OPERATIONAL ALGORITHMIC GAME SEMANTICS

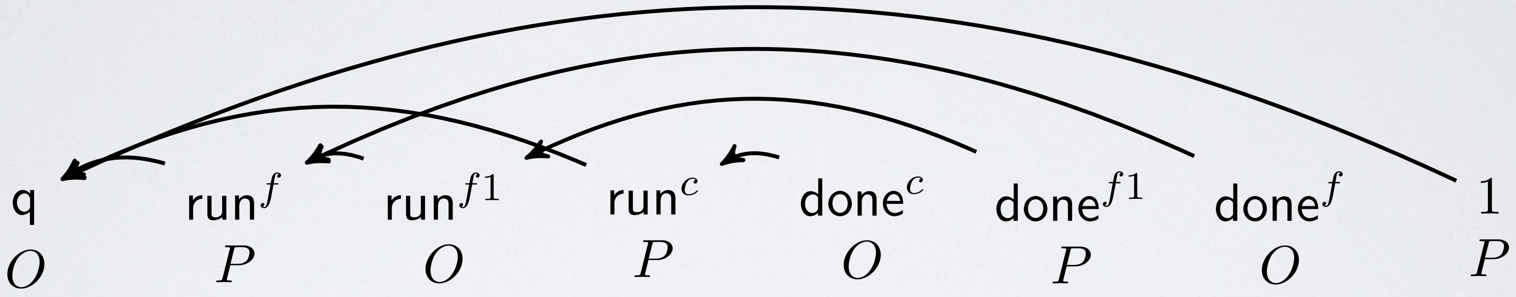
Benedict Bunting
University of Oxford

Andrzej Murawski
University of Oxford

HIGHER-ORDER WITH STATE (FINITARY SETTING)

- **finite base types**
- **(typed) lambda calculus**
- **assignable variables (only base type)**
- **iteration, no recursion**
- **termination decidable**
- **contextual equivalence undecidable**

GAME SEMANTICS



q O run^{f} P run^{f1} O run^{c} P done^{c} O done^{f1} P done^{f} O 1 P

- O (environment, context), P (program)
- program is interepreted compositionally as a strategy for P
- full abstraction
- plays are words with extra structure

ALGORITHMIC GAME SEMANTICS

- **represent plays as words (strategies as languages)**
- **identify cases when the languages can be specified in formalisms with a decidable equivalence problem**
- **translate terms to automata inductively (for canonical forms)**
- **numerous results over the last two decades**
- **full classifications (type-based) for Idealized Algol (CBN) and RML (CBV)**

IDEALIZED ALGOL (CBN)

Order	Type	Automata / Status
1	$\mathrm{Int} \to \cdots \to \mathrm{Int}$	DFA / decidable (ICALP'00)
2	$(\mathrm{Int} \to \mathrm{Int}) \to \mathrm{Int}$	DFA / decidable (ICALP'00)
3	$((\mathrm{Int} \to \mathrm{Int}) \to \mathrm{Int}) \to \mathrm{Int}$	VPA / decidable (FoSSaCS'05)
4	$(((\mathrm{Int} \to \mathrm{Int}) \to \mathrm{Int}) \to \mathrm{Int}) \to \mathrm{Int}$	undecidable (LICS'03)

ICALP'00: Ghica, McCusker

LICS'03: M.

FoSSaCS'05: M., Walukiewicz

RML (CBV)

Order	Type	Automata / Status
1	$\text{Int} \to \cdots \to \text{Int}$	NDCMA / decidable (FoSSaCS'15)
2	$(\text{Int} \to \cdots \to \text{Int}) \to \text{Int}$	VPA / decidable (ICALP'11)
2	$\text{Int} \to (\text{Int} \to \cdots \to \text{Int}) \to \text{Int}$	EBVASS / open (ESOP'17)
2	$\text{Int} \to \text{Int} \to (\text{Int} \to \text{Int}) \to \text{Int}$	Undecidable (ESOP'17)
2	$(\text{Int} \to \text{Int}) \to \text{Int} \to \text{Int}$	Undecidable (FoSSaCS'15)
3	$((\text{Int} \to \text{Int}) \to \text{Int}) \to \text{Int}$	Undecidable (FoSSaCS'15)

ICALP'11: Hopkins, M., Ong

FoSSaCS'15: Cotton-Barratt, Hopkins, M., Ong

ESOP'17: Cotton-Barratt, M., Ong

THIS TALK

- revisit the results in view of new advances in game semantics (operational game semantics), which present game models as special LTSs
- attempt to extract the automata directly from the LTS
- unify the results for CBN and CBV
- this talk: DVPA and DFA
- claimed advantages: accessibility, generality, model-checking friendly

CBPV (LEVY 1999)

