

Nagy megbízhatóságú refaktorálás

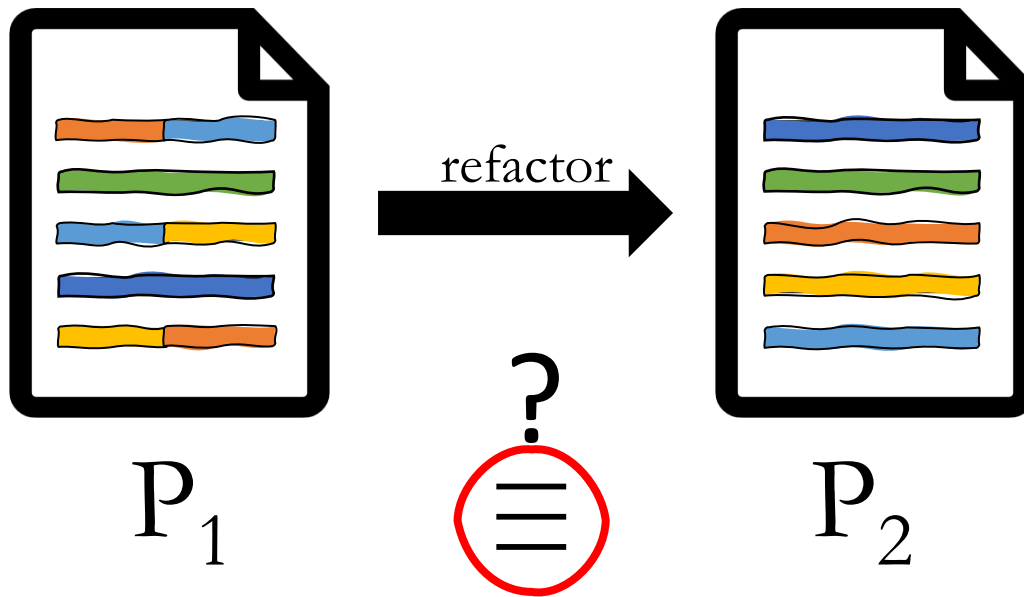
Horpácsi Dániel

Simon Thompson, Bereczky Péter, Mizsei Tamás, Sevella Márton

TKP Workshop,
2021. június 10.

