w2, w3 as
    let \( \ell_1 \) = \([\_]\) in
    let \( \ell'_2 \) = \text{amp}_{d, \triangleright} \ w1 \ \text{nil} \ in
    let \( \ell_2 \) = \text{append} \ w2 \ \ell'_2 \ in
    let ps = \text{amp}_{d, (\langle \_ \rangle)} \ w3 \ \text{nil} \ in
    simulate q0 \ \ell_1 \ \ell_2 \ ps, \quad (A.6)
```

where \( \text{amp}_{d, \triangleright} \) creates a list of size \( \left\lceil \frac{\text{size}(w)}{d} \right\rceil \) filled with blank symbols, and \( \text{amp}_{d, (\langle \_ \rangle)} \) performs the same task, except that the output is filled with \( \langle \_ \rangle \) instead of \( \triangleright \). \([\_]\) denotes a singleton list containing \( \_ \). If \( p(n) \), which is the polynomial representing \( M' \)’s running time, cannot be expressed in the form of \( \binom{d}{n} \) for any \( d \in \mathbb{N} \), we express \( p(n) \) as a linear combination of binomial coefficients (due to Lemma 9) and hard-code this linear combination inside (A.6).
The auxiliary functions \textit{append} and \textit{simulate} are defined as

\begin{verbatim}
fun append ℓ₁ ℓ₂ = case ℓ₁ { nil → ℓ₂ |
        x :: xs ← let _ = tick 1 in
        let xs' = append xs ℓ₂ in
        x :: xs'}

fun simulate s ℓ₁ ℓ₂ ps = case ps { nil → shift ℓ₁ ℓ₂ |
        p :: ps' ← let _ = tick 1 in
        let (s', b, direction) = δ(s, head ℓ₂) in
        if s' = qfinal then
            shift ℓ₁ ℓ₂
        else if direction = L then
            simulate s' (tail ℓ₁) ((head ℓ₁) :: b :: (tail ℓ₂)) ps'
        else
            simulate s' (b :: ℓ₁) (tail ℓ₂) ps' }.
\end{verbatim}

The function \textit{shift} used in (A.7) reverses the first input list and appends it to the second input list:

\begin{verbatim}
fun shift ℓ₁ ℓ₂ = case ℓ₁ { nil → ℓ₂ |
        x :: xs ← let _ = tick 1 in
        let ys = x :: ℓ₂ in
        shift xs ys}.
\end{verbatim}

In (A.7), for the sake of brevity, we use the standard form of function application in place of let-normal form. Also, \((s', b, \text{direction}) = \delta(s, \text{head} \ ℓ₂)\) is a slight abuse of notation because this is ill-formed with respect to the syntax of RaML and also because we would need to introduce a new type for directions (i.e. \(L\) or \(R\)). Nevertheless, we write it this way to keep \(\delta\) general. If we are given a specific transition function, we can embed it in the code, dedicating one branch of if-else statements (or pattern matching) to each possible combination of \(s\) (i.e. the current machine state) and \(\text{head} \ ℓ₂\) (i.e. the symbol in the current cell).

Lastly, for completeness, \textit{head} and \textit{tail} are defined as

\begin{verbatim}
fun head ℓ = case ℓ { nil ← error | x :: xs ← x }
fun tail ℓ = case ℓ { nil ← error | x :: xs ← xs }.
\end{verbatim}

Finally, we are now in a position to prove the theorem about embedding polynomial-time Turing machines in RaML.

\begin{itemize}
    \item \textbf{Theorem 2 (Embedding of polynomial-time Turing machines in RaML).} Let \(M\) be a polynomial-time Turing machine that inputs and outputs bit strings from \(\{0, 1\}^*\). There exists a RaML program \(M' : \{0, 1\}^* \rightarrow \{0, 1\}^*\) such that
        \begin{itemize}
            \item For every input \(w \in \{0, 1\}^w\), we have \(M(w) = M'(w)\);
        \end{itemize}
\end{itemize}
The computational cost of $M'$ (according to the tick metric) is larger than or equal to the running time of $M$.

Univariate AARA can infer a polynomial upper bound of the computational cost of $M'$.

**Proof.** Without loss of generality, assume that the running time of $M$ is bounded by $n \mapsto \binom{n}{d}$ for some fixed $d \in \mathbb{N}$. In this case, a desirable $M'$ is defined in (A.6). If this assumption is false, we can use Lemma 9 to express a polynomial as a linear combination of binomial coefficients and hard-code it in (A.6). By construction, $M'(w) = M(w)$ for every $w \in \{0,1\}^*$.

Throughout the execution of $M'$, $\ell_1$, $\ell_2$, and $ps$ must contain one unit of potential in each cell. The potential in $\ell_1$ and $\ell_2$ will be used to account for shift $\ell_1 \ell_2$ right before $M'$ terminates. The potential stored in $ps$ is for the execution of simulate.

Hence, the input $w$ to $M'$ must contain sufficient potential to pay for the following costs:

- Creating singleton list $\ell_1$ that contains $\cdot$. Due to the invariant we impose $\ell_1$'s potential, it requires one unit of potential to create $\ell_1$ in the initial configuration.
- Creating list $\ell'_2$ of size $\binom{|w|}{d}$, which has one unit of potential in each cell.
- Creating list $ps$ of size $\binom{|w|}{d}$, which stores one unit of potential in each cell.
- Appending $w$ to $\ell'_2$ to create $\ell_2$, which has size $|w| + \binom{|w|}{d}$ and stores one unit of potential in each cell. Thus, we have $|w|$ many units of potential to execute append and another $|w|$ units to be stored in the first $|w|$ cells of $\ell_2$. This gives a total of $2|w|$ units of potential. By Proposition 11, each of the first two costs can be covered by $2|w|^2$ units of potential. Hence, summing the above three costs, we obtain $1 + 2|w|^2 + 2|w|^2 + 2|w|$. This is the amount of potential that must be stored in the input $w$ to $M'$ at the start of computation.

Each auxiliary function appearing in (A.6) can be type-annotated. More concretely, $amp_d$ can be type-annotated as shown in Proposition 11, and simulate can be assigned this type:

$$simulate : \text{State} \rightarrow L^1(\text{Sym}) \xrightarrow{0/0} L^1(\text{Sym}) \xrightarrow{0/0} L^1(\text{Sym}) \xrightarrow{0/0} L^0(\text{Sym}).$$

Since it is relatively easy to see that this type can be inferred using AARA, we will omit its formal proof. In summary, univariate AARA can infer a polynomial cost bound of $M'$. \(\blacksquare\)

### B Running time of Resource-Aware ML

A cost semantics of a programming language $L$ is a mapping $\cdot : [L] \rightarrow \mathbb{Q}_{\geq 0}$. Here, $[L]$ is the set of all programs in $L$ where inputs are already included in them; that is, programs in $[L]$ have base types as opposed to arrow types. In the literature of automatic amortized resource analysis (AARA), cost semantics are typically defined by specifying how each inference rule of the big-step operational semantics gives rise to computational costs. A mapping from inference rules of the operational semantics to $\mathbb{Q}$ (or vectors of $\mathbb{Q}$) is referred to as a cost metric. Examples of cost metrics include the running time and memory usage.

We now formalize the running time of Resource-Aware ML (RaML) with general recursion replaced by primitive recursion. This is because in Sections 4 and 5, where we discuss the main result of this article, we use primitive recursion instead of general recursion. The running time of general recursion should be fairly straightforward to deduce.

The running time is given by a judgment $V \vdash e \Downarrow v \mid n$, where $n \in \mathbb{N}$. This judgment is defined by the following inference rules.

$$\frac{V \vdash x \Downarrow v \mid 1}{V \vdash \text{Var} \mid x \Downarrow v \mid 1} \quad \frac{V \vdash \text{Unit} \mid 0}{V \vdash \text{Unit} \mid 0}$$

$$d \in \{\ell, r\} \quad V \vdash d \cdot x \Downarrow v \mid 2 \quad \frac{V \vdash d \cdot x \Downarrow v \mid 2}{V \vdash d \cdot x \Downarrow v \mid 2} \quad \text{(E:Sum)}$$
and AARA accordingly. However, it will not fundamentally affect the theorems and their proofs because it is only necessary for the tick metric.

In (E:UNIT) and (E:NIL), the running time is zero. One might argue that these cases could have positive running time in practice. If we are to assign positive running time to (E:UNIT) and (E:NIL), we will need to revise the type systems of univariate and multivariate AARA accordingly. However, it will not fundamentally affect the theorems and their proofs in this article. In (E:Rec), even if the stepping function \( e_1 \) has zero running time (e.g. due to (E:NIL)), the total running time of the whole primitive recursion is positive and is proportional to the length of an input list. Consequently, even if (E:UNIT) and (E:NIL) have zero running time as they do now, the running time of any primitive recursion is non-zero.

We do not have a rule for tick, because it is only necessary for the tick metric.
\section{Univariate polynomial \textsc{AARA}}

\subsection{Type system}

This section presents a type system for univariate polynomial \textsc{AARA} of \textsc{Resource-Aware ML} (RaML) with primitive recursion. Again, we focus on a variant of RaML with primitive recursion instead of general recursion because this is the variant used in Sections 4 and 5 where the main result of this article is discussed. The content and presentation style of this section are attributed to Hoffmann’s PhD thesis \cite{Hoffmann2004}.

The typing judgment for univariate polynomial \textsc{AARA} has the form $\Gamma_{\text{anno}}; q \vdash e : A$, where $q$ is a non-negative rational number and $\Gamma_{\text{anno}}$ is a resource-annotated typing context (i.e. a set of pairs of variable symbols and their resource-annotated types).

\paragraph*{Syntax-directed rules}

The syntax-directed rules for univariate polynomial \textsc{AARA} are presented below.

\begin{equation}
\begin{array}{c}
x : \tau ; 1 \vdash x : \langle \tau, 0 \rangle \quad (\text{U:VAR}) \\
; 0 \vdash \langle \rangle : \langle 1, 0 \rangle \quad (\text{U:UNIT}) \\
\Gamma ; 1 \vdash x : \langle b_1, 0 \rangle \quad (\text{U:SUML}) \\
\Gamma ; 2 \vdash \ell \cdot x : \langle b_1 + b_2, 0 \rangle \quad (\text{U:SUMR})
\end{array}
\end{equation}

\begin{equation}
\begin{array}{c}
x_1 : b_1, x_2 : b_2 ; 3 \vdash \langle x_1, x_2 \rangle : \langle b_1 \times b_2, 0 \rangle \quad (\text{U:PAIR}) \\
; 0 \vdash \langle \rangle : \langle 0 \rangle \quad (\text{U:NIL}) \\
x_1 : b, x_2 : L^{q/q}(q); 1 \vdash x_1 :: x_2 : \langle L^{q}(q), 0 \rangle \quad (\text{U:CONS})
\end{array}
\end{equation}

In (U:CONS), $q_1$ is not a fresh variable—it denotes the first component of vector $\vec{q}$.