Value Type	σ	$\triangleq$	$U\underline{\tau} \mid \text{Unit} \mid \text{Int} \mid \text{Ref}$
Computation Type	$\underline{\tau}$	$\triangleq$	$F\sigma \mid \sigma \to \underline{\tau}$

$$\frac{\Sigma;\Gamma \vdash^c M : \underline{\tau}}{\Sigma;\Gamma \vdash^v \text{thunk } M : U\underline{\tau}} \qquad \frac{\Sigma;\Gamma \vdash^v V : U\underline{\tau}}{\Sigma;\Gamma \vdash^c \text{force } V : \underline{\tau}}$$

$$\frac{\Sigma;\Gamma \vdash^v V : \sigma}{\Sigma;\Gamma \vdash^c \text{return } V : F\sigma} \qquad \frac{\Sigma;\Gamma \vdash^c M : F\text{Int} \qquad \Sigma;\Gamma \vdash^c N : F\text{Unit}}{\Sigma;\Gamma \vdash^c \text{while}\, M \,\text{do}\, N : F\text{Unit}}$$

$$\frac{}{\Sigma;\Gamma \vdash^{v} () : \mathrm{Unit}} \qquad \frac{n \in \{0,\cdots,\max\}}{\Sigma;\Gamma \vdash^{v} \widehat{n} : \mathrm{Int}} \qquad \frac{(x,\sigma) \in \Gamma}{\Sigma;\Gamma \vdash^{v} x : \sigma} \qquad \frac{\ell \in \Sigma}{\Sigma;\Gamma \vdash^{v} \ell : \mathrm{Ref}} \qquad \frac{\Sigma;\Gamma \vdash^{c} M : \underline{\tau}}{\Sigma;\Gamma \vdash^{v} \mathrm{thunk}\ M : U\underline{\tau}}$$

$$\frac{\Sigma;\Gamma \vdash^{v} V : \sigma}{\Sigma;\Gamma \vdash^{c} \mathrm{return}\ V : F\sigma} \qquad \frac{\Sigma;\Gamma \vdash^{v} V : U\underline{\tau}}{\Sigma;\Gamma \vdash^{c} \mathrm{force}\ V : \underline{\tau}} \qquad \frac{\Sigma;\Gamma \vdash^{v} V : \sigma \qquad \Sigma;\Gamma, x : \sigma \vdash^{c} M : \underline{\tau}}{\Sigma;\Gamma \vdash^{c} \mathrm{let}\ x\ \mathrm{be}\ V.M : \underline{\tau}}$$

$$\frac{\Sigma;\Gamma \vdash^{v} V : \mathrm{Int} \qquad \Sigma;\Gamma \vdash^{c} M_i : \underline{\tau}}{\Sigma;\Gamma \vdash^{c} \mathrm{case}\ V\ \mathrm{of}\ (M_i)_{i \in I} : \underline{\tau}} \qquad \frac{\Sigma;\Gamma \vdash^{c} M : F\sigma \qquad \Sigma;\Gamma, x : \sigma \vdash^{c} N : \underline{\tau}}{\Sigma;\Gamma \vdash^{c} M\ \mathrm{to}\ x.N : \underline{\tau}} \qquad \frac{\Sigma;\Gamma, x : \sigma \vdash^{c} M : \underline{\tau}}{\Sigma;\Gamma \vdash^{c} \lambda x^{\sigma}.M : \sigma \to \underline{\tau}}$$

$$\frac{\Sigma;\Gamma \vdash^{c} M : \sigma \to \underline{\tau} \qquad \Sigma;\Gamma \vdash^{v} V : \sigma}{\Sigma;\Gamma \vdash^{c} MV : \underline{\tau}} \qquad \frac{\Sigma;\Gamma \vdash^{v} V : \mathrm{Int}}{\Sigma;\Gamma \vdash^{c} \mathrm{ref}\ V : F\mathrm{Ref}} \qquad \frac{\Sigma;\Gamma \vdash^{v} V : \mathrm{Ref}}{\Sigma;\Gamma \vdash^{c} !V : F\mathrm{Int}}$$

$$\frac{\Sigma;\Gamma \vdash^{v} V : \mathrm{Ref} \qquad \Sigma;\Gamma \vdash^{v} U : \mathrm{Int}}{\Sigma;\Gamma \vdash^{c} V := U : F\mathrm{Unit}} \qquad \frac{\Sigma;\Gamma \vdash^{c} M : F\mathrm{Int} \qquad \Sigma;\Gamma \vdash^{c} N : F\mathrm{Unit}}{\Sigma;\Gamma \vdash^{c} \mathrm{while}\, M\, \mathrm{do}\, N : F\mathrm{Unit}}$$

CBN AND CBV IN CBPV

For an CBN environment $\Gamma = \{x_1 : \underline{\tau}_1 \cdots x_k : \underline{\tau}_k\}$, let $\Gamma^{\text{CBN}} = \{x_1 : U\underline{\tau}_1{}^{\text{CBN}} \cdots x_k : U\underline{\tau}_k{}^{\text{CBN}}\}$.

The sequent $\Gamma \vdash M : \underline{\tau}$ is translated into $\Gamma^{\text{CBN}} \vdash^c M^{\text{CBN}} : \underline{\tau}^{\text{CBN}}$.

CBN type		CBPV computation types
Int^{CBN}	$=$	$F\text{Int}$
$(\underline{\tau}_1 \to \underline{\tau}_2)^{\text{CBN}}$	$=$	$U\underline{\tau}_1{}^{\text{CBN}} \to \underline{\tau}_2{}^{\text{CBN}}$

For a CBV environment $\Gamma = \{x_1 : \sigma_1 \cdots x_k : \sigma_k\}$, let $\Gamma^{\text{CBV}} = \{x_1 : \sigma_1{}^{\text{CBV}} \cdots x_k : \sigma_k{}^{\text{CBV}}\}$.

The sequent $\Gamma \vdash M : \sigma$ is translated into $\Gamma^{\text{CBV}} \vdash^c M^{\text{CBV}} : F\sigma^{\text{CBV}}$.