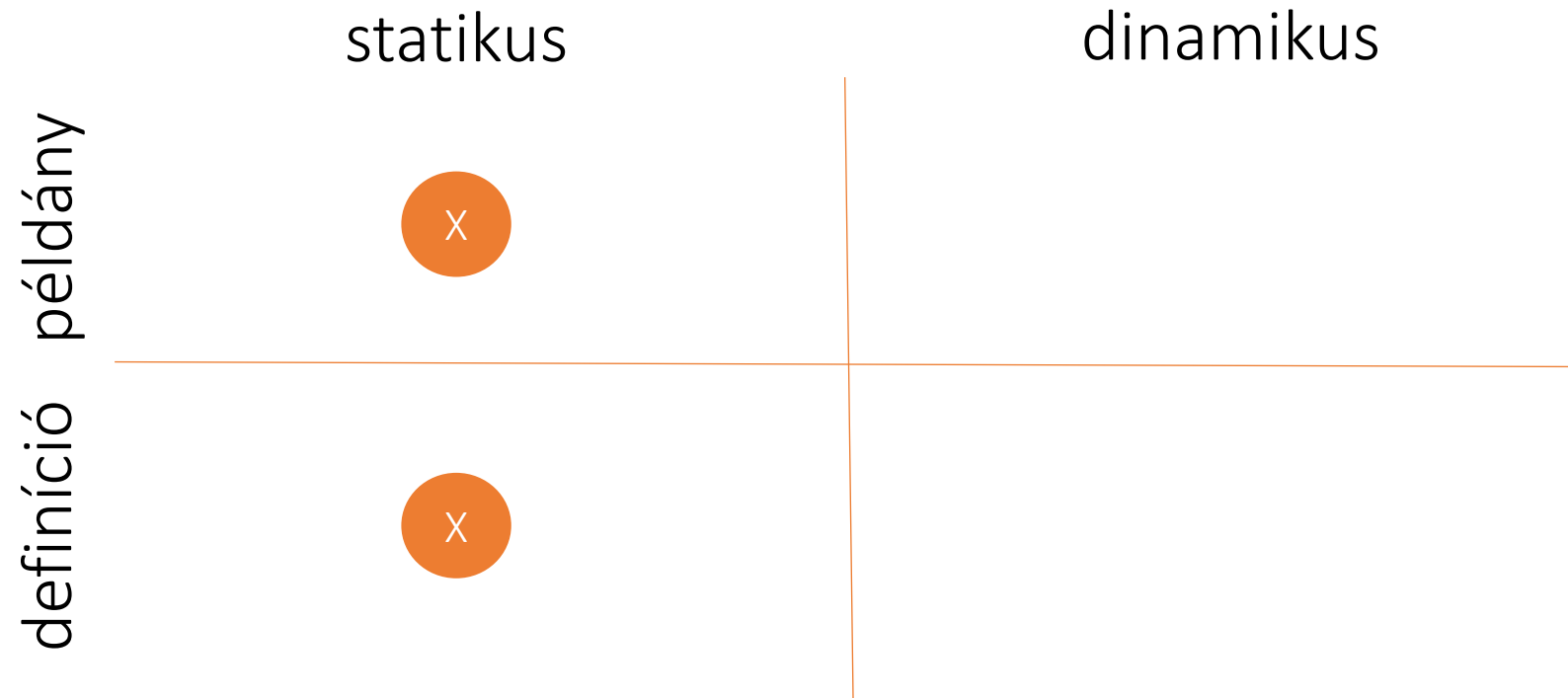


Emlékeztető: refaktorálás



$$\forall P: (P \stackrel{?}{\equiv} \text{refactor}(P))$$

Emlékeztető: refaktorálás verifikációja



Jelenlegi fókusz témák

Core Erlang szemantika és programekvivalencia

Illesztési logika formalizációja, helyessége

Séma alapú transzformációdefiníciók

...

Jelenlegi fókusz témák

Core Erlang szemantika és programekvivalencia

Illesztési logika formalizációja, helyessége

Séma alapú transzformációdefiníciók

Core Erlang szemantika



- Bereczky Péterrel közös munka
- Cél: formális szemantikát adni a (Core) Erlang nyelvhez, amit jól tudunk használni refaktorálás verifikációjához
- Eredmény: „big-step” szemantikák a szekvenciális részhez
 - Gépileg ellenőrizhető bizonyítások (Coq)
 - Hatékony program-kiértékelés (Haskell)
 - Validálva a referenciaimplementáció alapján (QuickCheck)

} programgenerálás és
egyszerűsítés (IFL2020)

Core Erlang szemantika



- Kihívások: típusok hiánya, magasabb rendű függvények, mellékhatások, kivételek, divergencia
- Több különböző stílusú szemantikát is formalizáltunk Coqban: természetes, „pretty big-step”, „functional big-step”

Péter Bereczky, Dániel Horpácsi, Simon Thompson: A Comparison of Big-step Semantics Definition Styles. 2020. Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae, Sectio Computatorica

- Jelenleg még a „frame stack” szemantikát vizsgáljuk (Andrew M. Pitts), amely alkalmasabb lehet környezeti ekvivalencia igazolására és konkurens nyelvi elemek jelentésének megadására

Core Erlang viselkedési ekvivalencia



- Ekvivalenciareláció (reflexív, tranzitív, szimmetrikus), kongruencia
- Tankönyvi definíció

$$e_1 \approx e_2 ::= \forall(\Gamma: Environment)(v: Value): \\ \langle \Gamma, e_1 \rangle \Downarrow v \Leftrightarrow \langle \Gamma, e_2 \rangle \Downarrow v$$