\begin{equation}
\begin{array}{c}
B_1 = \langle b, q \rangle \\
\Gamma ; 1 \vdash \lambda x. e : \langle B_1 \rightarrow B_2, 0 \rangle \quad (\text{U:ABS}) \\
B_1 = \langle b, q \rangle \\
\Gamma ; 1 \vdash \lambda x. e : \langle B_1 \rightarrow B_2, 0 \rangle \quad (\text{U:ABS})
\end{array}
\end{equation}

\begin{equation}
\begin{array}{c}
x_1 : B_1 \rightarrow B_2, x_2 : b ; 1 \vdash e : B_2 \quad (\text{U:APP}) \\
\Gamma ; 1 \vdash \lambda x. e : \langle B_1 \rightarrow B_2, 0 \rangle \quad (\text{U:APP}) \\
x_1 : B_1 \rightarrow B_2, x_2 : b ; 1 \vdash e : B_2 \quad (\text{U:APP})
\end{array}
\end{equation}

\begin{equation}
\begin{array}{c}
x : b_1 + b_2, \Gamma ; 1 \vdash \text{case } x \{ \ell \cdot y \mapsto e_\ell | r \cdot y \mapsto e_r \} : B \quad (\text{U:CASE-SUM}) \\
\Gamma ; y : b_1 ; q \vdash e : B \\
\Gamma ; y : b_2 ; q \vdash e : B \\
x \vdash b_1 \times b_2, \Gamma ; 1 \vdash \text{case } x \{ \langle x_1, x_2 \rangle \mapsto e \} : B \quad (\text{U:CASE-PRODUCT})
\end{array}
\end{equation}

\begin{equation}
\begin{array}{c}
x : L^{q/q}(q); q \vdash \text{case } x \{ \langle \rangle \mapsto e_0 | x_1 :: x_2 \mapsto e_1 \} : B \quad (\text{U:CASE-LIST}) \\
\Gamma ; q \vdash e : B \\
\Gamma ; q \vdash e : B \\
\Gamma ; \tau \vdash \text{case } x \{ \tau ; p \mapsto e_1 | \tau ; q \mapsto e_2 \} : B \quad (\text{U:CASE-LIST})
\end{array}
\end{equation}

\begin{equation}
\begin{array}{c}
\Gamma ; q \vdash e : B \\
\Gamma \vdash \text{let } x = e_1 \text{ in } e_2 : B \quad (\text{U:LET}) \\
\tau \vdash \text{case } x \{ \tau ; p \mapsto e_1 | \tau ; q \mapsto e_2 \} : B \quad (\text{U:CASE-LIST}) \\
\Gamma ; x : \tau ; q \vdash \text{share } x \text{ as } x_1, x_2 \text{ in } e : \langle \tau, q \rangle \quad (\text{U:SHARE})
\end{array}
\end{equation}
In (U:SHARE), \( \tau \Rightarrow (\tau_1, \tau_2) \) means the resource-annotated type \( \tau \) can be split into \( \tau_1 \) and \( \tau_2 \). When we split a resource-annotated arrow type \( \tau \equiv B_1 \rightarrow B_2 \), variables \( x_1 \) and \( x_2 \) need not have the same annotation. They are allowed to have distinct annotations as long as these annotations can be legally derived using \( (U:Abs) \). Thus, it is possible to use a different resource annotation for a function \( f \) each time \( f \) is invoked.

In (U:CONS) and (U:CASE-LIST), we use the univariate additive shift operator (denoted by \( \ll \)) that splits the potential of a list between the head element and the tail. This is formally defined below.

**Definition 12 (Additive shift of potential vectors).** Given a potential vector \( \overrightarrow{q} = (q_1, q_2, \cdots, q_k) \), its additive shift is defined as

\[
\ll(\overrightarrow{q}) := (q_1 + q_2, q_2 + q_3, \cdots, q_{k-1} + q_k, q_k).
\]

**Primitive recursion**

The typing rule for \( \text{rec} \) is explained below.

\[
\begin{align*}
\frac{\Gamma; q \vdash e : \langle b_2, 0 \rangle \quad y : b_1, ys : L^{\ll(\overrightarrow{w})} - \overrightarrow{\tau}(b_1), z : b_2 + b_3; w_1 - 1 \vdash e_1 : \langle b_2, 0 \rangle}{x : L^{\overrightarrow{\tau}}(b_1), \Gamma; 1 + q \vdash \text{rec} x \{ \langle \rangle \leftarrow e_0 \mid (y :: ys) \text{ with } z \leftarrow e_1 \} : \langle b_2, 0 \rangle} & \quad \text{(U:REC)}
\end{align*}
\]

\( w_1 \) denotes the first component of \( w \). We additionally impose the following conditions:

- \( \overrightarrow{\tau} \) has a strictly lower degree than \( \overrightarrow{w} \).
- \( \overrightarrow{\tau} \) and \( b_3 \) satisfy

\[
\begin{align*}
x : L^{\overrightarrow{\tau}}(\langle b_1 \rangle), |\Gamma|; 0 \vdash \text{rec} x \{ \langle \rangle \leftarrow e_0 \mid (y :: ys) \text{ with } z \leftarrow e_1 \} : \langle b_3, 0 \rangle & \quad \text{(C.1)}
\end{align*}
\]

under the cost-free metric. Here, \( |b_1| \) and \( |\Gamma| \) are the annotation-free versions of \( b_1 \) and \( \Gamma \), respectively.

To justify (U:REC), firstly, consider the special case of \( \overrightarrow{\tau} = 0 \). Due to (C.1), it follows from \( \overrightarrow{\tau} = 0 \) that \( b_2 = |b_3| \); that is, \( b_3 \) carries zero potential. In this particular situation, (U:REC) becomes

\[
\frac{\Gamma; q \vdash e : \langle b_2, 0 \rangle \quad y : b_1, ys : L^{\ll(\overrightarrow{w})} - \overrightarrow{\tau}(b_1), z : b_2; w_1 - 1 \vdash e_1 : \langle b_2, 0 \rangle}{x : L^{\overrightarrow{\tau}}(b_1), \Gamma; 1 + q \vdash \text{rec} x \{ \langle \rangle \leftarrow e_0 \mid (y :: ys) \text{ with } z \leftarrow e_1 \} : \langle b_2, 0 \rangle}
\]

After pattern matching (i.e. splitting \( x \) into \( y \) and \( ys \)), the potential stored in \( ys \) in the second premise is \( \ll(\overrightarrow{w}) \). Out of this potential, \( \overrightarrow{w} \) is used in the recursive call to compute \( z \). This is why the resource-annotated type of \( z \) is \( b_2 \). The remaining potential, \( \ll(\overrightarrow{w}) - \overrightarrow{w} \), is for the current step of primitive recursion.

More generally, \( z \)'s annotation is allowed to be different from \( b_2 \). Let \( b_3 \) represent the difference between \( z \)'s and \( e_1 \)'s annotations. In order to account for \( b_3 \), we must establish another annotation \( x : L^{\overrightarrow{\tau}}(\langle b_1 \rangle), |\Gamma|; 0 \vdash e : \langle b_3, 0 \rangle \) under the cost-free metric, where \( e \) refers to the whole primitive recursion. This technique is known as resource-polymorphic recursion [17]. The type inference algorithm of AARA assumes that \( \overrightarrow{\tau} \) has a strictly lower degree than \( \overrightarrow{w} \) in order to guarantee termination. An example of resource-polymorphic recursion that is beyond the reach of the existing type inference algorithm is given in [14].
Structural rules

The structural rules are displayed below.

$\Gamma; q \vdash e : \tau \quad \tau' \quad (U:SUB)$

$\Gamma; x : \tau; g \vdash e : B \quad \tau' \quad (U:SUP)$

$\Gamma; q \vdash e : B \quad \Gamma_1 \subseteq \Gamma_2 \quad (U:WEAK)$

$\Gamma; p_1 \vdash e : \langle \tau, p_2 \rangle \quad q_1 \geq p_1 \quad q_1 - q_2 \geq p_1 - p_2 \quad (U:RELAX)$

C.2 Examples

`append` and `quicksort` introduced in Section 2.2 are implemented as follows:

`append`:

```
append : (L(1), L(1)) → L(1)
append := fun f ⟨ℓ₁, ℓ₂⟩ = case ℓ₁ {{}} ← ℓ₂ | (y :: ys) ← (f ⟨ys, ℓ₂⟩)
```

`quicksort`:

```
quicksort : L(b) → L(b)
quicksort := fun ℓ = case ℓ {[]} ← [[]] | (y :: ys) ← e₁
            e₁ ≡ let ⟨ℓ₁, ℓ₂⟩ = split ⟨y, ys⟩, x₁ = f ℓ₁, x₂ = f ℓ₂ in append ⟨x₁, y :: x₂⟩.
```

Here, `split ⟨y, ys⟩` classifies each element in the list `ys` according to whether it is smaller than `y` or not. `split` is defined as

```
split : (b × L(b)) → (L(b) × L(b))
split := fun f ⟨x, ℓ⟩ = case ℓ {[]} ← [[]] | (y :: ys) ← e₁
            e₁ ≡ let ⟨ℓ₁, ℓ₂⟩ = f ⟨x, ys⟩ in if y < x then ⟨y :: ℓ₁, ℓ₂⟩ else ⟨ℓ₁, y :: ℓ₂⟩.
```

D Multivariate polynomial AARA

This section describes multivariate polynomial AARA of Resource-Aware ML (RaML) with primitive recursion, which is a variant of RaML considered in Sections 4 and 5. As before, the content and presentation style of this section are attributed to Hoffmann’s PhD thesis [14].

