Higher-Order Attribute Semantics of Flat Languages

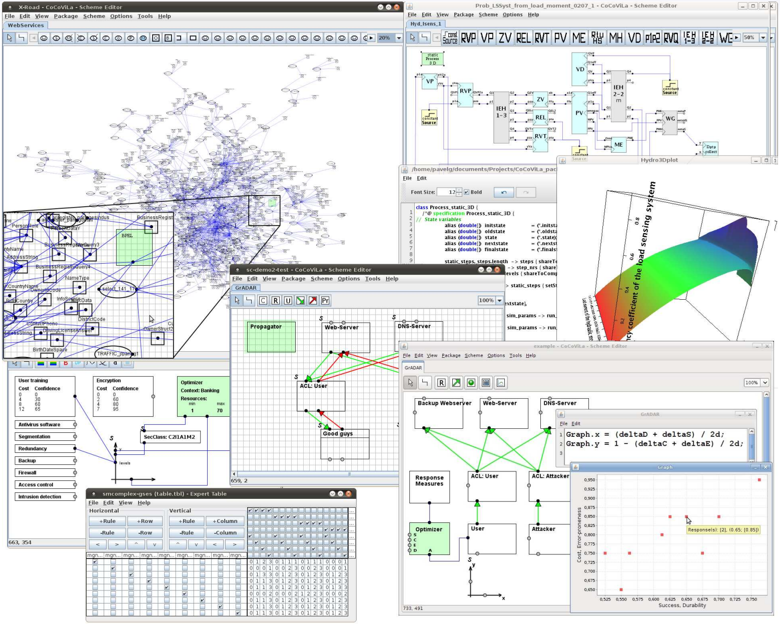
Pavel Grigorenko
Joint work with Enn Tyugu

Institute of Cybernetics, Tallinn University of Technology

Rakari Theory Days

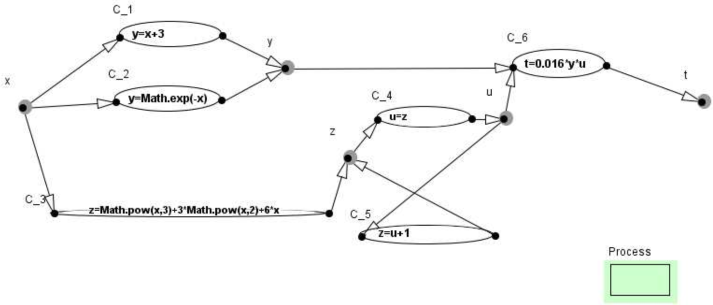
1 October 2010

CoCoViLa


X-Road - CoCoViLa - Scheme Editor
File Edit View Package Scheme Options Tools Help
WebServices
Prob_LSSyst_from_load_moment_0207_1 - CoCoViLa - Scheme Editor
Hyd_lsens_1
VP
RVP
ZV
REL
RVT
PV
ME
VD
IEH 1-3
IEH 2-2 m
WG
Data collect
constant Source
/home/pavelg/documents/Projects/CoCoViLa_pac
Font Size: 12 Bold
class Process_static_3D {
Hydro3Dplot
coefficient of the load sensing system
sc-demo2-test - CoCoViLa - Scheme Editor
GrADAR
Propagator
Web-Server
DNS-Server
ACL: User
Good guys
User training
Encryption
Optimizer
Context: Banking
Resources:
SecClass: C2I1A1M2
Antivirus software
Segmentation
Redundancy
Backup
Firewall
Access control
Intrusion detection
smcomplex-gses (table.tbl) - Expert Table
Horizontal
Vertical
+Rule
+Row
+Column
-Rule
-Row
-Column
example - CoCoViLa - Scheme Editor
Backup Webserver
Response Measures
ACL: Attacker
User
Attacker
Graph.x = (deltaD + deltaS) / 2d;
Graph.y = 1 - (deltaC + deltaE) / 2d;
Graph
Cost, Error-proneness
Success, Durability
Response(s): [2], (0.65; [0.85])

Flat languages

Flat languages are declarative specification languages suitable for defining and composing objects into descriptions of concepts by binding their components by equalities (using *ports*).