CBV type		CBPV value types
Int^{CBV}	$=$	Int
$(\sigma_1 \to \sigma_2)^{\text{CBV}}$	$=$	$U(\sigma_1{}^{\text{CBV}} \to F\sigma_2{}^{\text{CBV}})$

CONTEXTUAL EQUIVALENCE

A ***terminal*** is a (closed) computation of the form $\mathrm{return}\ V$ or $\lambda x^\sigma.M$. Termination means that a term reduces to a terminal: we write $(M, h) \Downarrow_{ter}$ if there exist N, h' such that $(M, h) \to^* (N, h')$ and N is a terminal.

Definition 1. Given computations $\Gamma \vdash^c M_1, M_2 : \underline{\tau}$, we define $\Gamma \vdash^c M_1 \lesssim^{\mathrm{CBPV}}_{ter} M_2$ to hold, when for all contexts $\vdash^k C : \underline{\tau} \Longrightarrow F\sigma$, we have $(C[M_1], \emptyset) \Downarrow_{ter}$ implies $(C[M_2], \emptyset) \Downarrow_{ter}$. We write $\cong^{\mathrm{CBPV}}_{ter}$ for the equivalence induced by $\lesssim^{\mathrm{CBPV}}_{ter}$.

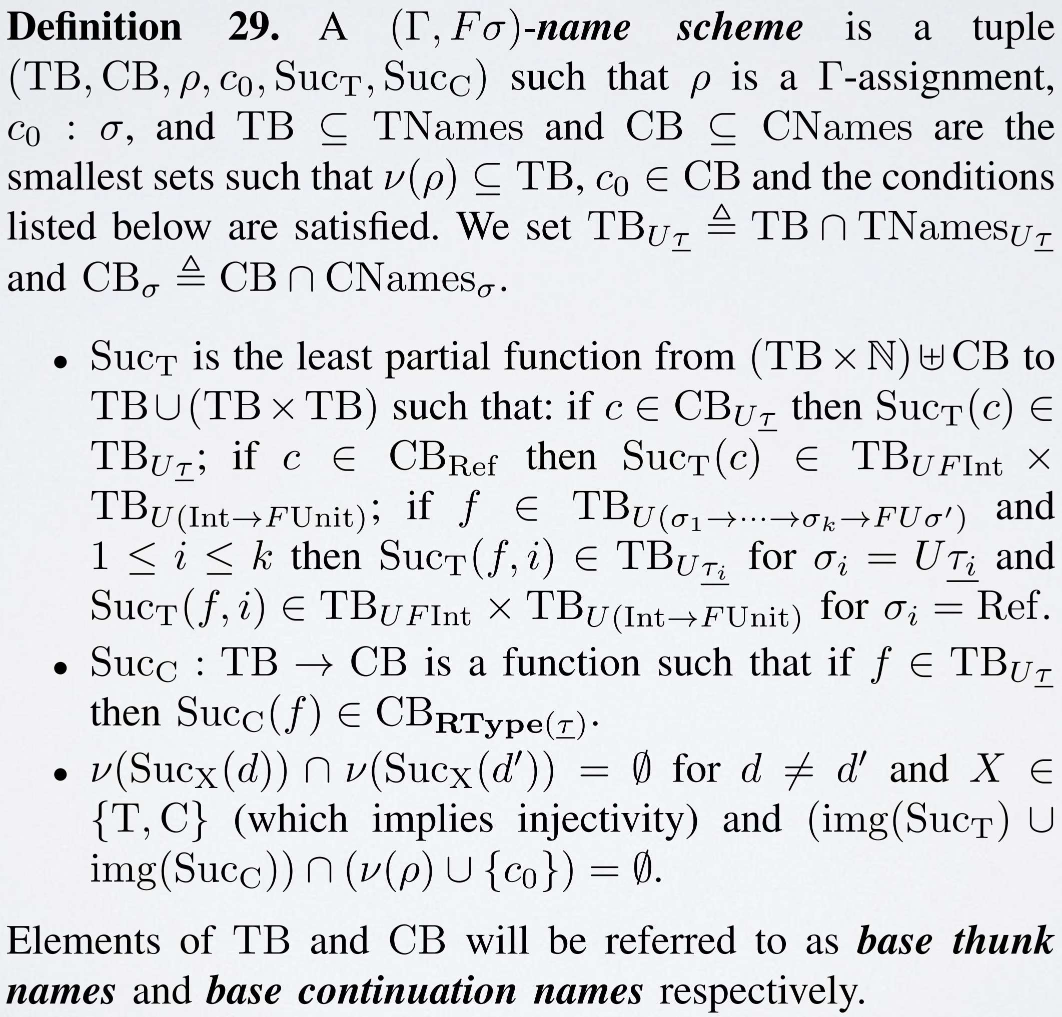
OPERATIONAL GAME SEMANTICS (LTS)