D.1 Notation

We will introduce the projection and extension operators on multivariate annotations. To define projection, suppose we are given a base-type typing context $\Gamma_1 \cup \Gamma_2$. If $j \in I(\Gamma_2)$, the projection $\pi_j^{\Gamma_1}(Q)$ is defined as

$$\pi_j^{\Gamma_1}(Q)(i) := Q(i, j). \quad (D.1)$$

Next, to define the extension operator, let $Q$ be a multivariate annotation over $\Gamma_1$. Given $r \in I(\Gamma_2)$, the extension $\eta_r^{\Gamma_1 \cup \Gamma_2}(Q)$ is defined as

$$\eta_r^{\Gamma_1 \cup \Gamma_2}(Q)(i, j) := \begin{cases} Q(i) & \text{if } j = r; \\ 0 & \text{otherwise.} \end{cases} \quad (D.2)$$
Denoted by $\triangledown$, additive shift specifies how to split the potential of a list between the head element and the tail. We now explain additive shift of multivariate AARA. Suppose that we are given a base-type context $\Gamma_1 = \Gamma \cup \{\ell : L(b)\}$, where $\ell$ is the last element without loss of generality. Let $Q$ be a multivariate annotation over $\Gamma \cup \{\ell : L(b)\}$. $\ell : L(b)$ is split into the head element $x : b$ and the tail $xs : L(b)$, yielding a new typing context $\Gamma_2 = \Gamma \cup \{x : b, xs : L(b)\}$. The resource annotation for the new context is given by the (multivariate) additive shift of $Q$ with respect to $\ell : L(b)$. This is denoted by $\triangledown \ell Q$ and is defined as

$$\triangledown(Q)(i,j,k) := \begin{cases} Q(i,0_b :: k) + Q(i,k) & \text{if } j = 0_b; \\ Q(i,j :: k) & \text{otherwise.} \end{cases}$$

(D.3)

Here, $i$, $j$, and $k$ are indexes of $\Gamma$, $x : b$, and $xs : L(b)$, respectively. Recall that $j = 0_b$ refers to the base polynomial $\lambda v.1$ for type $b$. The notation $j :: k$ denotes the concatenation of $j$, which is an index for type $b$, to $k$, which is an index for type $L(b)$.

Lastly, for variable sharing, it is sufficient to know that for any multivariate resource annotation $Q$ for a base-type typing context $\Gamma \cup \{x_1 : b, x_2 : b\}$, we have a way to produce $P$ for the unified typing context $\Gamma \cup \{x : b\}$ such that no potential from $Q$ is lost. The relation between $Q$ and $P$ will be denoted by $P \triangledown x_1,x_2 Q$. The details of variable sharing are deferred to [14, 15].

### D.2 Type system

A typing judgment in multivariate AARA has the form

$$\Sigma_{anno}; \Gamma; Q \vdash e : \langle \tau, P \rangle.$$  

$\Sigma_{anno}$ is a resource-annotated arrow-type typing context, where each variable binding is of the form $f : (b_1, Q_1) \rightarrow (b_2, Q_2)$. $\Gamma$ is a base-type typing context without resource annotations, and $Q$ is a multivariate resource annotation/polynomial for $\Gamma$. Likewise, $P$ is a multivariate resource annotation for $\tau$. When $\tau$ is a resource-annotated arrow type, $P$ will just be a constant.

#### Syntax-directed rules

Syntax-directed rules are presented below.

$$Q(0_b) = 0$$  

(M:VAR-BASE)

$$\vdash x : b; 1 + Q \vdash x : (b, Q)$$  

(M:VAR-ARROW)

In (M:VAR-BASE), $c + Q$, where $c \in \mathbb{Q}_{\geq 0}$ and $Q$ is a multivariate resource annotation, denotes the addition of $x$ to $Q(0)$; i.e. the constant potential of $Q$. Those coefficients for all the other indexes, i.e. $i \neq 0 \in I(\Gamma)$, remain unchanged.

$$\vdash 0 \vdash \langle \rangle : \langle 1, 0 \rangle$$  

(M:UNIT)

$$Q(0_b) = 0$$  

(M:SUML)
Typable Fragments of Polynomial Automatic Amortized Resource Analysis

\[
Q(\theta_b) = 0 \\
\vdash x : \theta_2 ; 1 + \theta \vdash r \cdot x : (\theta_1 + \theta_2, \theta) \\
\quad (\text{M:SUMR})
\]

\[
Q(\theta_b) = 0 \\
\vdash x_1 : \theta_1, x_2 : \theta_2 ; 3 + \theta \vdash (x_1, x_2) : (\theta_1 \times \theta_2, \theta) \\
\quad (\text{M:PAIR})
\]

\[
Q(\theta_b) = 0 \\
\vdash \exists : \theta \vdash \langle L(\theta), \theta \rangle \\
\quad (\text{M:Nil})
\]

\[
Q = \xi_{x_1 \mapsto x_2} (\theta') \\
\vdash x_1, x_2 : L(\theta) ; 1 + \theta \vdash x_1 :: x_2 : (L(\theta), \theta) \\
\quad (\text{M:Cons})
\]

\[
B_1 = \langle \theta, \theta \rangle \\
\Sigma; \vdash 1 \vdash \lambda (x : \theta) : L(\theta) ; 1 : \theta \vdash B_2 _1 \rightarrow B_2 _1 \rightarrow B_2 _1 \\
\quad (\text{M:Abs})
\]

\[
\Sigma; x : \theta_1 + \theta_2, \Gamma; \vdash case \ x \ {\ell \cdot y \mapsto e_\ell} | r \cdot y \mapsto e_r : \theta, \theta_1 \cdot (\ell \cdot y \mapsto e_\ell) | r \cdot y \mapsto e_r : \theta \quad (\text{M:CASE-SUM})
\]

\[
\Sigma; \vdash x : \theta_1 + \theta_2, \Gamma; \vdash e_\ell : \theta, \theta_1 \quad (\text{M:CASE-PROD})
\]

\[
\Sigma; \vdash x : \theta_1 \times \theta_2, \Gamma; \vdash case \ (x_1, x_2) \mapsto e_1 : \theta, \theta_1 \\
\quad (\text{M:CASE-LIST})
\]

\[
\Sigma; \vdash x : \theta_1 + \theta_2, \Gamma; \vdash let \ x \ = \ e_1 \ in \ e_2 : \theta, \theta_1 \\
\quad (\text{M:LET})
\]

\[
\Sigma; \vdash x_1 : \theta_1, x_2 : \theta_2 ; \theta \vdash case \ f_1, f_2 \ in \ e : \theta, \theta_1 \\
\quad (\text{M:SHARE-BASE})
\]

\[
\Sigma; \vdash f : \theta_1 \rightarrow \theta_2, \Gamma; \vdash let \ f \ = \ f_1, f_2 \ in \ e : \theta, \theta_1 \\
\quad (\text{M:SHARE-ARROW})
\]

In (M:CASE-SUM), \(Q[\ell \cdot y / x] \vdash e_\ell / B, \theta, \theta_1\) denotes the result of discarding the resource annotations within \(Q\) for \(x = r \cdot y\), which has a wrong tag.

\[
\Sigma; \vdash x : \theta_1 + \theta_2, \Gamma; \vdash case \ x \ \{ \ell \cdot y \mapsto e_\ell | r \cdot y \mapsto e_r \} : \theta, \theta_1 \\
\quad (\text{M:CASE-PROD})
\]

\[
\Sigma; \vdash x : \theta_1 \times \theta_2, \Gamma; \vdash case \ (x_1, x_2) \mapsto e_1 : \theta, \theta_1 \\
\quad (\text{M:CASE-LIST})
\]

\[
\Sigma; \vdash x : \theta_1 + \theta_2, \Gamma; \vdash let \ x \ = \ e_1 \ in \ e_2 : \theta, \theta_1 \\
\quad (\text{M:LET})
\]

According to the first premise of (M:LET), \(e_1\) must carry \(\pi_{\theta_1}(R)\) much potential after computation. This potential is part of \(R\) that only concerns size variables inside \(x : \theta_1\).

However, being multivariate in nature, \(R\) may involve a product of both size variables outside \(x\) and those inside \(x\). How can we squeeze such multivariate potential into \(Q\) such that it becomes available in \(R\)? To achieve this, we additionally impose this requirement: for each \(j \in I(\Gamma_2)\) such that \(j \neq \Gamma_2\), we have

\[
\Sigma; \vdash x_1 : \theta_1, x_2 : \theta_2; \theta \vdash e_1 : (\theta_1, \pi_{\theta_1}(R)) \\
\quad (\text{M:LET})
\]

under the cost-free metric. We could not place this requirement inside the rule (M:LET) simply due to the shortage of space.
**Primitive recursion**

We now systematically derive the typing rule for rec. The general form of primitive recursion in RaML is

\[ \Sigma; x : L(b_1), \Gamma \vdash \text{rec } x \{ [] \mapsto e_0 \mid (y :: ys) \mapsto e_1 \}: b_2. \]  

(D.4)

Without loss of generality, in this section, we assume \( \Sigma = \emptyset \); we will set aside arrow-type variables and will instead focus on base-type variables. To clarify what \( z \) really is in (D.4), we can rewrite the primitive recursion in the form of general recursion as

\[ f := \lambda (x, \Gamma). \begin{cases} e_0 \mid (y :: ys) \rightarrow \text{share } ys \text{ as } ys_1, ys_2 \text{ in } \\
\text{let } z = f \ ys_1 \Gamma \text{ in } e_1. \end{cases} \]  

(D.5)

(D.5) uses a similar syntax to that of Resource-Aware ML (RaML) in Section 3.1. \( f \) refers to the entire recursion and is treated as a function whose input is \( \{ x \} \cup \text{dom}(\Gamma) \). In the second branch of (D.5), \( z \) is bound to \( f \ ys \Gamma \); i.e. \( f \) applied to \( y \) and \( \Gamma \). Variable \( y \) will split into \( y_1 \) and \( y_2 \). \( y \) is passed on to the recursive call, and \( y \) is used in the current step of primitive recursion (if \( e_1 \) mentions \( y \)).

As (D.5) uses \text{share} and \text{let}, we can obtain a typing rule for primitive recursion by combining (M:Share) and (M:Let). However, the resulting rule will be excessively complicated. Hence, we will not attempt to derive a typing rule for primitive recursion. The absence of a typing rule for rec will not negatively affect our study of a typable fragment of Resource-Aware ML (RaML), because we can always rewrite a primitive recursion as general recursion as in (D.5).

**Structural rules**

Structural rules are presented below.