(Screenshot from a paper by J. Sanko and J. Penjam)

Flat languages: types, classes

Compound types:

$$a : (t_1, \ldots, t_n;\ a_1 : s_1, \ldots, a_k : s_k),$$

Classes:

$$c : (s, (p_1, \ldots, p_m), \mathfrak{S}),$$

- c – name
- s – type
- $p_1, \ldots, p_m$ – ports
- $\mathfrak{S}$ – local semantics

Flat languages: syntax, semantics

Syntax:

$$\begin{aligned} \textit{Statement} &::= \textit{ObjectDeclaration} \mid \textit{Binding} \\ \textit{ObjectDeclaration} &::= \textit{TypeName ObjectName} \\ \textit{TypeName} &::= \textit{Primitive} \mid \textit{ClassName} \\ \textit{Port} &::= \textit{ObjectName} \mid \textit{ObjectName.ComponentName} \\ \textit{Binding} &::= \textit{Port} = \textit{Port} \end{aligned}$$

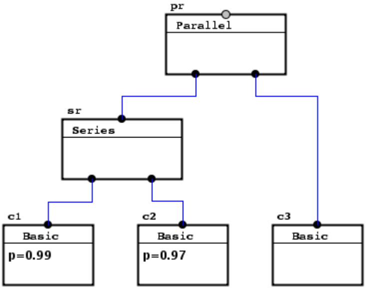
Semantics:

Local semantics $\mathfrak{S}$ + semantics of bindings (unfolding):

a) Primitive types

b) Compound types

Flat languages: computing reliability



Name of type	Supertype	Components	Computations
double			
Basic		*double p* *double q*	$p + q = 1$
Parallel	*Basic*	*Basic part1* *Basic part2*	$q = part1.q * part2.q$
Series	*Basic*	*Basic part1* *Basic part2*	$p = part1.p * part2.p$

Attribute models in a nutshell

- Attributes

$$a^{\sigma} \in A$$

- Attribute dependencies

$$r : x_1, ..., x_m \rightarrow y_1, ..., y_n\{f\},\ r \in R$$

- Computational problems

$$G = U \rightarrow V,\ G \in P$$

- Higher-order attribute dependencies ($s \in P,\ x, y \in A$)

$$r^{ho} : s_1, \ldots, s_k, x_1, \ldots, x_m \rightarrow y_1, \ldots, y_n\{f\},\ r^{ho} \in R^{ho}$$

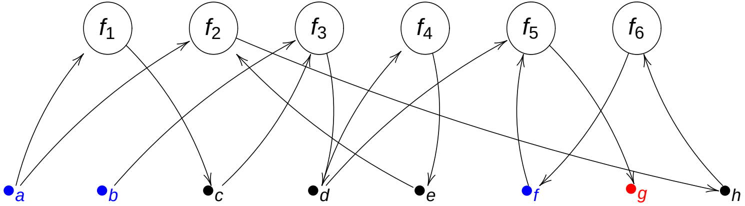
- Attribute model

$$\langle A, R \cup R^{ho} \rangle$$

Attribute evaluation example

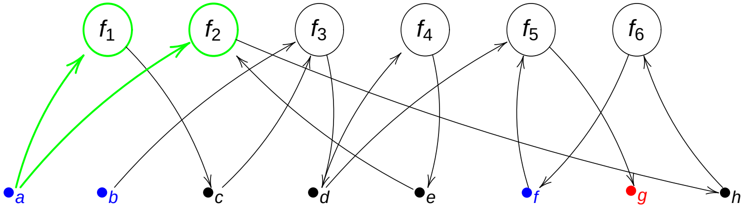
$$
\begin{aligned}
\langle A = \{&a, b, c, d, e, f, g, h\},\\
R = \{&a \to c\{f_1\};\\
&a, e \to h\{f_2\};\\
&b, c \to d\{f_3\};\\
&d \to e\{f_4\};\\
&d, f \to g\{f_5\};\\
&h \to f\{f_6\};\}\rangle
\end{aligned}
$$

Value propagation



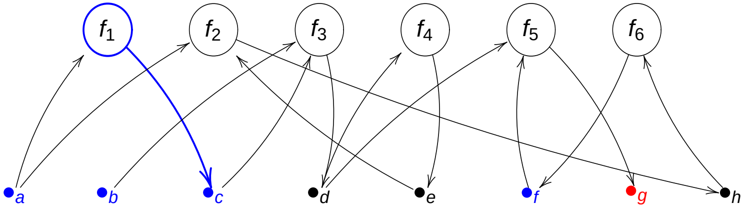
Computational problem $G = U : \{a, b, f\} \rightarrow V : \{g\}$