$$
\begin{array}{l|llll}
(P\tau) & \langle M, c, \gamma, \phi, h, H\rangle & \xrightarrow{\tau} & \langle N, c, \gamma, \phi, h', H\rangle \\
 & \quad \text{when } (M,h) \to (N,h') & & \\
(PA) & \langle \text{return } V, c, \gamma, \phi, h, H\rangle & \xrightarrow{\bar{c}(A)} & \langle \gamma\cdot\gamma', \phi \uplus \nu(A), h, H, H(c) \uplus \nu(A)\rangle \\
 & \quad \text{when } c:\sigma,\ (A,\gamma') \in \mathbf{AVal}_\sigma(V) & & \\
(PQ) & \langle K[(\text{force } f)\overrightarrow{V}], c, \gamma, \phi, h, H\rangle & \xrightarrow{\bar{f}(\overrightarrow{A},c')/(c',(K,c))} & \langle \gamma\cdot\gamma', \phi \uplus \phi', h, H, H(f) \uplus \nu(\overrightarrow{A})\rangle \\
 & \quad \text{when } f : U\underline{\tau},\ (\overrightarrow{A},\gamma') \in \mathbf{AVal}(\overrightarrow{V}),\ \sigma = \mathbf{RType}(\underline{\tau}),\ c' : \sigma \text{ and } \phi' = \nu(\overrightarrow{A}) \uplus \{c'\} & & \\
(OA) & \langle \gamma, \phi, h, H, Fn\rangle & \xrightarrow{c(A),(c,(K,c'))} & \langle K[\text{return } A], c', \gamma, \phi \uplus \nu(A), h, H\cdot[\nu(A) \mapsto Fn]\rangle \\
 & \quad \text{when } c:\sigma,\ A:\sigma & & \\
(OQ) & \langle \gamma, \phi, h, H, Fn\rangle & \xrightarrow{f(\overrightarrow{A},c)} & \langle (\text{force } V)\overrightarrow{A}, c, \gamma, \phi \uplus \phi', h, H\cdot[\phi' \mapsto Fn]\rangle \\
 & \quad \text{when } f \in Fn,\ f : U\underline{\tau},\ \overrightarrow{A} \in \mathbf{ASeq}(\underline{\tau}),\ \sigma = \mathbf{RType}(\underline{\tau}),\ c:\sigma,\ \gamma(f) = V \text{ and } \phi' = \nu(\overrightarrow{A}) \uplus \{c\} & &
\end{array}
$$

Given $N \subseteq \text{Names}$, $[N \mapsto \mathcal{V}]$ stands for the map $[n \mapsto \mathcal{V} \mid n \in N]$.

Theorem (Full Abstraction)**.** *For any* CBPV *computations* $\Gamma \vdash^c M_1, M_2 : F\sigma$*, then* $\Gamma \vdash^c M_1 \lesssim_{ter}^{\mathrm{CBPV}} M_2$ *iff* $\mathbf{Tr}_{\mathrm{CBPV}}(\Gamma \vdash^c M_1) \subseteq \mathbf{Tr}_{\mathrm{CBPV}}(\Gamma \vdash^c M_2)$.

TOWARDS A VPA (FINITE ALPHABET)

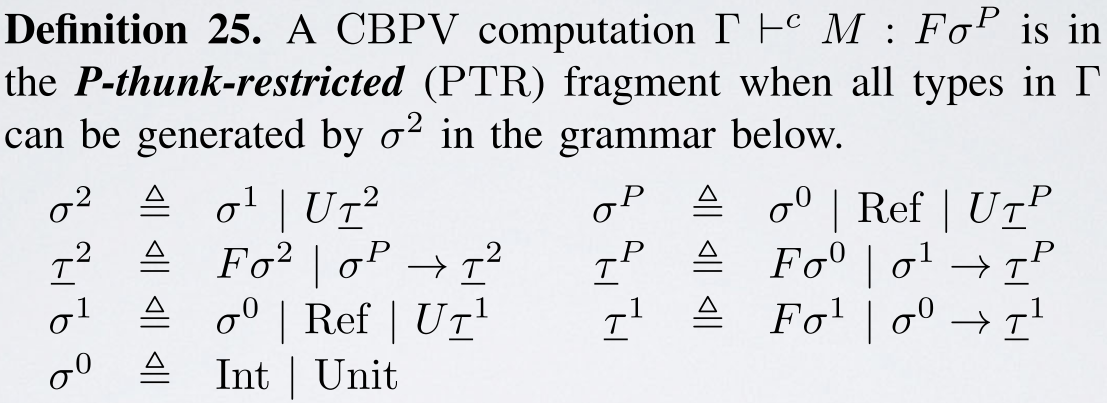


Definition 29. A $(\Gamma, F\sigma)$-***name scheme*** is a tuple $(\mathrm{TB}, \mathrm{CB}, \rho, c_0, \mathrm{Suc_T}, \mathrm{Suc_C})$ such that ρ is a Γ-assignment, $c_0 : \sigma$, and $\mathrm{TB} \subseteq \mathrm{TNames}$ and $\mathrm{CB} \subseteq \mathrm{CNames}$ are the smallest sets such that $\nu(\rho) \subseteq \mathrm{TB}$, $c_0 \in \mathrm{CB}$ and the conditions listed below are satisfied. We set $\mathrm{TB}_{U\underline{\mathcal{T}}} \triangleq \mathrm{TB} \cap \mathrm{TNames}_{U\underline{\mathcal{T}}}$ and $\mathrm{CB}_\sigma \triangleq \mathrm{CB} \cap \mathrm{CNames}_\sigma$.