\[ \frac{\Sigma; \Gamma; Q \vdash e : \langle \tau, P_1 \rangle}{\Sigma; \Gamma; Q \vdash e : \langle \tau, P_2 \rangle} \text{(M:Sub)} \quad \frac{\Sigma; \Gamma; Q \vdash e : B}{\Sigma; \Gamma; Q_2 \vdash e : Q_1} \text{(M:Sup)} \]

The subtyping relationship is determined by the point-wise inequality of coefficients of resource polynomials: \( Q < : P \) if and only if \( \forall i \in I(\Gamma) \cdot Q(i) \geq P(i) \).

\[ \frac{\Sigma_1 \subseteq \Sigma_2 \quad \Sigma_1; \pi_1^\rho(Q) \vdash e : B}{\Sigma_2; \Gamma; Q \vdash e : B} \text{(M:Weak)} \quad \frac{\Sigma; \Gamma; P \vdash e : \langle \tau, P' \rangle \quad Q = P + c \quad Q' = P' + c}{\Sigma; \Gamma; Q \vdash e : \langle \tau, Q' \rangle} \text{(M:Relax)} \]

**E Proof of the typability theorem**

This section provides detailed proofs of Theorem 5 and Theorem 8. The proof of Theorem 5 makes use of Theorem 8, while the proof of Theorem 8 is self-contained; that is, its statement is strong enough for an inductive proof to go through.

First of all, for completeness, we present three inference rules for inherently polynomial time that are missing from Figure 1.

\[ \frac{\Delta_1; \vdash e_1 \text{ time}}{\Delta_1 \cup \Delta_2; \Gamma \vdash \text{let } x = e_1 \text{ in } e_2 \text{ inhpoly}(V)} \text{(IP:Let-Arrow)} \]
\[ \Delta[\text{x time } \mapsto x_1 \text{ time}, x_2 \text{ time}]; \Gamma, x_1 : b_1 \to b_2, x_2 : b_1 \to b_2 \vdash e \text{ inhpoly}(V) \]
\[ \Delta; \Gamma, x : b_1 \to b_2 \vdash \text{share x as } x_1, x_2 \text{ in e inhpoly}(V) \] (IP:SHARE-ARROW)

\[ \Delta_1; \Gamma_1 \vdash e \text{ inhpoly}(V_1) \]
\[ \Delta_1 \subseteq \Delta_2 \]
\[ \Gamma_1 \subseteq \Gamma_2 \]
\[ V_1 \subseteq V_2 \] (IP:WEAKEN-BASE)

In (IP:WEAKEN-BASE), we require \( V_2 \) to be a subset of base-type variables in \( \text{dom}(\Gamma) \).

**Theorem 5** (Inherently polynomial time implies typability). Suppose we are given a term \( \Sigma; \Gamma \vdash e : b \) with \( b \in B \), where \( \Delta; \Sigma; \Gamma \vdash e \text{ inhpoly}(V) \) holds for some \( V \subseteq \text{dom}(\Gamma) \). Additionally, assume Assumption 4. There exist \( P \) and \( Q \) satisfying \( \Sigma; \Gamma; P \vdash \cdot : \langle b, Q \rangle \) such that each \( v \in \text{dom}(\Gamma) \backslash V \) contains zero potential (Definition 3).

Consider an arrow-type term \( \Sigma; \cdot \vdash e : b_1 \to b_2 \) and assume Assumption 4. There exist \( P \) and \( Q \) such that \( \Sigma; \cdot \vdash e : \langle b_1, P \rangle 
\to \langle b_2, Q \rangle \). Additionally, if \( \Delta; ; \Gamma \vdash e \text{ const} \) is true, \( P \) contains constant potential; i.e. \( b_1 \) stores zero potential in \( P \).

**Proof.** The proof proceeds by structural induction on \( \Delta; \Sigma; \Gamma \vdash e \text{ inhpoly}(V) \).

For base cases, we have (IP:BASE), (IP:ARROW), (IP:UNIT), and (IP:NIL). In all of them, since the running time is constant, we only need constant potential. Thus, the theorem is indeed true.

Moving on to inductive cases, let us consider (IP:SUM-L):

\[ \cdot; x : b \vdash x \text{ inhpoly}(\emptyset) \]
\[ \cdot; x : b \vdash \ell \cdot x \text{ inhpoly}(\emptyset) \] (IP:SUML)

Again, \( \ell \cdot x \) runs in constant time. Therefore, it is easy to see that the theorem holds. The same reasoning applies to (IP:SUM-R), (IP:PAIR), and (IP:CONS).

(IP:CONST) and (IP:POLY) are straightforward.

Next, we consider (IP:APP-CONST):

\[ \Delta = \{ x_1 \text{ const} \} \]
\[ \Delta; x_1 : b_1 \to b_2, x_2 : b_1 \vdash x_2 \text{ inhpoly}(\emptyset) \] (IP:APP-CONST)

From the inductive hypothesis, it is given that \( x_1 : b_1 \to b_2 \) can be typed as \( \langle b_1, P \rangle \to \langle b_2, Q \rangle \), where \( P \) contains constant potential. Therefore, \( x_1 x_2 \) can be annotated in such a way that the annotation for \( x_2 \) contains zero potential; that is, only constant potential is needed. Thus, the theorem holds. The inductive case for (IP:APP-POLY) can be proved in the same manner.

The next case we consider is (IP:CASE-SUM):

\[ \Delta; \Gamma, y : b_1 \vdash e_{\ell} \text{ inhpoly}(V[x \mapsto y]) \]
\[ \Delta; \Gamma, y : b_2 \vdash e_r \text{ inhpoly}(V[x \mapsto y]) \]
\[ \Delta; \Gamma, x : b_1 + b_2 \vdash \text{case } x \{ \ell : y \mapsto e_{\ell} \mid r : y \mapsto e_r \} \text{ inhpoly}(V) \] (IP:CASE-SUM)

Applying the inductive hypothesis to the two premises, we obtain that both \( e_{\ell} \) and \( e_r \) are typable in multivariate AARA. Let \( P_1 \) and \( P_2 \) be the multivariate annotations for the two premises. We can derive a multivariate annotation for the conclusion by taking \( \max\{P_1(i), P_2(i)\} \) for each index/base polynomial \( i \in I(\Gamma \cup \{y : b_1, b_2\}) \). Furthermore, it follows from the inductive hypothesis that any variable \( v \in \text{dom}(\Gamma) \cup \{y\} \backslash V[x \mapsto y] \) has zero potential in both \( P_1 \) and \( P_2 \). Consequently, \( \max\{P_1(i), P_2(i)\} = \max\{0, 0\} = 0 \) if index \( i \) involves a size variable from \( v \). This establishes the theorem. (IP:CASE-PROD) can be proved in the same fashion.

We next consider (IP:CASE-LIST):
\[ \Delta; \Gamma \vdash e_0 \text{inpoly}(V \setminus \{x\}) \quad \Delta; \Gamma, x_1 : b, x_2 : L(b) \vdash e_1 \text{inpoly}(V[x \mapsto x_1, x_2]) \]

\[ \Delta; \Gamma, x : L(b) \vdash \text{case } x \{ [ ] \mapsto e_0 \mid (x_1 : x_2) \mapsto e_1 \} \text{ inpoly}(V) \] (IP:CASE-LIST)

Assume that the inductive hypothesis gives us annotations \( P_0 \) and \( P_1 \) for the two premises of (IP:CASE-LIST). From \( P_1 \), we can construct an annotation \( P_2 \) over the typing context \( \Gamma \cup \{ x : L(b) \} \) such that \( P_1 = \llhd(P_2) \). It follows from the definition of \( \llhd \) that

\[ \llhd(P_2)(i, j, k) := \begin{cases} 
P_2(i, 0_b :: k) + P_2(i, k) & \text{if } j = 0_b; \\
P_2(i, j :: k) & \text{otherwise.}
\end{cases} \quad (E.1) \]

We will define \( P_2 \) as follows. For any variable \( v \in (\text{dom}(\Gamma) \cup \{x\}) \setminus V \), the coefficient of a base polynomial in \( P_2 \) that involves \( v \)'s size variables is set to 0. All the other coefficients are set to the largest coefficient that appears in \( P_1 \). Consequently, by construction, every \( v \in (\text{dom}(\Gamma) \cup \{x\}) \setminus V \) contains zero potential in \( P_2 \). Let \( M \) denote the largest coefficient in \( P_1 \).

It remains to ascertain that \( \llhd(P_2) \) is a subtype of \( P_1 \). We will first consider the first clause of (E.1). Suppose that \( P_1(i, j, k) > 0 \) for some \( i, j, k \). This implies that \( (i, j, k) \) does not involve any variables from \( (\text{dom}(\Gamma) \cup \{x_1, x_2\}) \setminus V[x \mapsto x_1, x_2] \); otherwise, \( P_1(i, j, k) = 0 \) due to the inductive hypothesis of the second premise. If \( j = 0_b \), then \( P_2(i, k) = M \) holds because

\[ (i, 0_b, k) \text{ contains size variables of some } v \in (\text{dom}(\Gamma) \cup \{x_1, x_2\}) \setminus V[x \mapsto x_1, x_2] \]

\[ \iff (i, k) \text{ contains size variables of some } v \in (\text{dom}(\Gamma) \cup \{x\}) \setminus V. \]

Thus, \( \llhd(P_2)(i, j, k) \geq P_1(i, j, k) \) in this case. Conversely, if \( j \neq 0_b \), \( P_2(i, j :: k) \) is guaranteed to be \( M \). Hence, \( \llhd(P_2)(i, j, k) \geq P_1(i, j, k) \) is true in this case as well. Therefore, \( \llhd(P_2) \) is indeed a subtype of \( P_1 \). Finally, we can easily combine \( P_2 \) with \( P_0 \) to yield a desirable annotation for the conclusion of (IP:CASE-LIST).

