Semantic foundations of potential-synthesis for expected amortised-cost analysis

Ohad Kammar and Georg Moser

11^{th} ACM SIGPLAN Workshop
on
Higher-Order Programming with Effects
HOPE@ICFP'23

Seattle
04 September, 2023

THE UNIVERSITY of EDINBURGH informatics lfcs Laboratory for Foundations of Computer Science BayesCentre

supported by: THE ROYAL SOCIETY The Alan Turing Institute Facebook Research

Complexity analysis of Data Structures

Interface

Operations

Guaranteed complexity bounds

Implementation

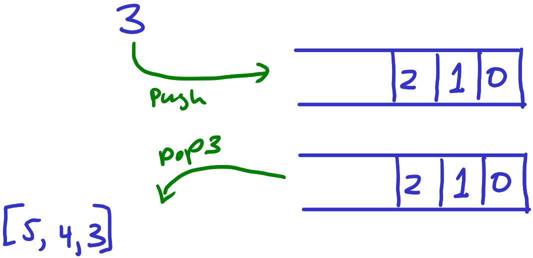
Datatype (invariants)

functions (specs)

Complexity analysis of Data Structures

Interface	Implementation
Operations	Datatype (invariants)
Guaranteed complexity bounds	functions (specs)

Ex: Stacks



Complexity analysis of Data Structures

Worst case analysis

$c(\mathrm{push})(a, s)$ 1 insertion

$c(\mathrm{pop})(k, s)$ k deletions

Interface

Operations

Guaranteed complexity bounds

Amortized analysis [Tarjan '85]

Worst case for operation sequences

$a(\mathrm{push})(a, s)$ 2 units

$a(\mathrm{pop})(k, s)$ 0 units

$$\rightsquigarrow c(op_1, \ldots, op_n) \le a(op_1) + \ldots + op(o_n) \le 2n$$

Complexity analysis of Data Structures

Worst Case analysis

$c(\mathrm{push})(a,s)$ 1 insertion

$c(\mathrm{pop})(k,s)$ k deletions

Amortized analysis [Tarjan '85]

Worst case for operation sequences

$a(\mathrm{push})(a,s)$ 2 units

$a(\mathrm{pop})(k,s)$ 0 units

$\rightsquigarrow$ $c(op_1, \ldots, op_n)$

$\leq a(op_1) + \ldots + op(o_n)$

$\leq 2n$

Proof idea

$c(\text{deletions}) \leq \#\text{insertions}$

$\sum a(op_i) = 2 \times \#\text{insertions to}$

$\geq \#\text{insertions} +$

$\#\text{deletions}$

$= c(op_1 \ldots op_n)$

Complexity analysis of Data Structures

Worst case analysis

$c(push)(a,s)$ 1 insertion

$c(pop)(k,s)$ k deletions

Amortized analysis [Tarjan '85]

Worst case for operation sequences

$a(push)(a,s)$ 2 units

$a(pop)(k,s)$ 0 units

imaginary/abstract costs

$\rightsquigarrow c(op_1, \ldots, op_n)$

$\leq a(op_1) + \ldots + op(o_n)$

$\leq 2n$

Proof idea

$c(\text{deletions}) \leq \#\text{insertions}$

$\sum a(op_i) = 2 \times \#\text{insertions to}$

$\geq \#\text{insertions} + \#\text{deletions}$

$= c(op_1 - op_n)$

Potential method [Tarjan '85]

Guess $\phi : \text{data structure} \to \text{Cost}$

$a(op) : \text{input} \to \text{Cost}$

Such that

$$a(op)(x,s) + \phi(s) \geq \phi(op(x,s)) + C(op)(x,s)$$

$\Delta\phi(op)(x,s) := \phi(s) - \phi(op(x,s))$ potential difference

$\geq C(op) - a(op)$

telescopic & accounts for amortisation discrepency

Potential method [Tarjan '85]

$$C(op_1 \ldots op_n)(s) \leq \sum a(op_i) + \Delta\phi(op_1 \ldots op_n)(s)$$

Telescopic argument:

$$\phi(op_1 \ldots op_n)(s) + C(op_1 \ldots op_n) \leq$$

$$a(op_1) + \phi(op_2 \ldots op_n)(s) + C(op_2 \ldots op_n) \leq \cdots$$

$$a(op_1) + \ldots + a(op_n) + \phi(s) \qquad \blacksquare$$

NB:

$$a(op)(x,s) + \phi(s) \geq \phi(op(x,s)) + C(op)(x,s)$$

Automated / interactive

Amortized Analysis of Resources (A^3R)

[Hofmann, Jost, Hoffmann et al 2000
2003
2006
4x 2009
⋮
2021]

Interface

Implementation

Operations $\xrightarrow{\text{declare}}$ Datatype (invariants)

↓ implement

Guaranteed complexity bounds $\xleftarrow{\text{derive}}$ functions (specs)

automatically / interactively

A^3R architecture (bird's eye)

effectful typed
λ-calculus with
cost modelling primitives

$\downarrow$

Cost semantics $\models$ Cost analysis

soundness thm.