- $\mathrm{Suc_T}$ is the least partial function from $(\mathrm{TB} \times \mathbb{N}) \uplus \mathrm{CB}$ to $\mathrm{TB} \cup (\mathrm{TB} \times \mathrm{TB})$ such that: if $c \in \mathrm{CB}_{U\underline{\mathcal{T}}}$ then $\mathrm{Suc_T}(c) \in \mathrm{TB}_{U\underline{\mathcal{T}}}$; if $c \in \mathrm{CB_{Ref}}$ then $\mathrm{Suc_T}(c) \in \mathrm{TB}_{UF\mathrm{Int}} \times \mathrm{TB}_{U(\mathrm{Int} \to F\mathrm{Unit})}$; if $f \in \mathrm{TB}_{U(\sigma_1 \to \cdots \to \sigma_k \to FU\sigma')}$ and $1 \leq i \leq k$ then $\mathrm{Suc_T}(f, i) \in \mathrm{TB}_{U\underline{\mathcal{T}_i}}$ for $\sigma_i = U\underline{\mathcal{T}_i}$ and $\mathrm{Suc_T}(f, i) \in \mathrm{TB}_{UF\mathrm{Int}} \times \mathrm{TB}_{U(\mathrm{Int} \to F\mathrm{Unit})}$ for $\sigma_i = \mathrm{Ref}$.
- $\mathrm{Suc_C} : \mathrm{TB} \to \mathrm{CB}$ is a function such that if $f \in \mathrm{TB}_{U\underline{\mathcal{T}}}$ then $\mathrm{Suc_C}(f) \in \mathrm{CB}_{\mathbf{RType}(\underline{\mathcal{T}})}$.
- $\nu(\mathrm{Suc_X}(d)) \cap \nu(\mathrm{Suc_X}(d')) = \emptyset$ for $d \neq d'$ and $X \in \{\mathrm{T}, \mathrm{C}\}$ (which implies injectivity) and $(\mathrm{img}(\mathrm{Suc_T}) \cup \mathrm{img}(\mathrm{Suc_C})) \cap (\nu(\rho) \cup \{c_0\}) = \emptyset$.

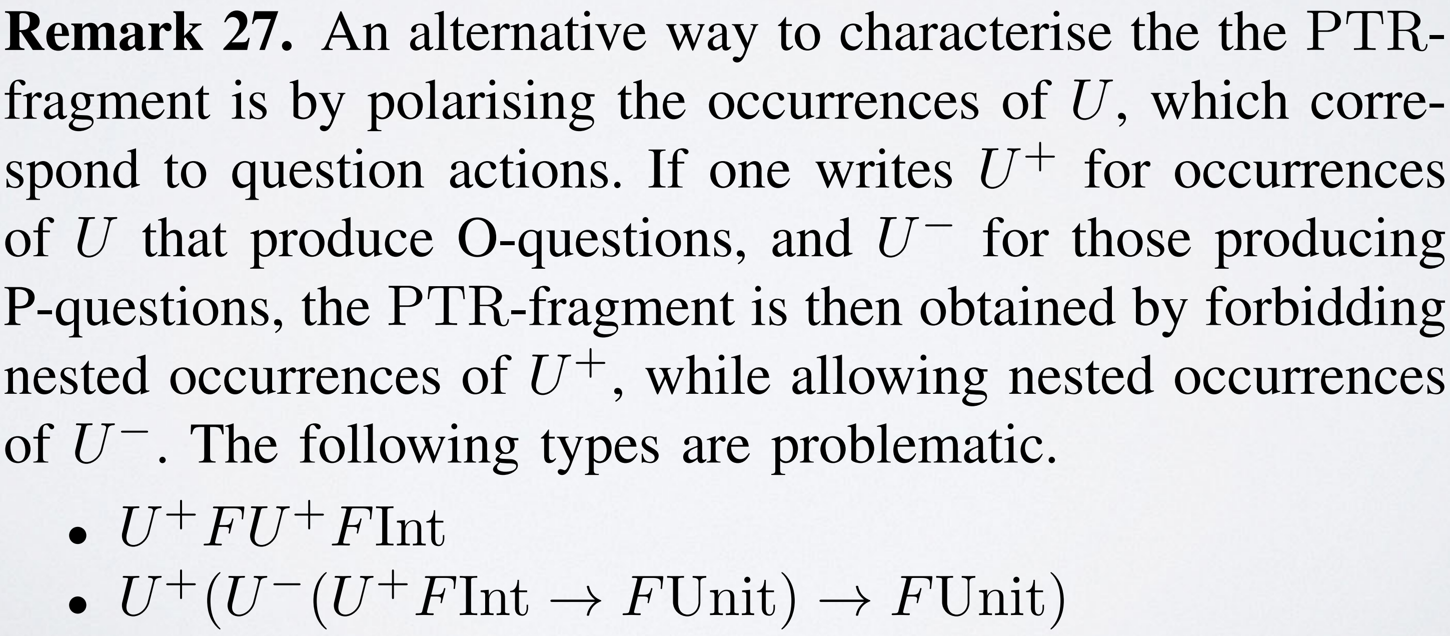
Elements of TB and CB will be referred to as ***base thunk names*** and ***base continuation names*** respectively.

SPECIAL FRAGMENT



Definition 25. A CBPV computation $\Gamma \vdash^c M : F\sigma^P$ is in the ***P-thunk-restricted*** (PTR) fragment when all types in Γ can be generated by σ^2 in the grammar below.

$$\begin{array}{lcl@{\qquad\qquad}lcl}
\sigma^2 & \triangleq & \sigma^1 \mid U\underline{\tau}^2 & \sigma^P & \triangleq & \sigma^0 \mid \mathrm{Ref} \mid U\underline{\tau}^P \\
\underline{\tau}^2 & \triangleq & F\sigma^2 \mid \sigma^P \to \underline{\tau}^2 & \underline{\tau}^P & \triangleq & F\sigma^0 \mid \sigma^1 \to \underline{\tau}^P \\
\sigma^1 & \triangleq & \sigma^0 \mid \mathrm{Ref} \mid U\underline{\tau}^1 & \underline{\tau}^1 & \triangleq & F\sigma^1 \mid \sigma^0 \to \underline{\tau}^1 \\
\sigma^0 & \triangleq & \mathrm{Int} \mid \mathrm{Unit} & & &
\end{array}$$



Remark 27. An alternative way to characterise the the PTR-fragment is by polarising the occurrences of U, which correspond to question actions. If one writes U^+ for occurrences of U that produce O-questions, and U^- for those producing P-questions, the PTR-fragment is then obtained by forbidding nested occurrences of U^+, while allowing nested occurrences of U^-. The following types are problematic.