Next is (IP:REC):

\[ \Delta; \Gamma \vdash e_0 \text{inpoly}(V) \quad ; y : b, y s : L(b), z : b_2 \vdash e_1 \text{inpoly}([y, y s]) \]

\[ \Delta; \Gamma, x : L(b) \vdash \text{rec } x \{ [ ] \mapsto e_0 \mid (y :: y s) \text{ with } z \mapsto e_1 \} \text{ inpoly}(V \cup \{x\}) \] (IP:REC)

Appealing to the inductive hypothesis, we know that \( e_0 \) and \( e_1 \) can be annotated as

\[ \Gamma; P_0 \vdash e_0 : \langle b_2, Q_0 \rangle \quad y : b, y s : L(b), z : b_2; P_1 \vdash e_1 : \langle b_2, Q_1 \rangle, \]

where \( P_1 \) assigns zero potential to \( z \) because of \( e_1 \text{inpoly}([y, y s]) \). From \( P_0 \) and \( P_1 \), it is possible to construct a multivariate annotation for the conclusion of (IP:REC). Furthermore, any variable in \( \text{dom}(\Gamma) \setminus V \) stores zero potential. The details of this construction are presented in Lemma 13.

The next case we consider is (IP:LET-BASE):

\[ \Delta_1; \Sigma_1; \Gamma_1 \vdash e_1 \text{inpoly}(V_1) \quad \Delta_2; \Gamma_2, x : b_1 \vdash e_2 \text{inpoly}(V_2) \]

\[ \Delta_1 \cup \Delta_2; \Sigma_1 \cup \Gamma_1 \cup \Gamma_2 \vdash \text{let } x = e_1 \text{ in } e_2 \text{inpoly}(V_3) \] (IP:LET-BASE)

The inductive hypothesis tells us that there exists a multivariate annotation

\[ \Gamma_2, x : b; P_2 \vdash e_2 : \langle b_2, Q_2 \rangle. \]

Let \( P \) be a multivariate annotation of the entire let-binding that we aim to derive. According to (IP:LET-BASE), \( P \) must satisfy the following two conditions:

1. \( \Sigma_1; \Gamma_1; \pi_0^\Gamma(P) \vdash e_1 : \langle b_1, \pi_0^x b_1(P_2) \rangle \) holds under the cost metric of the running time;
2. For all \( i \neq b \in \mathcal{I}(\Gamma_2) \), we have \( \Sigma_1; \Gamma_1; \pi_{1}^{\Gamma_1}(P) \vdash e_1 : \langle b_1, \pi_{1}^{x,b_1}(P_2) \rangle \) under the cost-free metric.

We will now conduct case analysis on whether \( x \in V_2 \). Assume \( x \notin V_2 \). It follows from the inductive hypothesis that \( x \) contains zero potential in \( P_2 \). As a result, \( \pi_{0}^{x,b_1}(P_2) \) in the first condition above is essentially constant potential. Applying the inductive hypothesis to \( e_1 \), we obtain a multivariate annotation of \( e_1 \) under the cost metric of the running time. If the output of \( e_1 \) in this annotation contains less potential than \( \pi_{0}^{x,b_1}(P_2) \), we can always inject constant potential into the annotation of \( e_1 \). The resulting annotation will serve as a suitable \( \pi_{0}^{\Gamma_1}(P) \). Likewise, \( \pi_{1}^{x,b_1}(P_2) \) in the second condition above, where \( i \neq b, \) is constant potential. Therefore, a suitable \( \pi_{1}^{\Gamma_1}(P) \) can be constructed (note that the second condition concerns the cost-free metric).

Lastly, we need to ensure that any \( v \in \text{dom}(\Gamma_1) \cup \text{dom}(\Gamma_2) \setminus V_3 \) has zero potential in \( P \). If \( v \in \text{dom}(\Gamma_2) \setminus V_2 \), since \( \pi_{1}^{\Gamma_1}(P) \) will be constant potential, it is impossible for any base polynomial with a size variable of \( v \) to have a non-zero coefficient. The same reasoning applies to the case of \( v \in \text{dom}(\Gamma_1) \setminus V_1 \).

Conversely, if \( x \in V_2 \), \( e_2 \) demands potential from \( x = e_1 \), meaning that we need a multivariate annotation for \( e_1 \) with some potential available in the output of \( e_1 \). Although the theorem gives us some multivariate annotation of \( e_1 \), we have no guarantee that the output of \( e_1 \) contains a desired arbitrary amount of potential. This is where Theorem 8 comes in. By Theorem 8, we can derive a cost-free annotation of \( e_1 \) such that its output stores a desirable amount of potential. Finally, summing this cost-free annotation with the annotation given by Theorem 5, we obtain a suitable \( \pi_{1}^{\Gamma_1}(P) \) in the first condition above. Regarding \( \pi_{1}^{\Gamma_1}(P) \) for \( i \neq b \) in the second condition, again, we resort to Theorem 8.

Lastly, we need to ensure that any \( v \in \text{dom}(\Gamma_1) \cup \text{dom}(\Gamma_2) \setminus V_3 \) contains zero potential in \( P \). As we assume \( x \in V_2 \), we have \( V_3 = \text{dom}(\Gamma_1) \cup (V_2 \setminus \{x\}) \). Therefore, it is guaranteed that \( v \in \text{dom}(\Gamma_2) \setminus V_2 \). Due to the inductive hypothesis of the theorem on \( e_2 \), \( v \) contains zero potential in \( P_2 \). Thus, for any \( i \in \mathcal{I}(\Gamma) \) that involves a size variable of \( v \), \( \pi_{1}^{x,b_1}(P_2) \) is essentially constant potential. Therefore, \( \pi_{1}^{\Gamma_1}(P) \) will be constant potential as well. Consequently, \( v \) will contain zero potential in \( P \), which is the annotation of the whole let-binding.

The final inductive case we consider is (IP:Share-Base):

\[
\Delta; \Gamma, x_1 : b, x_2 : b \vdash e \text{ in } \text{inhpoly}(V[x \mapsto x_1, x_2])
\]

By the inductive hypothesis, the premise of (IP:Share-Base) can be assigned a multivariate annotation. Using this, we can build a multivariate annotation for the conclusion by merging the coefficients for those base polynomials that mention either \( x_1 \) or \( x_2 \). Moreover, if \( x \notin V \), then \( x_1, x_2 \notin V[x \mapsto x_1, x_2] \). According to the inductive hypothesis, both \( x_1 \) and \( x_2 \) store zero potential. As a result, in the multivariate annotation of the rule’s conclusion, \( x \) stores zero potential as well. This establishes the theorem.

The inductive cases for (IP:Let-Arrow) and (IP:Share-Arrow) are straightforward to prove since they do not affect base-type variables; hence, we will not formally present their proof. Likewise, it is immediate to prove (IP:Weaken-Base). This concludes the proof. ▲

**Theorem 8 (Existence of a multivariate annotation with arbitrary potential in the output).**

Given a term \( \Sigma; \Gamma \vdash e : b \) with \( b \in \mathbb{B} \), suppose that \( \Delta; \Sigma; \Gamma \vdash e \text{ in } \text{inhpoly}(V) \) holds, where \( V \subseteq \text{dom}(\Gamma) \). Also, assume Assumption 4. Fix a multivariate annotation \( Q \) for the base type \( b \) such that \( Q \) uniform\((d,n)\). Then there exists a multivariate annotation \( P \) such that \( \Sigma; \Gamma; P \vdash e : \langle b, Q \rangle \) under the cost-free metric. Furthermore, \( P \) uniform\((d,n,V)\) holds.
Consider an arrow-type term \( \Sigma; \vdash e : b_1 \rightarrow b_2 \) and assume Assumption 4. Fix a multivariate annotation \( Q \) for base type \( b_2 \) such that \( Q \) uniform\((d,n)\). Then there exists \( P \) such that \( \Sigma; \vdash (b_1, P) \rightarrow (b_2, Q) \) under the cost-free metric. Furthermore, if \( \Delta; \Sigma; \vdash e \text{ const} \) is true, \( P \) uniform\((d,n)\) holds.

**Proof.** Like in the above proof of Theorem 5, this proof will proceed by induction on \( \Delta; \Gamma \vdash e \text{ in} \text{poly}(V) \). Although this document does not present inference rules for the cost-free annotations in multivariate AARA, the absence of their formal presentation should not affect the typability proof.

As before, nothing interesting happens in the base cases: (IP:Base), (IP:Arrow), (IP:Unit), and (IP:Nil). Likewise, it is straightforward to prove the inductive cases of (IP:SumL), (IP:SumR), and (IP:Pair).

By contrast, (IP:Cons) is nontrivial:

\[
\frac{\vdash x_1 : b \vdash x_1 \text{ in} \text{poly}(\emptyset) \quad \vdash x_2 : L(b) \vdash x_2 \text{ in} \text{poly}(\emptyset)}{\vdash x_1 : b, x_2 : L(b) \vdash x_1 \cdot x_2 \text{ in} \text{poly}(\emptyset)} \quad \text{(IP:Cons)}
\]

Suppose that we would like \( x_1 \cdot x_2 \) to be annotated with \( Q \). If \( Q \) is univariate, it is clear that there exists \( P \) such that

\[
x_1 : b, x_2 : L(b) ; P \vdash x_1 \cdot x_2 : (L(b), Q)
\]

and more importantly, \( P \) and \( Q \) only differ in lower-degree terms. This is because \( \vec{q} \) and \( \langle \vec{q} \rangle \) have the same coefficient of the maximum degree for any potential vector \( \vec{q} \). If \( Q \) is multivariate, the proof is more complicated and is deferred to Lemma 14.

As before, it is straightforward to prove (IP:Const) and (IP:Poly).

We next consider (IP:App-Const):

\[
\Delta = \{ x_1 \text{ const} \} \\
\frac{\Delta; x_1 : b \rightarrow b_2, x_2 : b_1 \vdash x_1 \cdot x_2 \text{ in} \text{poly}(\emptyset)}{\Delta; \Gamma \vdash e \text{ in} \text{poly}(V[\ell \mapsto y])} \quad \text{(IP:App-Const)}
\]

From the inductive hypothesis of \( x_1 \text{ const} \), we know that the annotation of \( x_1 \text{'s} \) input is identical to that of \( x_1 \text{'s} \) output when restricting our attention to base polynomials of degree \( d \). Therefore, the claim holds. (IP:App-Poly) can be proved straightforwardly.