$P \rightsquigarrow V, \mathrm{Cost}(P)$

(SOS)

spend 1 unit

```
let push(x,s) =
  ✓1;
  cons(x,s)
```

Analyzer

SMT solver

```
let push(x,s) $2 =
  ✓1;
  cons(x,s)
```

Workhorse: a quantitative Hoare logic

potential functions

amortised costs

$$\frac{\Gamma \,\{\!\{\phi_1\} \vdash M : A \,\{\!\{a_1\} \qquad \Gamma, x{:}A \,\{\!\{\phi_2\} \vdash K : B \,\{\!\{a_2\}}{\Gamma \,\{\!\{\phi_3\} \vdash \mathrm{let}\ x = M\ \mathrm{in}\ K : B \,\{\!\{a_3\}} \quad \phi_1 \rightsquigarrow \ldots$$

constraint

Quantitative weakest pre "condition" calculus [Kozen '85, McIver & Morgan '04]

- ϕ_i, a_j synthesised by SMT solver

- constraints guarantee soundness w.r.t. cost semantics.

$$\cdot|\cdot \vdash P : A \,\{\!\{a\} \implies \mathrm{cost}\ P \leq a$$

Motivation: ATLAS [Leutgeb, Moser, Zuleger '22]

Probabilistic data structures

- randomized splay trees [Albers & Karpinski '02]
- splay heaps [Gambin & Malinowski '98]
- meldable heaps

Achieves tight bounds using hereditary ranking functions & poly-logarithmic cost functions:

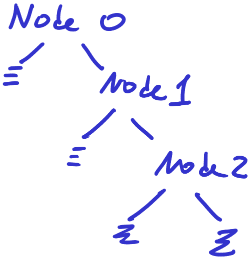
$$\left[\!\left[\begin{matrix} rk \\ q \end{matrix} \middle| \begin{matrix} (a_1, b_1) \\ p_1 \end{matrix} \quad \text{—} \quad \begin{matrix} (a_n, b_n) \\ p_n \end{matrix} \right]\!\right] : \text{Binary Search Trees} \longrightarrow [0, \infty]$$

$$t \mapsto q \cdot rk(t) + \sum_i p_i \cdot lg(a_i \cdot size\, t + b_i)$$

Motivation: ATLAS [Leutgeb, Moser, Zuleger '22]

But bad bounds on, e.g., stacks

encoded as trees: $[0,1,2] \rightsquigarrow$



Synthesizes amortized cost for push:

$$a(push) + \Delta\phi(t) \approx \log t \gg 2.$$

A^3R design tensions

expressivity

tighter bounds

quantity DSL expressivity

\+

\+

rapid prototyping of analysis

\-

\-

solveable by SMT

Soundness

Our Proposal: Nano-pass architecture

Layer | Semantics | Meta-theory

Challenge: manage expressivity tradeoffs

Computational cost model

$\Gamma \vdash M : A$

$[\![\Gamma]\!] \xrightarrow[{[\![M]\!]}]{} K([\![A]\!] \times [0,\infty])$

adequacy

Our Proposal: Nano-pass architecture

Layer | Semantics | meta-theory

E.g. t: binary tree $\vdash \varphi \iff t$ is a search tree

Logical spec (not today)

$\Gamma \mid \Lambda \vdash M : A \mid \varphi$

$$\begin{tikzcd}
{[\![\Gamma \mid \Lambda]\!]} \arrow[r] \arrow[d, hook, "\text{refinement}"] & K([\![\Gamma \mid \Lambda \vdash A \mid \varphi]\!] \times [0,\infty]) \arrow[d, hook] \\
{[\![\Gamma]\!]} \arrow[r, "{[\![M]\!]}"'] & K([\![A]\!] \times [0,\infty])
\end{tikzcd}$$

adequacy

Computational cost model

$\Gamma \vdash M : A$

Our Proposal: Nano-pass architecture

Layer | **Semantics** | **Meta-theory**

Quantitative estimands

$\Gamma \mid \xi_1 \leq \xi_2 \vdash M : A \mid \xi_3 \leq \xi_4$

estimand semantics

$[\![\Gamma \vdash \xi]\!] : [\![\Gamma]\!] \to [0,\infty]$

$\Gamma \vdash \mathrm{cost}\ M : [\![\Gamma]\!] \to [0,\infty]$

soundness of wp transformers

Logical spec (not today)