- Kongruens, de:

$e_1 ::= \text{fun}(X) \rightarrow X + 2$

$\text{fun}(X) \rightarrow X + 1 + 1$

Tetszőleges
szintaktikus
környezet (fun)

- Naiv környezeti

$$e_1 \approx_{ctx} e_2 ::= \forall(C: Context)(\Gamma: Environment)(v: Value): \\ \langle \Gamma, C[e_1] \rangle \Downarrow v \Leftrightarrow \langle \Gamma, C[e_2] \rangle \Downarrow v$$

Core Erlang viselkedési ekvivalencia



- Értékegyenlőség helyett értékekvivalencia (logikai reláció)

$$e_1 \approx_{ctx} e_2 ::= \forall (C: Context): C[e_1] \approx_{exp} C[e_2]$$

$$e_1 \approx_{exp} e_2 ::= \forall (\Gamma: Environment)(v_1, v_2: Value): \\ \langle \Gamma, e_1 \rangle \Downarrow v_1 \wedge \langle \Gamma, e_2 \rangle \Downarrow v_2 \Rightarrow v_1 \approx_{val} v_2$$

$$v_1 \approx_{val} v_2 ::= v_1 = v_2 \\ clos(\Gamma, [x_1, \dots, x_n], e_1) \approx_{val} clos(\Gamma', [x_1, \dots, x_n], e_2) ::= \\ \forall v_1, \dots, v_n: (fun(x_1, \dots, x_n) \rightarrow e_1)(v_1, \dots, v_n) \approx_{exp} \\ (fun(x_1, \dots, x_n) \rightarrow e_2)(v_1, \dots, v_n)$$

Kongruencia?

Core Erlang viselkedési ekvivalencia



- Értékekvivalencia rekurzívan
- Terminálási feltétel hozzáadása (divergens kifejezéseknek nincs értéke)

$$\Gamma, e_1 \approx_{exp} \Gamma', e_2 ::= \forall (v_1, v_2: Value):$$

[Coq] Termination?
Strictly positiveness?

$$(\langle \Gamma, e_1 \rangle \Downarrow \wedge \langle \Gamma', e_2 \rangle \Downarrow \wedge v_1 \approx_{val} v_2)$$

$$v_1 \approx_{val} v_2 ::= v_1 = v_2$$
$$clos(\Gamma, [x_1, \dots, x_n], e_1) \approx_{val} clos(\Gamma', [x_1, \dots, x_n], e_2) ::=$$
$$\forall v_1, \dots, v_n, v'_1, \dots, v'_n: v_1 \approx_{val} v'_1 \wedge \dots \wedge v_n \approx_{val} v'_n \Rightarrow$$
$$\Gamma[x_1 \leftarrow v_1, \dots, x_n \leftarrow v_n], e_1 \approx_{exp} \Gamma'[x_1 \leftarrow v'_1 \dots x_n \leftarrow v'_n], e_2$$

Core Erlang szemantika és ekvivalencia



- Jelenlegi munka:
 - $\leq_{exp}^n, \leq_{ciu}$
 - $e_1 \leq_{exp}^n e_2 ::= \forall \Gamma, \Gamma': \Gamma \approx \Gamma' \Rightarrow \langle \Gamma, e_1 \rangle \downarrow^n \Rightarrow \langle \Gamma', e_2 \rangle \downarrow^*$
- Az eredmények általánosan felhasználhatóak
 - Konkrét refaktorálás helyességének igazolására mindazon nyelvekben, amelyek Core Erlangra fordulnak (pl. Erlang, Elixir, LFE, Alpaca)
 - Bizonyos séma-alapú transzformáció definíciók helyességének igazolására



[/harp-project/Core-Erlang-mini](#)