Next is (IP:Case-Sum):

\[
\frac{\Delta; \Gamma, y : b_1 \vdash e_1 \text{ in} \text{poly}(V[\{x \mapsto y\}]) \quad \Delta; \Gamma, y : b_2 \vdash e_2 \text{ in} \text{poly}(V[\{x \mapsto y\}])}{\Delta; \Gamma, x : b_1 + b_2 \vdash \text{case } x \{ \ell : y \mapsto e_\ell | r : y \mapsto e_r \} \text{ in} \text{poly}(V)} \quad \text{(IP:Case-Sum)}
\]

From the inductive hypothesis, we have \( P_1 \) and \( P_2 \) satisfying

\[
\Gamma, y : b_1 ; P_1 \vdash e_\ell : (b, Q) \quad \Gamma, y : b_2 ; P_2 \vdash e_r : (b, Q)
\]

To construct a desirable multivariate annotation for the conclusion, we simply need to integrate \( P_1 \) and \( P_2 \) by taking the maximum coefficient for each base polynomial. (IP:Case-Prod) can be proved similarly.

Next, we consider (IP:Case-List):

\[
\frac{\Delta; \Gamma \vdash e_0 \text{ in} \text{poly}(V \setminus \{x\}) \quad \Delta; \Gamma, x_1 : b, x_2 : L(b) \vdash e_1 \text{ in} \text{poly}(V[\{x \mapsto x_1, x_2\}])}{\Delta; \Gamma, x : L(b) \vdash \text{case } x \{ \} \mapsto e_0 | (x_1 \cdot x_2) \mapsto e_1 \text{ in} \text{poly}(V)} \quad \text{(IP:Case-List)}
\]
Lemma 15 provides details of how to construct an annotation for case \( x \{ [ ] \mapsto e_0 \mid (x_1 :: x_2) \mapsto e_1 \} \).

The next inductive case is (IP:Rec):

\[
\frac{\Delta; \Gamma \vdash e_0 \text{ inhpoly}(V) \quad \vdots; y : b, \text{ys} : L(b), z : b_2 \vdash e_1 \text{ inhpoly}\{y, \text{ys}\}}{\Delta; \Gamma, x : L(b) \vdash \text{rec} x \{ [ ] \mapsto e_0 \mid (y :: \text{ys}) \text{ with } z \mapsto e_1 \} \text{ inhpoly}(V \cup \{x\})} \quad \text{(IP:Rec)}
\]

Suppose that the inductive hypothesis of the second premise yields

\[
y : b, \text{ys} : L(b), z : b_2; P_1 \vdash e_1 : \{b_2, Q\},
\]

where \( Q \) uniform\((d, n)\) and \( P_1 \) uniform\((d, n, \{y, \text{ys}\})\). It follows that \( \pi_i^{\#_2}(P) - Q \), which will be paid by resource-polymorphic recursion, has a strictly lower degree than \( d \). Therefore, resource-polymorphic recursion will derive a multivariate annotation for \( z \) such that it has the annotation \( \pi_i^{\#_2}(P) - Q \). To formally prove this, we should have performed strong induction on \( d \) as well as structural induction on \( \Delta; \Sigma; \Gamma \vdash e \text{ inhpoly}(V) \). However, since it might make the proof overly complicated and thereby confuse the readers, we decided to hide this detail until now. Note that if \( d = 0 \), the theorem clearly holds. If we only demand \( \Sigma; \Gamma \vdash e : b \) to have constant potential in the output, it is immediate to type \( e \)'s context under the cost-free metric.

Assume that resource-polymorphic recursion yields \( P_{2,i} \) for \( i \in \mathcal{I}\{y : b, \text{ys} : L(b)\}\) defined by

\[
\Gamma, x : L(b); P_{2,0} \vdash e : \langle b_2, \pi_0^{\#_2}(P) - Q \rangle \quad \text{if } i = 0;
\Gamma, x : L(b); P_{2,i} \vdash e : \langle b_2, \pi_i^{\#_2}(P) \rangle \quad \text{otherwise},
\]

where \( e \) refers to the entire primitive recursion. Note that all of \( \pi_i^{\#_2}(P) - Q \) and \( \pi_i^{\#_2}(P) \) for any \( i \neq 0 \) have degrees lower than \( d \); hence, the existence of their annotation can be proved by strong induction on \( d \). Our goal is to build an annotation \( P \) for \( e \) from \( P_1 \) and \( P_{2,i} \). The details of \( P \)'s construction are provided in Lemma 16.

Next is (IP:Let-Base):

\[
\frac{\Delta_1; \Sigma_1; \Gamma_1 \vdash e_1 \text{ inhpoly}(V_1) \quad \Delta_2; \Gamma_2, x : b_1 \vdash e_2 \text{ inhpoly}(V_2)}{\Delta_1 \cup \Delta_2; \Sigma_1 \cup \Gamma_1 \cup \Gamma_2 \vdash \text{let } x = e_1 \text{ in } e_2 \text{ inhpoly}(V_3)} \quad \text{(IP:Let-Base)}
\]

Suppose that the inductive hypothesis of the second premise yields

\[
\Gamma_2, x : b_1; P_2 \vdash e_2 : \langle b_2, Q\rangle,
\]

where \( Q \) uniform\((d, n)\). As we currently work with the cost-free metric, the premises of (M:Let) can be simplified to

\[
\forall i \in \mathcal{I}(\Gamma_2) \Sigma_1; \Gamma_1; \pi_i^{\Gamma_i}(P) \vdash e_1 : \langle b_1, \pi_i^{\#_1}(P_2) \rangle \quad \text{(E.2)}
\]

under the cost-free metric. Here, \( P \) is a multivariate annotation of the whole let-binding—it is what we aim to derive in this proof.

We now conduct case analysis. If \( x \in V_2 \), it is fairly easy to establish the claim. First of all, we fix \( i \in \mathcal{I}(\Gamma_2) \). From \( \pi_i^{\#_1}(P_2) \), the inductive hypothesis allows us to create a suitable \( \pi_i^{\Gamma_i}(P) \) that satisfies (E.2). If \( \pi_i^{\#_1}(P_2) \) is not uniform at the maximum degree (this is required by the theorem), we can easily create a uniform annotation that is a subtype of \( \pi_i^{\#_1}(P_2) \). It remains to ensure \( P \) uniform\((d, n, V_3)\). The proof of this case is identical to the proof of the next case; hence, we omit it.
Next, assume \(x \notin V_2\). As above, we can create a multivariate annotation for the whole let-binding. It remains to ensure that \(P\) is a uniform annotation. Let \(v\) be a variable drawn from \(\text{dom}(\Gamma_1 \cup \Gamma_2) \setminus V_3\), where \(V_4 = V_1 \cup V_2\) due to the assumption \(x \notin V_2\). If \(v \in \text{dom}(\Gamma_2) \setminus V_2\), the inductive hypothesis of \(e_2\) already implies \(P_2\) \(\text{uniform}(d, n, V_2)\). It is easy to see that the first condition of Definition 7 holds for \(P\) with respect to variable \(v\).

To establish the third condition (and also the second condition) of Definition 7, consider

\[
i = (h, g) \in \mathcal{I}(\Gamma_2 \setminus \{v : b\}) \times \mathcal{I}(\{v : b\}),
\]

where \(h = 0_{\Gamma_2 \setminus \{v : b\}}\) and \(\text{deg}(g) = d\). Due to the inductive hypothesis \(\pi_i^{\text{inhpoly}}(P_2, d, n, V_2)\), \(\pi_i^{\text{inhpoly}}(P_2)\) must essentially be constant potential of \(n\). Hence, \(\pi_i^{\text{inhpoly}}(P)\) in (E.2) is constant potential of \(n\) as well. Therefore, \(P(0_{\Gamma_1}, i) = n\) holds, thereby establishing the third condition of \(P\) \(\text{uniform}(d, n, V)\). The second condition of \(P\) \(\text{uniform}(d, n, V)\) can be established by the same reasoning. This proof is also applicable to the previous case, where \(x \in V_2\) and \(v \in \text{dom}(\Gamma_2) \setminus V_2\).

Lastly, let us consider the final case of the case analysis: \(x \notin V_2\) and \(v \in \text{dom}(\Gamma_1) \setminus V_1\). Due to the inductive hypothesis \(P_2\) \(\text{uniform}(d, n, V_2)\), \(\pi_i^{\text{inhpoly}}(P_2)\) has degree at most \(d\). Therefore, it follows from the inductive hypothesis of \(e_1\) that, for any base polynomial \(r\) in \(\pi_i^{\text{inhpoly}}(P)\) with a non-zero coefficient, \(r\)'s projection on \(v\) must have degree at most \(d\). This establishes the first condition of \(P\) \(\text{uniform}(d, n, V)\) with respect to \(v\).

Furthermore, if \(i \neq 0_{\Gamma_2}\), then \(\pi_i^{\text{inhpoly}}(P_2)\) has degree at most \(d - 1\). This means that \(\pi_i^{\text{inhpoly}}(P)\) cannot have a base polynomial whose projection on \(v\) has degree \(d\). It can only be degree \(d - 1\) at largest. Consequently, we have established the second condition of \(P\) \(\text{uniform}(d, n, V)\) with respect to \(v\).

Finally, consider \(i = 0_{\Gamma_2}\). \(\pi_0^{\text{inhpoly}}(P_2)\) satisfies \(\text{uniform}(d, n)\). Therefore, by the inductive hypothesis of \(e_1\), we have \(\pi_0^{\text{inhpoly}}(P)\) uniform\((d, n, V_1)\). This establishes the third condition of Definition 7.

Finally, we will discuss (IP::SHARE-BASE):

\[
\begin{align*}
\Delta; \Gamma, x_1 : b, x_2 : b & \vdash e \text{ inhpoly}(V[x \mapsto x_1, x_2]) \\
\Delta; \Gamma, x : b & \vdash \text{share } x \text{ as } x_1, x_2 \text{ in } e \text{ inhpoly}(V)
\end{align*}
\]

(IP::SHARE-BASE)

Assume the inductive hypothesis of the premise yields

\[
\Gamma, x_1 : b, x_2 : b; P \vdash e : (b_2, Q),
\]

where \(Q\) is specified by a user and satisfies \(Q\) \(\text{uniform}(d, n)\). From \(P\), we can easily obtain a multivariate annotation \(P'\) for the context \(\Gamma \cup \{x : b\}\). If \(x \in V\), the theorem is true for \(P'\). Conversely, if \(x \notin V\), we need to establish \(\pi_0^{\text{inhpoly}}(P')\) \(\text{uniform}(d, n)\). Although the inductive hypothesis gives us \(\pi_0^{\text{inhpoly}}(P)\) \(\text{uniform}(d, n)\), it is not always the case that \(\pi_0^{\text{inhpoly}}(P')\) \(\text{uniform}(d, n)\) holds. To circumvent this problem, we impose the restriction that no variable sharing is permitted on those variables that are outside \(V\) (or their constituent variables derived by pattern matching).