- $U^+FU^+F\mathrm{Int}$
- $U^+(U^-(U^+F\mathrm{Int} \to F\mathrm{Unit}) \to F\mathrm{Unit})$

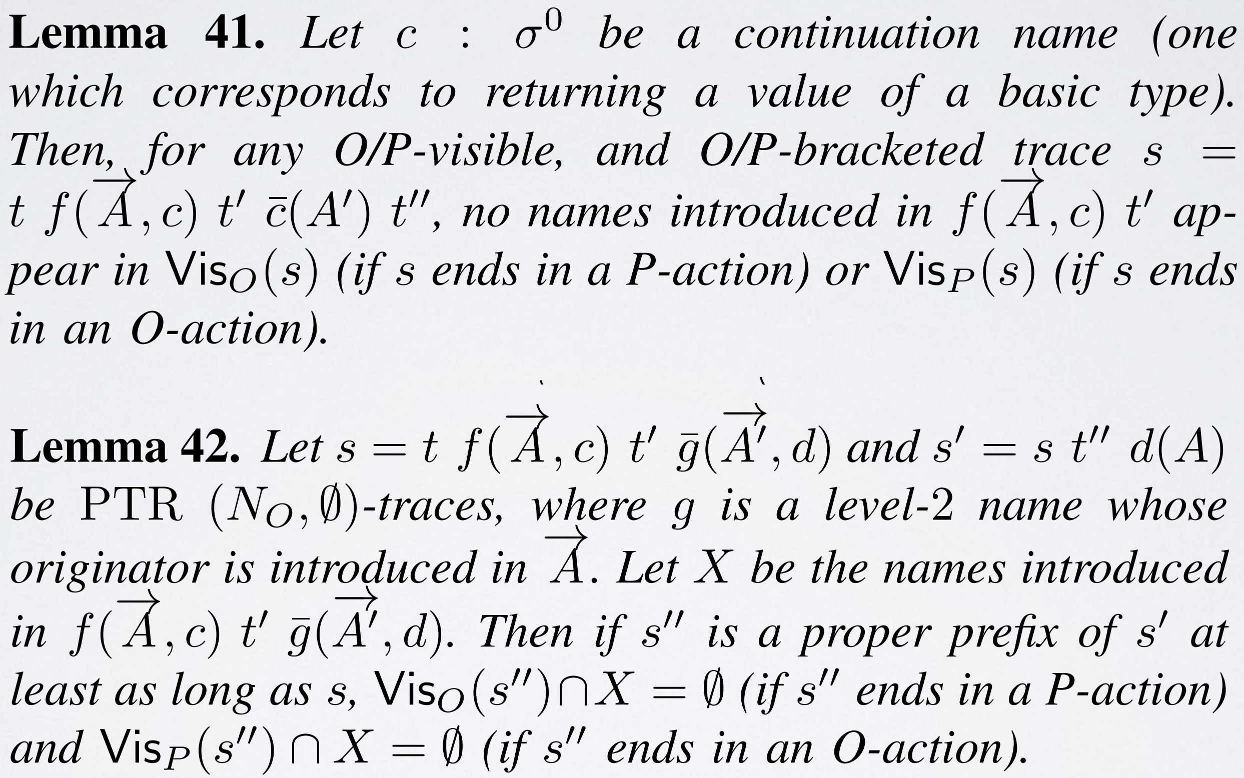
MARKED NAMES (FOR P-MOVES)

$\{\mathtt{t}\}$ where $\mathtt{t} = \bar{f}(\epsilon, d)\ d(g)\ \bar{f}(\epsilon, d)\ d(g)\ \bar{g}(\epsilon, e)\ e(())\ \bar{c_0}(())$

$\{\mathtt{t}, \bar{f}(\epsilon, d)\ d(\hat{g})\ \bar{f}(\epsilon, d)\ d(g)\ \bar{\hat{g}}(\epsilon, e)\ e(())\ \bar{c_0}(()), \bar{f}(\epsilon, d)\ d(g)\ \bar{f}(\epsilon, d)\ d(\hat{g})\ \bar{g}(\epsilon, e)\ e(())\ \bar{c_0}(())\}$

$\{\mathtt{t}, \bar{f}(\epsilon, d)\ d(\hat{g})\ \bar{f}(\epsilon, d)\ d(g)\ \bar{g}(\epsilon, e)\ e(())\ \bar{c_0}(()), \bar{f}(\epsilon, d)\ d(g)\ \bar{f}(\epsilon, d)\ d(\hat{g})\ \bar{\hat{g}}(\epsilon, e)\ e(())\ \bar{c_0}(())\}$

TOWARDS A VPA (INDEXING RECYCLING)



Lemma 41. *Let $c : \sigma^0$ be a continuation name (one which corresponds to returning a value of a basic type). Then, for any O/P-visible, and O/P-bracketed trace $s = t\ f(\overrightarrow{A}, c)\ t'\ \bar{c}(A')\ t''$, no names introduced in $f(\overrightarrow{A}, c)\ t'$ appear in $\mathsf{Vis}_O(s)$ (if s ends in a P-action) or $\mathsf{Vis}_P(s)$ (if s ends in an O-action).*