Jelenlegi fókusz témák

Core Erlang szemantika és programekvivalencia

Illesztési logika formalizációja, helyessége

Séma alapú transzformációdefiníciók

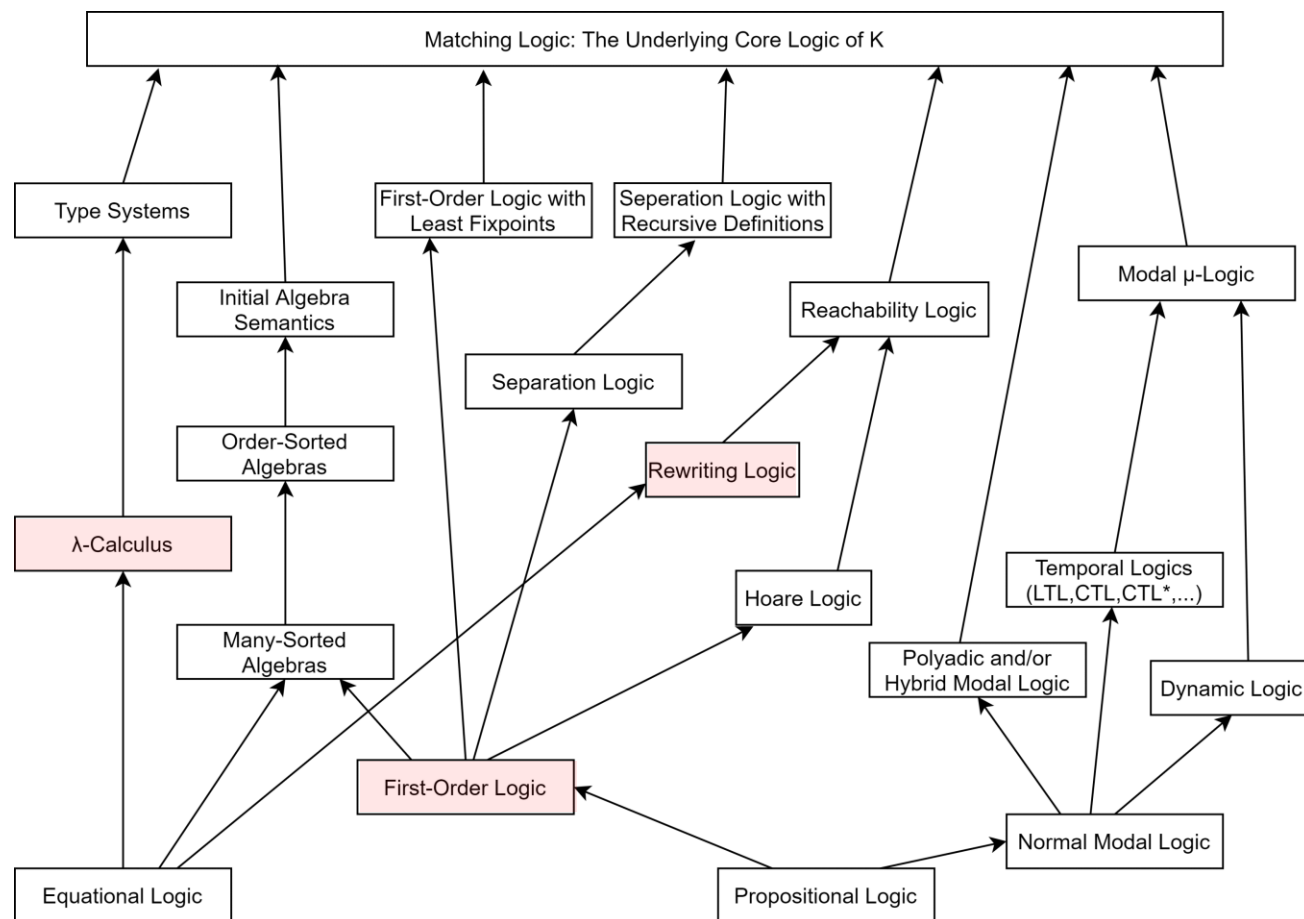
Illesztési logika formalizálása (locally nameless)