The remaining cases (i.e. (IP::LET-ARROW), (IP::SHARE-ARROW), and (IP::WEAKEN-BASE)) are immediate to prove. This concludes the proof.

\begin{lemma}[Construction of a multivariate annotation for primitive recursion] Consider a primitive recursion \(e\) of the form

\[
\Sigma; \Gamma \vdash \text{rec } x \{[] \leftarrow e_0 \mid (y :: ys) \text{ with } z \leftarrow e_1\} : b_2.
\]

\end{lemma}
Suppose we have $P_i, Q_i$ for $i \in \{0,1\}$ such that
\[
\Gamma; P_0 \vdash e_0 : \langle b_2, Q_0 \rangle \quad y : b, y : L(b), z : b_2; P_1 \vdash e_1 : \langle b_2, Q_1 \rangle
\]
under the cost metric of the running time. Here, $z$ contains zero potential in $P_1$. Then there exists a multivariate annotation $R$ such that $\Sigma; \Gamma, x : L(b); R \vdash e : \langle b_2, Q_1 \rangle$ holds under the cost metric of the running time.

Furthermore, assume $\Delta; \Sigma; \Gamma \vdash e_0 \in hpolym(V)$. For any $v \in \text{dom}(\Gamma) \setminus V$, if $v$ contains zero potential in $P_0$, then $z$ contains zero potential in $R$ as well.

Proof. Using general recursion, the primitive recursion $e$ can be written as
\[
f := \lambda x. \Gamma. \text{case } x \{ [] \mapsto e_0 | (y :: ys) \mapsto \text{share} \ ys \ as \ ys_1, ys_2 \ in \ let \ z = f \ ys_1 \ \Gamma \ in \ e_1 \}.
\]
Here, $ys_1$ is used in the recursive call, and $ys_2$ is (possibly) used inside $e_1$. It is safe to assume that the potential for $x : L(b)$ and that for $\Gamma$ in $R$ are completely separated (this assumption will yield a desired annotation $R$). In the second branch of $e$, $x = (y :: ys)$ is annotated with $\pi_0^{x:L(b)}(R)$, and $\Gamma$ is annotated with $\pi_0^\Gamma$. For $\pi_0^{x:L(b)}(R)$, it becomes $\psi(\pi_0^{x:L(b)}(R))$ as a result of pattern matching on $x$. Because $ys_2$ is used in the recursive call, it ought to be supplied with the same potential as $x : L(b)$; i.e., $\pi_0^{x:L(b)}(R)$. The remaining potential for $y$ and $ys_2$, which is given by $\psi(\pi_0^{x:L(b)}(R)) - \eta_0^{y:b,ys:L(b)}(\pi_0^{x:L(b)}(R))$, should be equal to $Q_1$.

Therefore, our goal is to find a suitable $\pi_0^{x:L(b)}(R)$ for $Q_1$. After this step, $\pi_0^{x:L(b)}(R)$ is combined with $P_0$, yielding a desirable $R$. Fortunately, as $Q_1$ does not need potential from $z$, we need not be concerned about it.

Let $A$ be a multivariate annotation for $x : L(b)$. $A$ represents $\pi_0^{x:L(b)}(R)$, and we will now work out what $A$ should be. $\psi(A)$, which is over the typing context $\{ y : b, ys : L(b) \}$, is given as
\[
\psi(A)(i, j) := \begin{cases} A(0_b :: j) + A(j) & \text{if } i = 0_b; \\ A(i :: j) & \text{otherwise.} \end{cases}
\]
If $i = 0_b$, we have
\[
\psi(A)(0_b, j) = A(0_b :: j) + A(j) - A(j) = A(0_b :: j),
\]
and this should be equal to $\pi_0^{y:b,ys:L(b)}(Q_1)(0_b, j)$. If $i \neq 0_b$, we should have $\psi(A)(i, j) = A(i :: j) = \pi_0^{y:b,ys:L(b)}(Q_1)(i, j)$. In summary, we have
\[
A(i :: j) := \pi_0^{y:b,ys:L(b)}(Q_1)(i, j) \tag{E.3}
\]
regardless of whether $i = 0_b$ or not. It is clear that, given $Q_1$, such $A$ exists. As a sanity check for (E.3), we can check whether it is correct when $Q_1$ is univariate (and hence $A$ is univariate). However, we will omit the details of the sanity check.

Finally, if $v \in \text{dom}(\Gamma) \setminus V$ contains zero potential in $P_0$, $z$ also has zero potential in $R$ that is constructed as above. This is essentially because $\pi_0^{x:L(b)}(R)$ and $P_0$ are completely separated in $P$. This concludes the proof.

Lemma 14 (Preservation of uniformity by list constructors). Consider a typing judgment $x_1 : b, x_2 : L(b) \vdash x_1 :: x_2 : L(b)$. Fix a multivariate annotation $Q$ of degree $d$ for $x_1 :: x_2$ such that $Q \text{ uniform}(d,n)$. There exists a cost-free multivariate annotation $P$ such that
\begin{itemize}
\item $x_1 : b, x_2 : L(b); P \vdash x_1 :: x_2 : \langle L(b), Q \rangle$;
\item $P$ uniform$(d, n, \emptyset)$.
\end{itemize}

Proof. $P$ is given by $\llangle Q \rrangle$, which is defined as

$$P(i, j) := \begin{cases} Q(0_b :: j) + Q(j) & \text{if } i = 0_b; \\ Q(i :: j) & \text{otherwise.} \end{cases} \quad \text{(E.4)}$$

Here, $i \in \mathcal{I}(\{x_1 : b\})$ and $j \in \mathcal{I}(\{x_2 : L(b)\})$.

We will now prove $P$ uniform$(d, n, \emptyset)$. Firstly, due to the definition of $P$ in (E.4), if the maximum degree of $Q$ is $d$, so is the maximum degree of $P$. That is, $P(i, j) > 0$ implies $\deg(i) + \deg(j) \leq d$. Hence, the first and second conditions for $P$ uniform$(d, n, \emptyset)$ (Definition 7) are met.

Secondly, in $P$, any base polynomial (i) that has degree $d$ and (ii) that only involves size variables of either $x_1$ or $x_2$ (but not both) must have coefficient $n$. To see this, let us first consider $x_2$. Fix an arbitrary $j \in \mathcal{I}(\{x_2 : L(b)\})$ such that $\deg(j) = d$. We get

$$P(0_b, j) = Q(0_b :: j) + Q(j)
= 0 + Q(j)
= Q(j).$$

In the second line, $0_b :: j$ would have degree $d + 1$, which exceeds the highest degree of $Q$. Hence, we must have $Q(0 :: j) = 0$. As a result, we obtain $P(0_b :: j) = Q(j)$, where both terms have the same degree, namely $d$.

Next, let us consider $x_1$. Fix an arbitrary $i \in \mathcal{I}(\{x_1 : b\})$ such that $\deg(i) = d$. This gives

$$P(i, 0_{L(b)}) = Q(i :: 0_{L(b)})
= 0,$$

where the last line follows from the fact that $\deg(i :: 0_{L(b)})$ exceeds $d$ and hence $Q(i :: 0_{L(b)}) = 0$ must hold. Thus, $(M; \text{Sup})$ allows us to increase $P(i, 0_{L(b)})$ such that the claim holds. Finally, the case where $i = 0_b$ is equivalent to the case where $d = 0$, and it is immediate to prove this case. This concludes the proof. \hfill \blacksquare

\begin{lemma}[Preservation of uniformity by list destructors] Consider $e \equiv \text{case } x \{ [] \leftarrow e_0 \mid (x_1 :: x_2) \leftarrow e_1 \}$, where $\Delta; \Sigma; \Gamma, x : L(b) \vdash e \text{ inhpoly}(V)$. Assume that the typing judgments of $e_0$ and $e_1$ are

$$\Gamma \vdash e_0 : b_2 \quad \Gamma, x : b, x_2 : L(b) \vdash e_1 : b_2,$$

where $b$ does not contain list types inside; that is, $L(b)$ is a non-nested list type. Additionally, suppose we are given $P_0$ and $P_1$ such that

$$\Gamma; P_0 \vdash e_0 : \langle b_2, Q \rangle \quad \Gamma, x_1 : b, x_2 : L(b); P_1 \vdash e_1 : \langle b_2, Q \rangle,$$

where $Q$ uniform$(d, n)$, $P_0$ uniform$(d, n, V \setminus \{x\})$, and $P_1$ uniform$(d, n, V[x \mapsto x_1, x_2])$. Then there exists a multivariate annotation $P$ for the entire $e$ such that (i) the output is annotated with $Q$ and (ii) $P$ uniform$(d, n, V)$ holds.

Proof. From $P_1$, we will construct an annotation $P_2$ over the typing context $\Gamma \cup \{x : L(b)\}$. $P_2$ should satisfy $\llangle P_2 \rrangle = P_1$ and $P_2$ uniform$(d, n, V)$. $\llangle P_2 \rrangle$ is defined as

$$\llangle P_2 \rrangle(i, j, k) := \begin{cases} P_2(i, 0_b :: k) + P_2(i, k) & \text{if } j = 0_b; \\ P_2(i, j :: k) & \text{otherwise.} \end{cases}$$

CVIT 2016
Because $L(b)$ is a non-nested list type by assumption, $j$ is always $0$. If we set

$$P_2(i, k) := P_1(i, 0, k), \quad \text{(E.5)}$$

we obtain

$$< (P_2)(i, 0, k) = P_2(i, 0, k) + P_2(i, k) \quad \text{by definition}$$

$$= P_1(i, 0, 0, k) + P_1(i, 0, k) \quad \text{by (E.5)}$$

$$\geq P_1(i, 0, k).$$

Therefore, $< (P_2)$ is a subtype of $P_1$; hence, $< (P_2)$ can be converted to $P_1$ by $(\text{M:SUB})$.

It remains to check that $P_2$ uniform$(d, n, V)$ holds. Let $v$ be a variable from $\text{dom} (\Gamma) \cup \{x\} \setminus V$. We now conduct case analysis on $v$. Suppose $v \not\equiv x$; that is, $x \in \text{dom} (\Gamma)$. This gives

$$P_2(i, k) > 0 \implies P_1(i, 0, k) > 0$$

$$\implies \deg(i) < d \lor (\deg(i) = d \land \deg(k) = 0)$$

by (E.5) and the assumption uniform $(d, n, V[x \mapsto x_1, x_2])$. Hence, the third condition of Definition 7 is true.