Value propagation



Computational problem $G = U : \{a, b, f\} \rightarrow V : \{g\}$

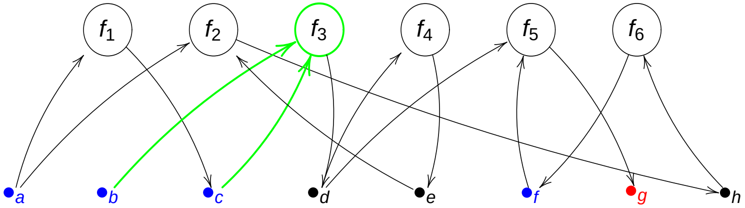
Value propagation



Computational problem $G = U : \{a, b, f\} \rightarrow V : \{g\}$
Algorithm:

$$c = f_1(a);$$

Value propagation

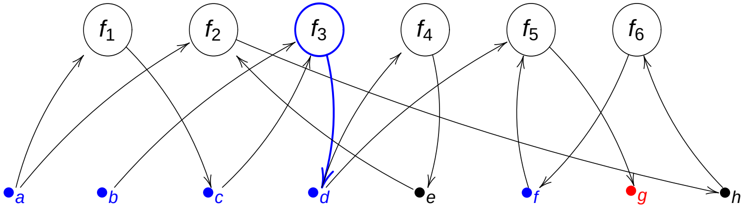


Computational problem $G = U : \{a, b, f\} \rightarrow V : \{g\}$

Algorithm:

$$c = f_1(a);$$

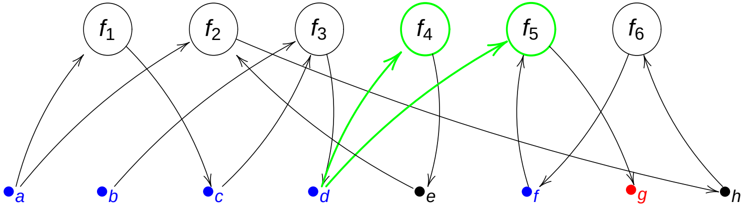
Value propagation



Computational problem $G = U : \{a, b, f\} \to V : \{g\}$
Algorithm:

$$c = f_1(a);$$
$$d = f_3(b, c);$$

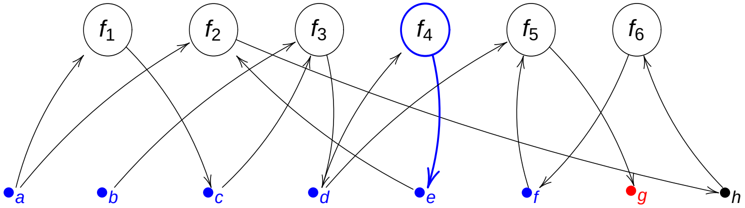
Value propagation



Computational problem $G = U : \{a, b, f\} \rightarrow V : \{g\}$
Algorithm:

$$c = f_1(a);$$
$$d = f_3(b, c);$$

Value propagation

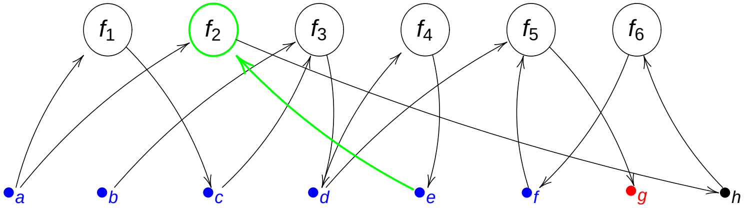


Computational problem $G = U : \{a, b, f\} \rightarrow V : \{g\}$

Algorithm:

$$c = f_1(a);$$
$$d = f_3(b, c);$$
$$e = f_4(d);$$

Value propagation

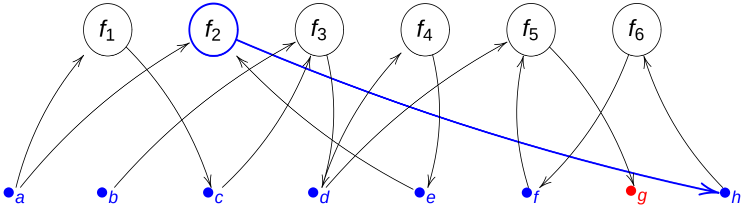


Computational problem $G = U : \{a, b, f\} \rightarrow V : \{g\}$

Algorithm:

$$c = f_1(a);$$
$$d = f_3(b, c);$$
$$e = f_4(d);$$

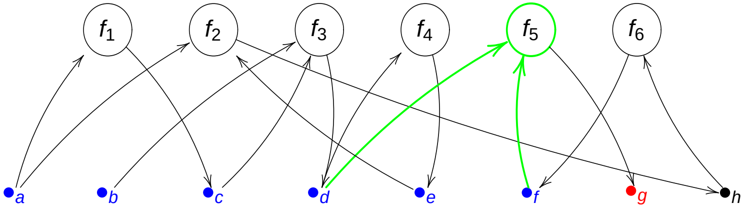
Value propagation



Computational problem $G = U : \{a, b, f\} \rightarrow V : \{g\}$
Algorithm:

$$c = f_1(a);$$
$$d = f_3(b, c);$$
$$e = f_4(d);$$
$$h = f_2(a, e);$$

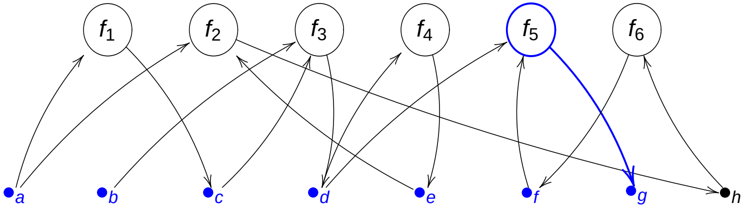
Value propagation



Computational problem $G = U : \{a, b, f\} \rightarrow V : \{g\}$
Algorithm:

$$c = f_1(a);$$
$$d = f_3(b, c);$$
$$e = f_4(d);$$
$$h = f_2(a, e);$$

Value propagation

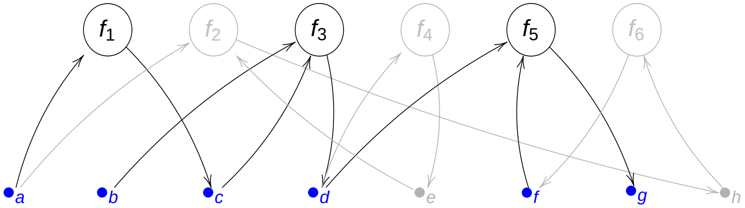


Computational problem $G = U : \{a, b, f\} \rightarrow V : \{g\}$

Algorithm:

$$c = f_1(a);$$
$$d = f_3(b, c);$$
$$e = f_4(d);$$
$$h = f_2(a, e);$$
$$g = f_5(d, f);$$

Optimization



Computational problem $G = U : \{a, b, f\} \rightarrow V : \{g\}$

Algorithm:

$$c = f_1(a);$$
$$d = f_3(b, c);$$
$$e = f_4(d);$$
$$h = f_2(a, e);$$
$$g = f_5(d, f);$$

Higher-order evaluation

Specification:

$$(a, b, f \to g), (a \to h), x \to y\{f_{ho}\}$$

Synthesized program:

$$y = f_{ho}(\lambda abf.f_5(f_3(b, f_1(a)), f),\ \lambda a.f_5(a),\ x)$$

Higher-order evaluation

Specification:

$$(a, b, f \to g), (a \to h), x \to y\{f_{ho}\}$$

Synthesized program:

$$y = f_{ho}(\lambda abf.f_5(f_3(b, f_1(a)), f),\ \lambda a.f_5(a),\ x)$$

Higher-order evaluation (2)

$$[y \to a] \to b$$
$$[a \to b] \to x$$
$$x, y \to a$$

Higher-order evaluation (2)

$S_1 : [y \to a]$

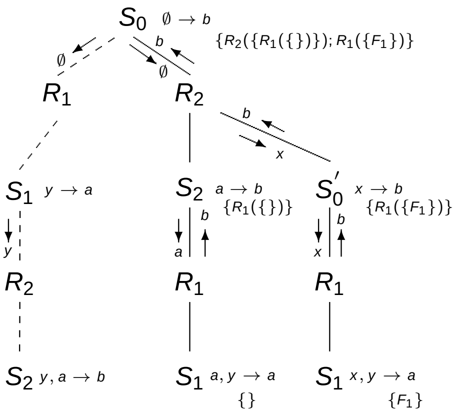
$S_2 : [a \to b]$

$R_1 : S_1 \to b$

$R_2 : S_2 \to x$

$F_1 : x, y \to a$

Solve: $\to b$



Theorem proving

$$((((A \to B) \to A) \to A) \to B) \to B$$

Theorem proving

$$((((A \to B) \to A) \to A) \to B) \vdash B$$

Theorem proving

$$((((A \to B) \to A) \to A) \to B) \vdash B$$

Equivalence replacement:

$$(X \leftrightarrow F) \to (G \leftrightarrow G_F[X])$$

$$\Gamma \vdash G[U \to V] \underset{ded}{=} X \to (U \to V), (U \to V) \to X, \Gamma \vdash G[X]$$