Lemma 42. *Let $s = t\ f(\overrightarrow{A}, c)\ t'\ \bar{g}(\overrightarrow{A'}, d)$ and $s' = s\ t''\ d(A)$ be PTR $(N_O, \emptyset)$-traces, where g is a level-2 name whose originator is introduced in $\overrightarrow{A}$. Let X be the names introduced in $f(\overrightarrow{A}, c)\ t'\ \bar{g}(\overrightarrow{A'}, d)$. Then if s'' is a proper prefix of s' at least as long as s, $\mathsf{Vis}_O(s'') \cap X = \emptyset$ (if s'' ends in a P-action) and $\mathsf{Vis}_P(s'') \cap X = \emptyset$ (if s'' ends in an O-action).*

Also: recycling for loops (both names and locations)

LTS

$$
\begin{array}{l|lcl}
(P\tau) & \langle M, c, \gamma, \phi, h, H\rangle & \xrightarrow{\tau} & \langle N, c, \gamma, \phi, h', H\rangle \\
 & \text{when } (M,h) \to (N,h') & & \\
(PA) & \langle \text{return } V, c, \gamma, \phi, h, H\rangle & \xrightarrow{\bar{c}(A)} & \langle \gamma\cdot\gamma', \phi \uplus \nu(A), h, H, H(c) \uplus \nu(A)\rangle \\
 & \text{when } c:\sigma,\ (A,\gamma') \in \mathbf{AVal}_{\sigma}(V) & & \\
(PQ) & \langle K[(\text{force } f)\overrightarrow{V}], c, \gamma, \phi, h, H\rangle & \xrightarrow{\bar{f}(\overrightarrow{A}, c')/(c',(K,c))} & \langle \gamma\cdot\gamma', \phi \uplus \phi', h, H, H(f) \uplus \nu(\overrightarrow{A})\rangle \\
 & \text{when } f : U\underline{\tau},\ (\overrightarrow{A},\gamma') \in \mathbf{AVal}(\overrightarrow{V}),\ \sigma = \mathbf{RType}(\underline{\tau}),\ c':\sigma \text{ and } \phi' = \nu(\overrightarrow{A}) \uplus \{c'\} & & \\
(OA) & \langle \gamma, \phi, h, H, Fn\rangle & \xrightarrow{c(A),(c,(K,c'))} & \langle K[\text{return } A], c', \gamma, \phi \uplus \nu(A), h, H \cdot [\nu(A) \mapsto Fn]\rangle \\
 & \text{when } c:\sigma,\ A:\sigma & & \\
(OQ) & \langle \gamma, \phi, h, H, Fn\rangle & \xrightarrow{f(\overrightarrow{A}, c)} & \langle (\text{force } V)\overrightarrow{A}, c, \gamma, \phi \uplus \phi', h, H \cdot [\phi' \mapsto Fn]\rangle \\
 & \text{when } f \in Fn,\ f : U\underline{\tau},\ \overrightarrow{A} \in \mathbf{ASeq}(\underline{\tau}),\ \sigma = \mathbf{RType}(\underline{\tau}),\ c:\sigma,\ \gamma(f) = V \text{ and } \phi' = \nu(\overrightarrow{A}) \uplus \{c\} & &
\end{array}
$$

Given $N \subseteq \text{Names}$, $[N \mapsto \mathcal{V}]$ stands for the map $[n \mapsto \mathcal{V} \,|\, n \in N]$.

$$(P\tau) \quad \langle M, c^j, \gamma, h, H, i_h, \eta, \mu, l\rangle \xrightarrow{\tau} \langle N, c^j, \gamma_{<\eta'}, h', H_{<\eta'}, i'_h, \eta', \mu_{<\eta'}, l\rangle$$

when $(M, h, i_h, \eta) \to_e (N, h', i'_h, \eta')$

$$(PA) \quad \langle \text{return } V, c_0^0, \gamma, h, H, i_h, \eta, \mu, l\rangle \xrightarrow{\bar{c_0}(\beta(A))} \langle \gamma\cdot\gamma', h, H, H(c_0) \uplus \nu(A), i_h, \eta', \mu, l\rangle$$

when $c_0 : \sigma$, $(A, \gamma', \eta') = \mathbf{IVal}^{\Delta}_{\sigma}(c_0, V, \eta)$

$$(PA) \quad \langle \text{return } V, c^i, \gamma, h, H, i_h, \eta, \mu, l\rangle \xrightarrow{\bar{c}(V)} \langle \gamma_{<\eta'}, h_{<i'_h}, H_{<\eta'}, H(c^i), i'_h, \eta', \mu_{<\eta'}, l\rangle$$

when $c \neq c_0$ and $(i'_h, \eta') = \mu(c^i)$

$$(PQ) \quad \langle K[(\text{force } f^i)\overrightarrow{V}], c'^j, \gamma, h, H, i_h, \eta, \mu, l\rangle \xrightarrow{\bar{f}(\beta(\overrightarrow{A}),c)/(c^0,(K,c'^j))} \langle \gamma\cdot\gamma', h, H, H(f^i) \uplus \nu(\overrightarrow{A}), i_h, \eta', \mu, l\rangle$$

when f is not a level 2 name, $(\overrightarrow{A}, \gamma', \eta') \in \mathbf{IVal}^{\Delta}(f, \overrightarrow{V}, \eta)$, and $\mathrm{Succ}_{\mathrm{C}}(f) = c$

$$(PQ) \quad \langle K[(\text{force } f^i)\overrightarrow{V}], c'^j, \gamma, h, H, i_h, \eta, \mu, l\rangle \xrightarrow{\bar{f}(\overrightarrow{V},c)/(c^0,(K,c'^j),P)} \langle \gamma_{<\eta'}, h_{<i'_h}, H_{<\eta'}, H(f^i), i'_h, \eta', \mu_{<\eta'}, l\rangle$$

