Developing Disciplined Programs

Seminar at Appalachian State University

Clément Aubert

Appalachian State University

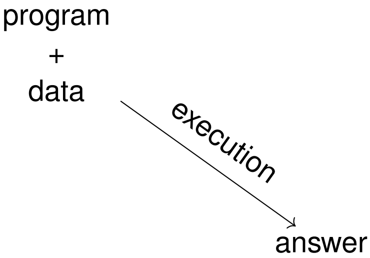
6th February 2017

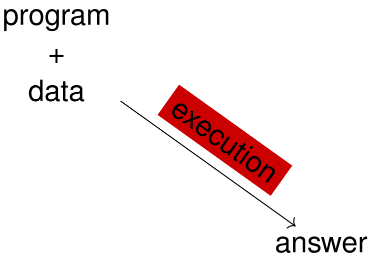
program

program

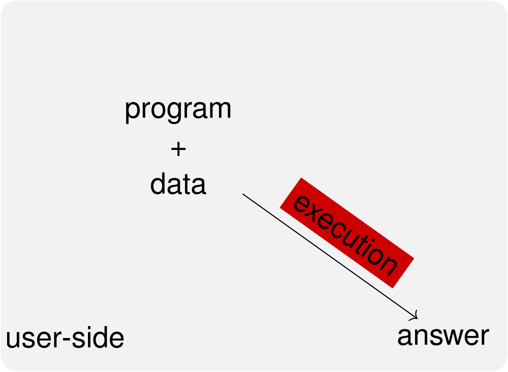
+

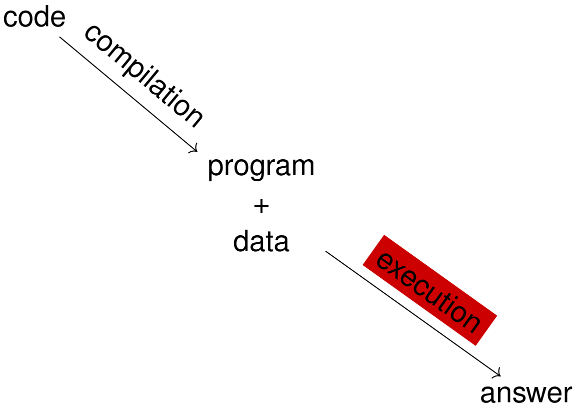
data

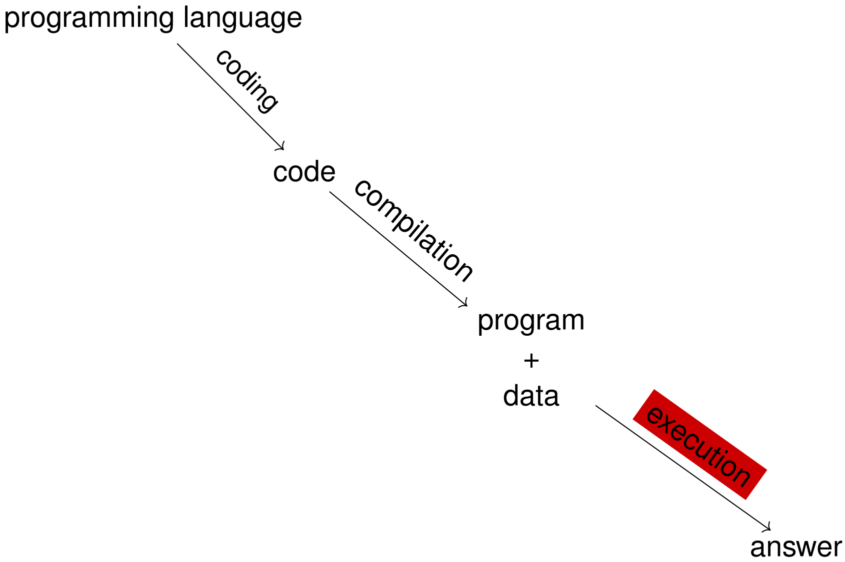

program
+
data
execution
answer

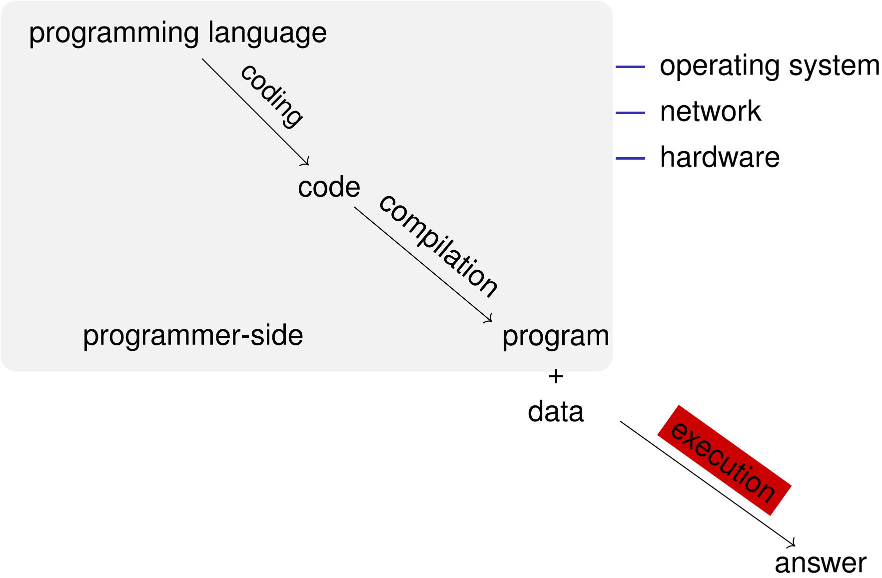

program
+
data
execution
answer

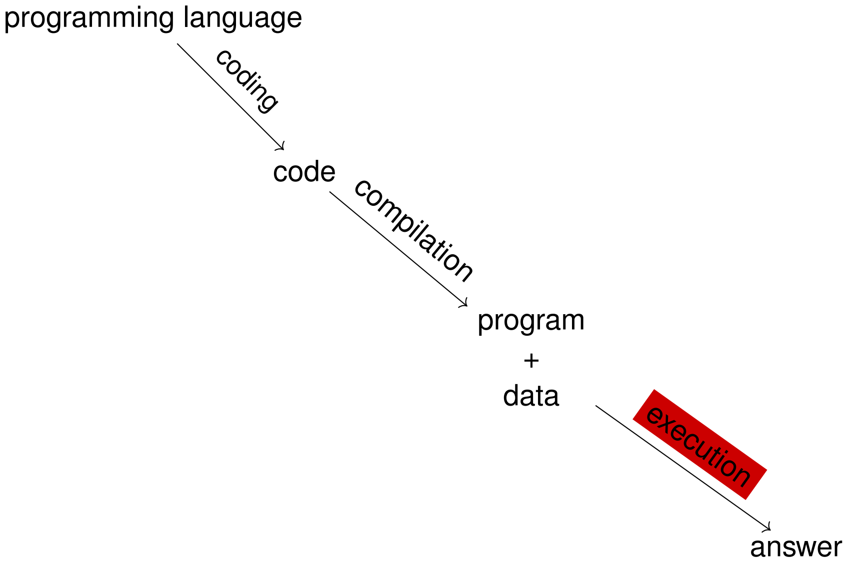
- operating system
- network
- hardware