Theorem proving

$$((((A \to B) \to A) \to A) \to B) \vdash B$$

- Replace subformula $(A \to B)$ with X:

$$\begin{aligned} (A \to B) \to X, \\ X \& A \to B, \\ ((X \to A) \to A) \to B \quad \vdash \quad B \end{aligned}$$

Theorem proving

$$((((A \to B) \to A) \to A) \to B) \vdash B$$

- Replace subformula $(A \to B)$ with X:

$$\begin{aligned} (A \to B) &\to X, \\ X \& A &\to B, \\ ((X \to A) \to A) \to B &\vdash B \end{aligned}$$

- Replace $(X \to A)$ with Y:

$$\begin{aligned} (X \to A) &\to Y, \\ Y \& X &\to A, \\ (A \to B) &\to X, \\ X \& A &\to B, \\ (Y \to A) \to B &\vdash B \end{aligned}$$

Theorem proving

$$((((A \to B) \to A) \to A) \to B) \vdash B$$

- Replace subformula $(A \to B)$ with X:

$$\begin{aligned} (A \to B) &\to X, \\ X \& A &\to B, \\ ((X \to A) \to A) \to B &\vdash B \end{aligned}$$

- Replace $(X \to A)$ with Y:

$$\begin{aligned} (X \to A) &\to Y, \\ Y \& X &\to A, \\ (A \to B) &\to X, \\ X \& A &\to B, \\ (Y \to A) \to B &\vdash B \end{aligned}$$

Theorem proving

The sequent:

$$
\begin{aligned}
(Y\&G \to A) \to B, \\
(A \to (B\&G\&Z)) \to X, \\
Y\&X\&U \to A, \\
U, \\
Z \vdash B
\end{aligned}
$$

Proof in GJ' (Mints):

$$\frac{A \vdash A}{A \vdash Y\&G \to A}\ \vdash\to$$

$$\frac{Z \vdash Z \qquad G \vdash G}{Z, G \vdash G\&Z}\ \vdash\&$$

$$\frac{B \vdash B \qquad Z, G \vdash G\&Z}{B, Z, G \vdash B\&G\&Z}\ \vdash\&$$

$$\frac{A \vdash Y\&G \to A \qquad B, Z, G \vdash B\&G\&Z}{(Y\&G \to A) \to B, Z, G, A \vdash B\&G\&Z}\ \to\vdash$$

$$\frac{(Y\&G \to A) \to B, Z, G, A \vdash B\&G\&Z}{(Y\&G \to A) \to B, Z, G \vdash A \to (B\&G\&Z)}\ \vdash\to$$

$$\frac{Y \vdash Y \qquad U \vdash U}{X, Y \vdash X\&Y}\ \vdash\&$$

$$\frac{X \vdash X \qquad X, Y \vdash X\&Y}{U, X, Y \vdash X\&Y\&U}\ \vdash\&$$

$$\frac{U, X, Y \vdash X\&Y\&U \qquad A \vdash A}{X\&Y\&U \to A, U, X, Y \vdash A}\ \to\vdash$$

$$\frac{(Y\&G \to A) \to B, Z, G \vdash A \to (B\&G\&Z) \qquad X\&Y\&U \to A, U, X, Y \vdash A}{(Y\&G \to A) \to B, (A \to (B\&G\&Z)) \to X, X\&Y\&U \to A, U, Z, Y, G \vdash A}\ \to\vdash$$

$$\frac{(Y\&G \to A) \to B, (A \to (B\&G\&Z)) \to X, X\&Y\&U \to A, U, Z, Y, G \vdash A}{(Y\&G \to A) \to B, (A \to (B\&G\&Z)) \to X, X\&Y\&U \to A, U, Z, Y\&G \vdash A}\ \&\vdash$$

$$\frac{(Y\&G \to A) \to B, (A \to (B\&G\&Z)) \to X, X\&Y\&U \to A, U, Z, Y\&G \vdash A}{(Y\&G \to A) \to B, (A \to (B\&G\&Z)) \to X, X\&Y\&U \to A, U, Z \vdash Y\&G \to A}\ \vdash\to$$

$$\frac{(Y\&G \to A) \to B, (A \to (B\&G\&Z)) \to X, X\&Y\&U \to A, U, Z \vdash Y\&G \to A \qquad B \vdash B}{(Y\&G \to A) \to B, (A \to (B\&G\&Z)) \to X, X\&Y\&U \to A, U, Z \vdash B}\ \to\vdash$$