$\Gamma \mid \Lambda \vdash M : A \mid \varphi$

Computational cost model

$\Gamma \vdash M : A$

$$\begin{array}{ccc} [\![\Gamma \mid \Lambda]\!] & \longrightarrow & K([\![\Gamma \mid \Lambda \vdash A \mid \varphi]\!] \times [0,\infty]) \\ \Big\downarrow & \text{refinement} & \Big\downarrow \\ [\![\Gamma]\!] & \xrightarrow[\ [\![M]\!]\ ]{} & K([\![A]\!] \times [0,\infty]) \end{array}$$

adequacy

Our Proposal: Nano-pass architecture

Layer | **Semantics** | **Meta-theory**

Analysis

$\Gamma \S\S \Phi \vdash M : A \S\S a$

$\Phi, a \rightsquigarrow \vec{\xi}_i$

Soundness of analysis

Quantitative estimands

$\Gamma \mid \xi_1 \leq \xi_2 \vdash M : A \mid \xi_3 \leq \xi_4$

estimand semantics

$[\![\Gamma \vdash \xi]\!] : [\![\Gamma]\!] \to [0,\infty]$

$\Gamma \vdash \mathrm{Cost}\, M : [\![\Gamma]\!] \to [0,\infty]$

Soundness of wp transforms

Logical spec (not today)

$\Gamma \mid \Lambda \vdash M : A \mid \varphi$

Computational cost model

$\Gamma \vdash M : A$

$$
\begin{tikzcd}
{[\![\Gamma \mid \Lambda]\!]} \arrow[r] \arrow[d, hook] \arrow[dr, phantom, "\text{refinement}"] & K([\![\Gamma \mid \Lambda \vdash A \mid \varphi]\!] \times [0,\infty]) \arrow[d, hook] \\
{[\![\Gamma]\!]} \arrow[r, "{[\![M]\!]}"'] & K([\![A]\!] \times [0,\infty])
\end{tikzcd}
$$

adequacy

Our Proposal: Nano-pass architecture [WIP]

Layer	Semantics	Meta-theory
Analysis $\Gamma \mid \Phi \vdash M : A \mid a$	$\Phi, a \rightsquigarrow \vec{\xi_i}$	Soundness of analysis
Quantitative estimands $\Gamma \mid \xi_1 \leq \xi_2 \vdash M : A \mid \xi_3 \leq \xi_4$	estimand semantics $[\![\Gamma \vdash \xi]\!] : [\![\Gamma]\!] \to [0, \infty]$ $\Gamma \vdash \mathrm{Cost}\ M : [\![\Gamma]\!] \to [0, \infty]$	Soundness of WP transforms
Logical spec (not today) $\Gamma \mid \Lambda \vdash M : A \mid \varphi$	$[\![\Gamma \mid \Lambda]\!] \longrightarrow K([\![\Gamma \mid \Lambda \vdash A \mid \varphi]\!] \times [0, \infty])$ refinement	
Computational cost model $\Gamma \vdash M : A$	$[\![\Gamma]\!] \xrightarrow[{[\![M]\!]}]{} K([\![A]\!] \times [0, \infty])$	adequacy

Rest of talk

Contribution: isolate a 1^{st} order language
resolving the expressivity tension

Technical details of:

1) data types & their semantics
2) computational layer terms & types
3) semantics with Kegelspitze [Keimel&Plotkin'17]

Data Types

$\Theta = \{\alpha, \beta, \gamma, \dots\}$

$$
\begin{array}{lll}
\rho & ::= C_1 \textbf{ of } A_1 \mid C_2 \textbf{ of } A_2 \mid \cdots \mid C_n \textbf{ of } A_n & \text{rows of typed data-constructors} \\
A, B, D & ::= & \text{ground types relative to } \Theta \\
 & \quad \alpha & \quad \text{named type } \alpha \in \Theta \\
 & \mid \quad \{\rho\} & \quad \text{variant/sum type} \\
 & \mid \quad \lhd \rho \rhd & \quad \text{record/product type}
\end{array}
$$