code
compilation
program
+
data
execution
answer


programming language
coding
code
compilation
program
+
data
execution
answer


programming language
coding
code
compilation
programmer-side
program
+
data
execution
answer
operating system
network
hardware


programming language
coding
code
compilation
program
+
data
execution
answer

Developing Disciplined Programs

Seminar at Appalachian State University

Clément Aubert

Appalachian State University

6th February 2017

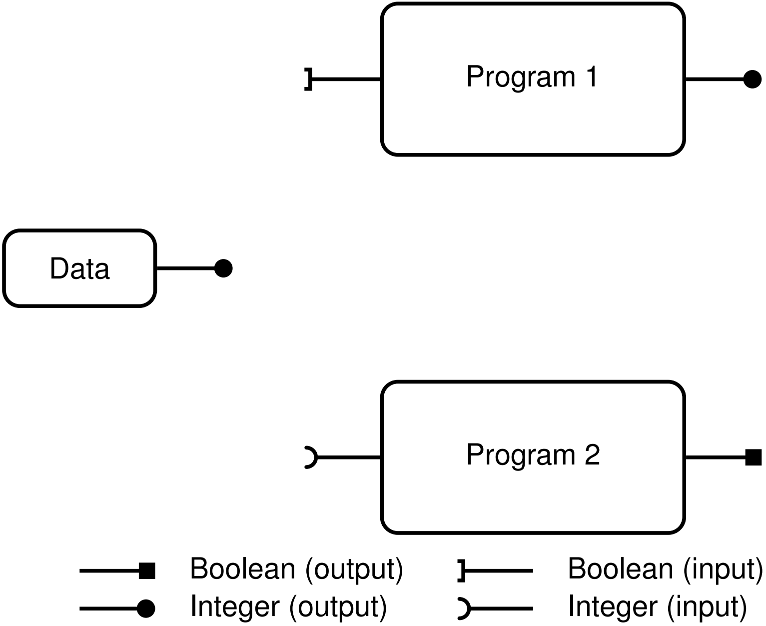
Developing Disciplined *Programing Languages*