Theorem proving

The sequent:

$$
\begin{aligned}
(Y\&G \to A) \to B,\\
(A \to (B\&G\&Z)) \to X,\\
Y\&X\&U \to A,\\
U,\\
Z \ \vdash B
\end{aligned}
$$

Proof in GJ' (Mints):

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{A \vdash Y\&G \to A}\vdash\to \quad \dfrac{B \vdash B \quad \dfrac{Z \vdash Z \quad G \vdash G}{Z,G \vdash G\&Z}\vdash\&}{B,Z,G \vdash B\&G\&Z}\vdash\&}{(Y\&G \to A) \to B,Z,G,A \vdash B\&G\&Z}\to\vdash}{(Y\&G \to A) \to B,Z,G \vdash A \to (B\&G\&Z)}\vdash\to \quad \dfrac{\dfrac{X \vdash X \quad \dfrac{Y \vdash Y \quad U \vdash U}{X,Y \vdash X\&Y}\vdash\&}{U,X,Y \vdash X\&Y\&U}\vdash\& \quad A \vdash A}{X\&Y\&U \to A,U,X,Y \vdash A}\to\vdash}{(Y\&G \to A) \to B,(A \to (B\&G\&Z)) \to X,X\&Y\&U \to A,U,Z,Y,G \vdash A}\to\vdash}{(Y\&G \to A) \to B,(A \to (B\&G\&Z)) \to X,X\&Y\&U \to A,U,Z,Y\&G \vdash A}\&\vdash}{(Y\&G \to A) \to B,(A \to (B\&G\&Z)) \to X,X\&Y\&U \to A,U,Z \vdash Y\&G \to A}\vdash\to \quad B \vdash B}{(Y\&G \to A) \to B,(A \to (B\&G\&Z)) \to X,X\&Y\&U \to A,U,Z \vdash B}\to\vdash
$$

Theorem proving

$$
\begin{aligned}
(Y_1 \& G_1 \rightarrow A_1) \rightarrow B_1, \\
(A_1 \rightarrow (B_1 \& G_1 \& Z_1)) \rightarrow X_1, \\
Y_1 \& X_1 \& U_1 \rightarrow A_1, \\
Z_1 \leftrightarrow B_2, \\
Y_1 \leftrightarrow U_2, \\
\ldots \\
(Y_n \& G_n \rightarrow A_n) \rightarrow B_n, \\
(A_n \rightarrow (B_n \& G_n \& Z_n)) \rightarrow X_n, \\
Y_n \& X_n \& U_n \rightarrow A_n, \\
Z_{n-1} \leftrightarrow B_n, \\
Y_{n-1} \leftrightarrow U_n, \\
U_1, \\
Z_n \quad \vdash \quad B_1, \\
\text{where } n \geq 2
\end{aligned}
$$

Benchmarking

	n-level sequent							
Tool	1	2	3	4	5	6	7	10
CoCoViLa (IDFS)	<0.01	<0.01	0.02	0.55	18.82	793.6	–	–
CoCoViLa (DFS)	<0.01	<0.01	<0.01	0.05	1.18	36.24	1579.6	–
STRIP (check)	<0.01	<0.01	<0.01	0.34	28.75	3781.3	–	–
STRIP (prove)	<0.01	34.87	–	–	–	–	–	–
iLeanCoP	0.01	–	–	–	–	–	–	–
iLeanSeP	0.02	–	–	–	–	–	–	–
iLeanTAP	–	–	–	–	–	–	–	–
LJT	<0.01	<0.01	0.01	0.05	1.04	35.15	1572.28	–
Gandalf	0.01	0.02	0.08	0.19	0.36	0.53	0.88	7.550
PITP	<0.01	0.01	0.01	0.05	0.68	15.73	343.5	–

Conclusions

- Introduced a concept of *flat languages*
- Represented *semantics* by means of attribute models
- Implemented the approach in CoCoViLa[1]

[1] www.cs.ioc.ee/cocovila