- Mizsei Tamással közös munka
- Együttműködés: University of Illinois at Urbana-Champaign
- Cél: érvelés K-ban megadott programozási nyelveken értelmezett transzformációk helyességéről
- Eredmény: logika leírva Coqban locally nameless változóreprezentációval, bizonyítórendszer helyességének igazolása, FOL beágyazása



Illesztési logika



Illesztési logika

- Szintaxis

$\varphi ::= x \mid X \mid \sigma \mid \varphi_1 \varphi_2 \mid \perp \mid \varphi_1 \rightarrow \varphi_2 \mid \exists x. \varphi \mid \mu X. \varphi$

- Szemantika

$\bar{\rho}(x) = \{\rho(x)\}$ for $x \in \text{EVAR}$

$\bar{\rho}(X) = \rho(X)$ for $X \in \text{SVAR}$

$\bar{\rho}(\perp) = \emptyset$

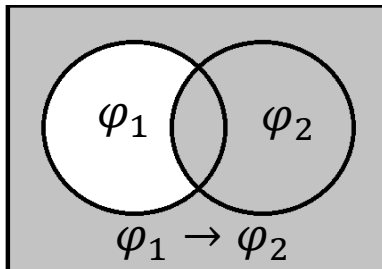
$\bar{\rho}(\sigma) = \sigma_M$ for $\sigma \in \Sigma$

$\bar{\rho}(\varphi_1 \varphi_2) = \bar{\rho}(\varphi_1) \bar{\rho}(\varphi_2)$

$\bar{\rho}(\varphi_1 \rightarrow \varphi_2) = M \setminus (\bar{\rho}(\varphi_1) \setminus \bar{\rho}(\varphi_2))$

$\bar{\rho}(\exists x. \varphi) = \bigcup_{a \in M} \overline{\rho[a/x]}(\varphi)$

$\bar{\rho}(\mu X. \varphi) = \mu \mathcal{F}_{\varphi, X}^{\rho}$ where $\mathcal{F}_{\varphi, X}^{\rho}(A) = \overline{\rho[A/X]}(\varphi)$ for $A \subseteq M$



- Bizonyítórendszer

(Soundness Theorem). $\Gamma \vdash \varphi$ implies $\Gamma \models \varphi$.

FOL
Reasoning

(PROPOSITIONAL TAUTOLOGY)	φ if φ is a propositional tautology over patterns
(MODUS PONENS)	$\frac{\varphi_1 \quad \varphi_1 \rightarrow \varphi_2}{\varphi_2}$
($\exists$ -QUANTIFIER)	$\frac{\varphi[y/x] \rightarrow \exists x. \varphi}{\varphi_1 \rightarrow \varphi_2}$ if $x \notin \text{FV}(\varphi_2)$
	$\frac{\varphi_1 \rightarrow \varphi_2}{(\exists x. \varphi_1) \rightarrow \varphi_2}$

Frame
Reasoning

(PROPAGATION $\vee$)	$\frac{C[\perp] \rightarrow \perp}{C[\varphi_1 \vee \varphi_2] \rightarrow C[\varphi_1] \vee C[\varphi_2]}$
(PROPAGATION $\exists$)	$\frac{C[\exists x. \varphi] \rightarrow \exists x. C[\varphi]}{C[\varphi_1] \rightarrow C[\varphi_2]}$ if $x \notin \text{FV}(C)$
(FRAMING)	$\frac{\varphi_1 \rightarrow \varphi_2}{C[\varphi_1] \rightarrow C[\varphi_2]}$