Ex

$$
\begin{array}{lll}
\textbf{data Unit} & = & \lhd\rhd \\
\textbf{data Bool} & = & \{\text{True}, \text{False of Unit}\} \\
\textbf{data Nat} & = & \{\text{Z of Unit} \mid \text{S of Nat}\} \\
\textbf{data List Nat} & = & \{\text{Nil of Unit} \\
 & & \mid \_ :: \_ \text{ of } \lhd \text{Head of Nat} \\
 & & \qquad \mid \text{Tail of List Nat} \rhd\} \\
\textbf{data Tree Nat} & = & \{\text{Nil of Unit} \\
 & & \mid \text{Node of } \lhd \text{L, R of Tree Nat} \\
 & & \qquad \mid \text{V of Nat} \rhd\}
\end{array}
$$

Data types: initial algebra semantics [Goguen, Thatcher '74]

$$[\![\Theta]\!] := \omega\mathrm{Cpo}^{\Theta}$$

$$[\![\Theta \vdash A]\!] := \left\{ \omega\mathrm{Cpo}^{\Theta} \xrightarrow{F} \omega\mathrm{Cpo} \;\middle|\; \begin{array}{l} F \text{ locally cts } + \\ \text{has initial algebra} \end{array} \right\}$$

Fixing a <u>data signature</u> $T = (\Theta, \mathrm{type} : \Theta \to \mathrm{Type}(\Theta))$

$$[\![\alpha]\!]_T := \mu\, [\![\Theta \vdash \mathrm{type}\ \alpha]\!]$$

1^{st} order types

$$
\begin{array}{llll}
\Gamma_{\mathbf{Gnd}} & := & x_1 : A_1, \ldots, x_n : A_n & \text{ground typing contexts} \\
F, G, H & ::= & (\Gamma_{\mathbf{Gnd}}) \longrightarrow A & 1^{\text{st}}\text{-order function type} \\
\Gamma_{\mathbf{Fun}} & ::= & f_1 : F_1, \ldots, f_n : F_n & \text{function typing contexts} \\
\Gamma & ::= & \Gamma_{\mathbf{Fun}}; \Gamma_{\mathbf{Gnd}} & \text{typing contexts}
\end{array}
$$

functions are 2^{nd} class here!

1^{st} order language: terms

STLC + Pattern matching on algebraic datatypes + recursion

$$
\begin{array}{lll}
M, N ::= & & \\
& x \mid c & \\
\mid & f(M_1, \ldots, M_n) & \mid\ A.CM \\
\mid & \textbf{let rec } f_1 : (\Gamma^1_{\mathrm{Gnd}}) \to A_1 = M_1 & \mid\ \textbf{case } M \textbf{ of} \\
& \qquad \vdots & \qquad C_1 x_1.N_1 \\
& \qquad f_n : (\Gamma^n_{\mathrm{Gnd}}) \to A_n = M_n & \qquad \vdots \\
& \textbf{in } N & \qquad C_n x_n.N_n \\
\mid & \textbf{let } x_1 = M_1 & \mid\ \langle C_1 := M_1, \ldots, C_n := M_n \rangle \\
& \quad \vdots & \mid\ \textbf{case } M \textbf{ of} \\
& \quad x_n = M_n & \qquad \langle C_1 := x_1, \ldots, C_n := x_n \rangle .N \\
& \textbf{in } N & \mid\ \textbf{unroll } M \mid \alpha.\textbf{roll } M
\end{array}
$$

$$
\begin{array}{ll}
\mid & \checkmark M \\
\mid & \textbf{sample } \mu \\
\mid & \textbf{sample } \mu(M_1, \ldots, M_n)
\end{array}
$$

→ cost modelling

} Probabilistic choice

1st order languge : terms

effects:

$[0,\infty]$

primitive distribution (countably supported)

$$\frac{\Gamma \vdash M : \mathbf{Weight}}{\Gamma \vdash \checkmark M : \mathbf{Unit}} \qquad \frac{(\mu : A) \in \mathcal{F}_{\mathcal{C}}}{\Gamma \vdash \mathbf{sample}\,\mu : A}$$

$$\frac{(\mu : B(x_1 : A_1, \ldots, x_n : A_n)) \in \mathcal{F}_{\mathcal{C}} \qquad \text{for all } i = 1, \ldots, n : \Gamma \vdash M_i : A_i}{\Gamma \vdash \mathbf{sample}\,\mu(M_1, \ldots, M_n) : B}$$

primitive kernel (countably supported)