Conversely, suppose $v \equiv x$. Consider $k \in \mathcal{I}(\{x : L(b)\})$. This yields

$$P_2(i, k) > 0 \implies P_1(i, 0, k) > 0$$

$$\implies \deg(k) < d \lor (\deg(k) = d \land \deg(i) = 0)$$

by (E.5) and the uniform assumption.

This satisfies the first and second conditions of Definition 7. Furthermore, for any $k \in \mathcal{I}(\{x : L(b)\})$, if $\deg(k) = d$, we have $P_2(0, 0, k) = n$. This is because $P_1(0, 0, k) = n$ holds due to the inductive hypothesis of $P_1$. Therefore, $P_2$ uniform $(d, n, V)$ holds as required.

Finally, we can merge $P_2$ and $\eta_0^{\mathcal{I}(\{x : L(b)\})}(P_0)$ into $P$ that satisfies $P$ uniform $(d, n, V)$. This concludes the proof.  

The following lemma concerns the construction of a multivariate annotation for a primitive recursion and is more general than Lemma 13.

\textbf{Lemma 16 (Resource annotation for resource-polymorphic recursion).} Consider a primitive recursion of the form

$$f := \lambda x, \Gamma. \text{case } x \{ [] \mapsto e_0 \mid y :: ys \mapsto \text{let } z = f \ ys \ \Gamma \ 	ext{in } e_1 \}. $$

Let $P_i$ and $Q_i$ for $i \in \{0, 1\}$ be multivariate annotations that satisfy

$$\Gamma; P_i \vdash e_0 : \langle b_2, Q_0 \rangle \quad y : b, ys : L(b), z : b_2; P_i \vdash e_1 : \langle b_2, Q_1 \rangle.$$ 

For each $i \in \mathcal{I}(\{y : b, ys : L(b)\})$, a multivariate annotation $P_{2,i}$ is defined by

$$\Gamma, x : L(b); P_{2,0} \vdash f \ x \ \Gamma : \langle b_2, \pi_{i}^{L_{b_2}}(P_1) - Q_1 \rangle \quad \text{if } i = 0;$$

$$\Gamma, x : L(b); P_{2,1} \vdash f \ x \ \Gamma : \langle b_2, \pi_{i}^{L_{b_2}}(P_1) \rangle \quad \text{otherwise},$$

where $f \ x \ \Gamma$ denotes the whole primitive recursion. From $P_1$ and $P_{2,i}$ for $i \in \mathcal{I}(\{y : b, ys : L(b)\})$, it is possible to build a multivariate annotation $P$ for the entire primitive recursion such that its final output is annotated with $Q_1$.

Furthermore, assume $\Delta; \Gamma \vdash e_0 \ \text{inhpoly} (V)$. If we have
\(P_0\) uniform \((d, n, V)\), where \(d > 0\), and
\(P_{2,i}\) uniform \((d - 1, n_i, V \cup \{x\})\) for each \(i \in \mathcal{I}\{(y : b, ys : L(b))\}\) and some \(n_i \in \mathbb{Q}_{>0}\) then \(P\) uniform \((d, n, V \cup \{x\})\) is true as well.

Proof. It is given that each recursive call needs \(P_1\) much potential. This information does not directly tell us the total amount of potential. This is because \(P_1\) involves \(z\), which is the result of the recursive call, and it is not immediately obvious how to relate \(z\) back to \(x\), which is the original input. Hence, the first task is to work out a multivariate annotation for each recursive call in terms of \(\{y, ys\} \cup \Gamma\) (instead of \(\{y, ys, z\}\)).

As stated in the theorem, let \(P\) be the annotation for the entire primitive recursion that we aim to construct in this proof. In the second branch of the primitive recursion, as a result of pattern matching in \(x\), \(P\) becomes \(\triangleleft(P)\) whose domain is \(\Gamma \cup \{y : b, ys : L(b)\}\).

Base polynomials in \(P_1\) can be classified into three categories:

- Base polynomials that only concern \(\{y, ys\}\). The coefficients of these polynomials are given by \(\pi_0^{\{y : b, ys : L(b)\}}(P_1)\).
- Base polynomials that only concern \(z\). The coefficients of these base polynomials are given by \(\pi_0^{\{z : b\}}(P_1)\). Out of this potential, \(Q_1\) will be paid by \(P\) because \(P\) is exactly what we are trying to establish at the moment and we are allowed to reuse \(\pi_0^{\{z : b\}}(P_1) - Q_1\), will be paid by \(P_{2,0}\) in the assumption.
- Base polynomials that concern both \(\{y, ys\}\) and \(z\). We can replace \(z\) with \(\{y, ys\}\) in the representation of these base polynomials by using \(P_{2,i}\), where \(i \neq 0 \in \mathcal{I}\{(y : b, ys : L(b))\}\).

Let \(\zeta\) be \(\Gamma \cup \{y : b, ys : L(b)\}\). The total potential needed by each recursive call is then given by
\[
\eta_0^\zeta(\pi_0^{\{y : b, ys : L(b)\}}(P_1)) + \sum_{i \in \mathcal{I}\{(y : b, ys : L(b))\}} P_{2,i} \cdot i,
\]
where \(P_{2,i} \cdot i\) denotes the product of \(P_{2,i}\), whose typing context is \(\Gamma \cup \{x : L(b)\}\), and base polynomial \(i\), whose typing context is \(\{y : b, ys : L(b)\}\). Notice that the typing context of \(P_{2,i}\) and that of \(i\) overlap—they have \(\{ys : L(b)\}\) in common.

Because this should be equal to \(\triangleleft(P)\), we obtain
\[
\triangleleft(P) - \eta_0^\zeta(P) = \eta_0^\zeta(\pi_0^{\{y : b, ys : L(b)\}}(P_1)) + \sum_{i \in \mathcal{I}\{(y : b, ys : L(b))\}} P_{2,i} \cdot i. \tag{E.6}
\]

From the right hand side, we can construct a desirable \(P\) such that (E.6) holds, as done in the proof of Lemma 13. Specifically, \(\triangleleft(P)\) is defined as
\[
\triangleleft(P)(i, j, k) := \begin{cases} P(i, 0_b :: k) + P(i, k) & \text{if } j = 0_b; \\ P(i, j :: k) & \text{otherwise.} \end{cases}
\]

Hence, \(\triangleleft(P) - \eta_0^\zeta(P)\) is given as follows. If \(j = 0_b\), then
\[
(\triangleleft(P) - \eta_0^\zeta(P))(i, j, k) = \triangleleft(P)(i, 0_b, k) - \eta_0^\zeta(P)(i, 0_b, k)
= P(i, 0_b :: k) + P(i, k) - P(i, k)
= P(i, 0_b :: k).
\]
Conversely, if \( j \neq 0_b \), then
\[
(\angle(P) - \eta^C_0(P))(i, j, k) = \angle(P)(i, j, k) - \eta^C_0(P)(i, j, k) = P(i, j :: k) + P(i, k) - 0 = P(i, j :: k).
\]

In conclusion, we obtain
\[
(\angle(P) - \eta^C_0(P))(i, j, k) = P(i, j :: k)
\]
regardless of whether \( j = 0_b \) or not. This must be equal to the right hand side of (E.6), and it is clear that such \( P \) is guaranteed to exist. In addition, it must be possible to extract \( Q_0 \) from \( P \) when \( x \) is the empty list. This yields \( P \)'s definition:
\[
P(i, j :: k) := \eta^C_0(\prod_{0}(\frac{y}{b}, \frac{y}{g} \cdot L(b))(P_1))(i, j, k) + \sum_{r \in \mathcal{I}(\{y, b, y \cdot g \cdot L(b)\})} (P_2, \cdot r)(i, j, k)
\]
\[
P(i, 0_b) := Q_0(i).
\]
(7.6)

It remains to check that \( P \) uniform\((d, n, V)\) holds. Consider \( v \in \text{dom}(\Gamma) \setminus V \). We will first prove the first and second conditions of Definition 7 for \( P \). If \( \text{deg}(i) \geq d > 0 \) (which is a stronger condition than \( \text{deg}(i) > d \)), it gives
\[
P(i, j :: k) = \eta^C_0(\prod_{0}(\frac{y}{b}, \frac{y}{g} \cdot L(b))(P_1))(i, j, k) + \sum_{r \in \mathcal{I}(\{y, b, y \cdot g \cdot L(b)\})} (P_2, \cdot r)(i, j, k)
\]
\[
= \sum_{r \in \mathcal{I}(\{y, b, y \cdot g \cdot L(b)\})} (P_2, \cdot r)(i, j, k) = 0.
\]

Here, the second line follows from the definition of the extension operator \( \eta^C_0 \). Because we extend \( \prod_{0}(\frac{y}{b}, \frac{y}{g} \cdot L(b))(P_1) \) with \( 0_r \), we have \( \eta^C_0(\prod_{0}(\frac{y}{b}, \frac{y}{g} \cdot L(b))(P_1))(i, j, k) = 0 \) whenever \( i \neq 0_r \) (which is the case since \( \text{deg}(i) \geq d > 0 \)). With regard to the third line above, due to the assumption \( P_2, \cdot r \) uniform\((d - 1, n_r, V \cup \{x\})\), \( (P_2, \cdot r)(i, j, k) > 0 \) only if \( \text{deg}(i) \leq d - 1 \). Therefore, if \( \text{deg}(i) = d \), we have \( P(i, j :: k) = 0 \) for any \( j :: K \), thereby establishing the second condition of Definition 7.

In the case of \( P(i, 0_b) \), if \( \text{deg}(i) > d \), we have
\[
P(i, 0_L(b)) = Q_0(i) = 0,
\]
where the second line follows from the assumption \( Q_0 \) uniform\((d, n, V)\). Therefore, the first and second conditions of Definition 7 are true for \( P \).

Finally, to prove the third condition of Definition 7, consider \( i \in \mathcal{I}(\Gamma) \), where \( \text{deg}(i) = d \). This gives
\[
P(i, 0_L(b)) = Q_0(i) = n
\]
where the second line follows from the assumption \( Q_0 \) uniform\((d, n, V)\).

In summary, all the three conditions of Definition 7 hold for \( P \). Therefore, \( P \) uniform\((d, n, V \cup \{x\})\) is indeed true. This concludes the proof.