Fixpoint
Reasoning

(SET VARIABLE SUBSTITUTION)	$\frac{\varphi}{\varphi[\psi/X]}$
(PRE-FIXPOINT)	$\frac{\varphi[\psi/X] \rightarrow \psi}{\varphi[\mu X. \varphi/X] \rightarrow \mu X. \varphi}$
(KNASTER-TARSKI)	$\frac{\varphi[\psi/X] \rightarrow \psi}{\mu X. \varphi \rightarrow \psi}$

Technical
Rules

(EXISTENCE)	$\exists x. x$
(SINGLETON)	$\neg (C_1[x \wedge \varphi] \wedge C_2[x \wedge \neg \varphi])$

Illesztési logika formalizálása

- További eredmény:
 - Elsőrendű logika beágyazása illesztési logikába (meglévő draft alapján)
 - (Conservative) extension tétel igazolása (locally nameless vs. totally nameless)

$$\begin{array}{ccc} \Omega \models_{\text{MSFOL}} \varphi & \xRightarrow{1} & \Gamma^{\text{MSFOL}} \vdash \varphi \\ \uparrow 4 & & \downarrow 2 \\ \Omega \models_{\text{MSFOL}} \varphi & \xleftarrow{3} & \Gamma^{\text{MSFOL}} \models \varphi \end{array}$$

Friss: ELTE-UIUC közös pályázat a formalizáció továbbfejlesztésére, további logikák beágyazására és bizonyítások exportálására

- Fontos következmény:
 - Érvelés illesztési logikai formulákról Coqban
=> Érvelés K-ban leírt programozási nyelvekről Coqban (K-to-Coq)



[/harp-project/AML-Formalization](#)
[/harp-project/FOL-in-ML](#)

Jelenlegi fókusz témák

Core Erlang szemantika és programekvivalencia

Illesztési logika formalizációja, helyessége

Séma alapú transzformációdefiníciók

Séma alapú refaktorálás Wranglerben



- Sevella Mártonnal közös munka
- Cél: sémák implementációja a Wrangler Erlang refaktor eszközben
- Eredmény: függvény transzformációk megvalósítva egy általános függvényátalakítás sémával
 - Függvények átnevezése, paraméterek átrendezése, hozzáadása, törlése stb.
 - Import/export és szignatúra hivatkozások automatikus kezelése
 - Tervezett publikáció a jövő évi CodeBEAM konferencián

Együttműködés, pályázatok



- TKP-n belül
 - Tóth Melinda, adatfolyam-elemzés formális leírása
 - Kaposi Ambrus, típuselméleti kérdések és Coq
- Nemzetközi
 - Simon Thompson / University of Kent (UKC)
 - Grigore Rosu, Xiaohong Chen / University of Illinois at Urbana-Champaign (UIUC)
- Nyertes pályázat (Simon Thompsonnal közösen)
 - Wrangler és ELS, €3000 (Erlang Ecosystem Foundation Stipend)
- Tervezés alatt ipari kutatási pályázat (UIUC-val közösen)
 - Az ML formalizáció alkalmazásai és a 'trust base' redukálása Coq bizonyítások külső ellenőrzésével

Disszemináció 2020-2021

- Publikációk
 - 4 megjelent és további 1 beküldött folyóiratcikk
 - 2 megjelent, 1 elfogadott és további 1 beküldött konferenciacikk
- Előadások
 - 4 konferenciaelőadás, 1 meghívott előadás
- Tehetséggondozás
 - Bevont hallgatók: 1 PhD és 10 MSc/BSc
 - OTDK 2. helyezés (Erlang szemantika) és kari TDK 1. helyezés (Illesztési logika)
- Szoftver



[/harp-project](#)



Köszönöm a figyelmet!



High Assurance Refactoring Project

Horpácsi Dániel
daniel-h@elte.hu

Az Alkalmazásiterület-specifikus nagy megbízhatóságú informatikai megoldások című projekt a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a Tématerületi kiválósági program (TKP2020-NKA-06, Nemzeti Kihívások Alprogram) finanszírozásában valósult meg.



PROGRAM
FINANCED FROM
THE NRDI FUND