Semantics

$$[\![\Gamma_{\mathrm{Gnd}} \to A]\!] := \omega\mathrm{Cpo}\left([\![\Gamma_{\mathrm{Gnd}}]\!], \mathcal{K}([\![A]\!] \times [0,\infty])\right)$$

free Kegelspitze monad

$$[\![\Gamma_{\mathrm{Gnd}}]\!] := \prod_{x:A} [\![A]\!] \qquad [\![\Gamma_{\mathrm{Fun}}]\!] := \prod_{f:\Gamma_{\mathrm{Gnd}} \to A} [\![\Gamma_{\mathrm{Gnd}} \to A]\!]$$

$$[\![\Gamma_{\mathrm{Fun}}; \Gamma_{\mathrm{Gnd}}]\!] := [\![\Gamma_{\mathrm{Fun}}]\!] \times [\![\Gamma_{\mathrm{Gnd}}]\!]$$

$$[\![\Gamma \vdash M : A]\!] : [\![\Gamma]\!] \longrightarrow \mathcal{K}([\![A]\!] \times [0,\infty])$$

Kegelspitze (Idea)

$$\begin{tikzcd}
\text{discrete measures} & & \text{Positive Cones [Tix '99 Selinger '04]} \\
\text{discrete probabilities} \arrow[u, hook] & & \text{Kegelspitzen [Keimel, Plotkin '17]} \arrow[u, hook]
\end{tikzcd}$$

Kegelspitze (algebraic effects)

Semantic domain for discrete measures: $[0,\infty]$-modules:

$$\left(A, \sum_{i=1}^{n} \underset{\underset{0}{\vee|}}{w_i} \cdot - : A^n \to A\right) + \text{equations}$$

Semantic domain for discrete Probability [Stone'42]

$$\left(A, \sum_{i=1}^{n} p_i \cdot - : A^n \to A\right) + \text{equations}$$

$$\Sigma_i p_i = 1$$

Barycentric algebra

Presented as $\rightsquigarrow$ $\left(A, \underset{r:s}{(+)} : A^2 \to A\right)$ betting odds

$$(r,s) \in [0,\infty)^2 \setminus \{(0,0)\}$$

Kegelspitze

scott cts

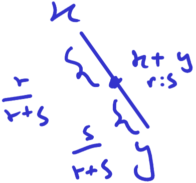
Kegelspitze $\left(A, \underset{r:s}{(+)} : A^2 \to A, (\cdot) : [0,1] \times A \to A\right)$

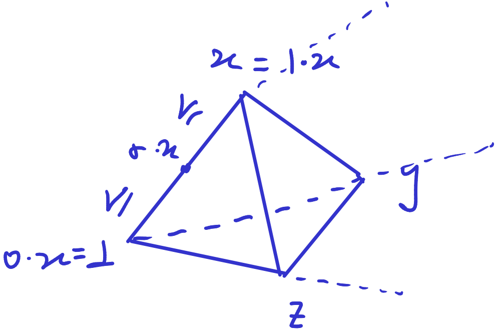
pointed wcpo

- $(A, (+))$ Barycentric
- $0 \cdot x = \bot$
- $r \cdot x = \bot \underset{(1-r):r}{+} x$

Kegelspitze (Geometric intuition)

Barycentric structure:





$\underbrace{\text{Kegel}}_{\text{cone}}\underbrace{\text{spitze}}_{\text{tip}}$

Kegelspitze

Representation Thm: [Adapted from Keimel & Plotkin]

Subprobability distributions on $[\![A]\!]$ with dirac measures form the free Kegelspitze on $[\![A]\!]$

Our Proposal: Nano-pass architecture

Layer | **Semantics** | **Meta-theory**

Analysis

$\Gamma \,\S\S\, \phi \vdash M : A \,\S\S\, a$

$\phi, a \rightsquigarrow \vec{\xi}_i$

Soundness of analysis

Quantitative estimands

$\Gamma \mid \xi_1 \leq \xi_2 \vdash M : A \mid \xi_3 \leq \xi_4$

estimand semantics

$[\![\Gamma \vdash \xi]\!] : [\![\Gamma]\!] \to [0,\infty]$

$\Gamma \vdash \mathrm{Cost}\, M : [\![\Gamma]\!] \to [0,\infty]$

Soundness of wp transforms

Logical spec (not today)

$\Gamma \mid \Lambda \vdash M : A \mid \varphi$

$$\begin{tikzcd}
[\![\Gamma \mid \Lambda]\!] \arrow[r] \arrow[d, hook, "\text{refinement}"] & K([\![\Gamma \mid \Lambda \vdash A \mid \varphi]\!] \times [0,\infty]) \arrow[d, hook] \\
[\![\Gamma]\!] \arrow[r, "{[\![M]\!]}"'] & K([\![A]\!] \times [0,\infty])
\end{tikzcd}$$

adequacy

Computational cost model

$\Gamma \vdash M : A$