when f is a level 2 name, and $(i'_h, \eta') = \mu(f^i)$, $\mathrm{Succ}_{\mathrm{C}}(f) = c$, and $P = (i_h, \eta, \gamma_{\geq\eta'}, h_{\geq i'_h}, H_{\geq\eta'}, \mu_{\geq\eta'})$

$$(OA) \quad \langle \gamma, h, H, Fn, i_h, \eta, \mu, l\rangle \xrightarrow{c(\beta(A)),(c^0,(K,c'^j))} \langle K[\text{return } A], c'^j, \gamma, h, H\cdot[\nu(A) \mapsto Fn], i_h, \eta', \mu, l'\rangle$$

when $c : \sigma$, $(A', \eta') \in \mathbf{IVals}^{\Delta}_{\sigma}(c, \eta)$ and if $l = 1$ then $A = A', l' = 1$ else $A \in \mathbf{Select}(A')$, and $l' = \mathbf{IsMark}(A)$

$$(OA) \quad \langle \gamma, h, H, Fn, i_h, \eta, \mu, l\rangle \xrightarrow{c(\beta(A)),(c^0,(K,c'^j),P)} \langle K[\text{return } A], c'^j, \gamma\cdot\gamma', h, H', i'_h, \eta', \mu', l'\rangle$$

when $c : \sigma$, $P = (i'_h, \eta'', \gamma', h', H'', \mu'')$, $(A', \eta') \in \mathbf{IVals}^{\Delta}_{\sigma}(c, \eta'')$ and if $l = 1$ then $A = A', l' = 1$
else $A \in \mathbf{Select}(A')$, and $l' = \mathbf{IsMark}(A)$; and $H' = H\cdot H''\cdot[\nu(A) \mapsto Fn]$, and $\mu' = \mu\cdot\mu''\cdot[\nu(A) \mapsto (i_h, \eta)]$

$$(OQ) \quad \langle \gamma, h, H, Fn, i_h, \eta, \mu, l\rangle \xrightarrow{f(\beta(\overrightarrow{A}),c)} \langle \text{force } V\overrightarrow{A}, c^j, \gamma, h, H\cdot[\nu(\overrightarrow{A}), c^j \mapsto Fn], i_h, \eta', \mu', l\rangle$$

when $f^i \in Fn$, $(\overrightarrow{A'}, \eta'') \in \mathbf{IValSeq}^{\Delta}(f, \eta)$, $\mathrm{Succ}_{\mathrm{C}}(f) = c$, $\eta(c) = j, \eta' = \eta''[c \mapsto j+1], \gamma(f^i) = V$, and
if $l = 1$ then $A = A', l' = 1$ else $A \in \mathbf{Select}(A')$, and $l' = \mathbf{IsMark}(A)$; and $\mu' = \mu\cdot[\nu(\overrightarrow{A}), c^j \mapsto (i_h, \eta)]$

In the PQ rules, the name f can be either marked or unmarked. In the second PA (PQ), V ($\overrightarrow{V}$) does not contain thunks, so is an abstract value. The second OA rule is sound as γ', h', H'', μ'' are disjoint from γ, h, H, μ. $\mathbf{Select}(A)$ is the set of marked indexed abstract values obtained by marking at most one name in A. $\mathbf{IsMark}(A) = 1$ if a name in A is marked, 0 otherwise.

MAIN RESULTS (CBPV)

Lemma 48. *For* PTR*-computation* $\Gamma \vdash^{c} M : F\sigma$ *and* (Γ, σ)*-name scheme* Δ*, one can effectively construct a deterministic VPA accepting* $\mathbf{Tr}^{\Delta}_{\mathrm{PTR}}(\mathsf{C}^{\mathrm{PTR},\Delta}_{M})$*. If* M *is in canonical form, the construction can be carried out in exponential time.*

Theorem 49. *Contextual approximation for the* PTR*-fragment of* CBPV *is decidable. For computations in canonical form, it is decidable in exponential time.*

TOWARDS A DFA

One can show that it is the use of level-2 names that forces us to make use of an unbounded stack. The computations that omit level-2 names are of the form $\Gamma \vdash^c M : F\sigma^1$, where each type in Γ is a σ^2 type according to the grammar given below.

$$\begin{array}{lcl@{\qquad\qquad}lcl}
\sigma^2 & \triangleq & \sigma^1 \mid U\underline{\tau}^1 & \sigma^1 & \triangleq & \sigma^0 \mid \mathrm{Ref} \mid U\underline{\tau}^0 \\
\underline{\tau}^1 & \triangleq & F\sigma^2 \mid \sigma^1 \to \underline{\tau}^1 & \underline{\tau}^0 & \triangleq & F\sigma^0 \mid \sigma^0 \to \underline{\tau}^0 \\
\sigma^0 & \triangleq & \mathrm{Int} \mid \mathrm{Unit} & & &
\end{array}$$

CONCLUSION

- From the CBPV results, one can recover all existing results for Idealized Algol and RML that were based on DFA and DVPA. To this end, it is necessary to show that the translations are fully abstract.

- Arguably, the methodology is more intuitive and accessible than earlier results.

- The results for CBPV are already new, but there is scope for other new results, based on "massaging" the LTS.

- Configurations of the resultant automata contain explicit operational information about run-time behaviour, which makes them suitable for other verification tasks.