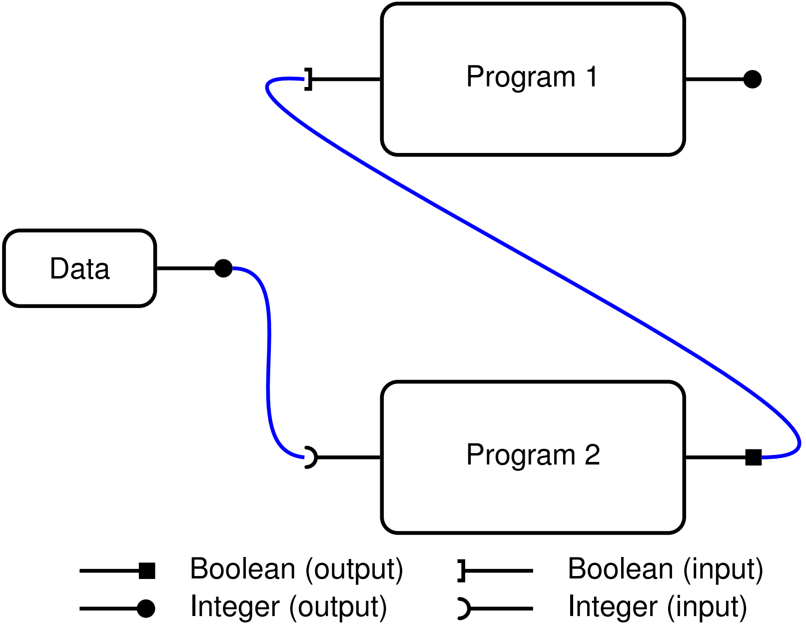
Seminar at Appalachian State University

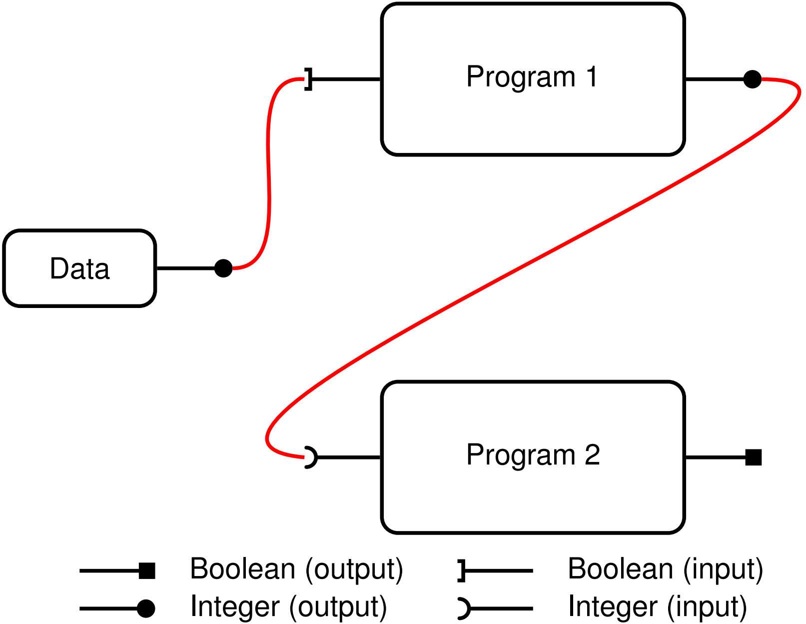
Clément Aubert

Appalachian
STATE UNIVERSITY

6th February 2017


Program 1
Data
Program 2
Boolean (output)
Boolean (input)
Integer (output)
Integer (input)


Program 1
Data
Program 2
Boolean (output)
Integer (output)
Boolean (input)
Integer (input)


Program 1
Data
Program 2
Boolean (output)
Boolean (input)
Integer (output)
Integer (input)

$$\dfrac{\vdash \text{Program 1} : \text{Bool} \to \text{Int} \qquad \dfrac{\vdash \text{Program 2} : \text{Int} \to \text{Bool} \qquad \vdash \text{data} : \text{Int}}{\vdash \text{Program 2 (data)} : \text{Bool}}}{\vdash \text{Program1 (Program 2 (data))} : \text{Int}}$$

$$\frac{\vdash \text{Program 1} : \text{Bool} \to \text{Int} \qquad \dfrac{\vdash \text{Program 2} : \text{Int} \to \text{Bool} \qquad \vdash \text{data} : \text{Int}}{\vdash \text{Program 2 (data)} : \text{Bool}}}{\vdash \text{Program1 (Program 2 (data))} : \text{Int}}$$

$$\rightsquigarrow$$

$$\frac{\vdash \text{Bool} \to \text{Int} \qquad \dfrac{\vdash \text{Int} \to \text{Bool} \qquad \vdash \text{Int}}{\vdash \text{Bool}}}{\vdash \text{Int}}$$

$$\frac{\vdash \text{Program 1} : \text{Bool} \to \text{Int} \qquad \dfrac{\vdash \text{Program 2} : \text{Int} \to \text{Bool} \qquad \vdash \text{data} : \text{Int}}{\vdash \text{Program 2 (data)} : \text{Bool}}}{\vdash \text{Program1 (Program 2 (data))} : \text{Int}}$$

$$\rightsquigarrow$$

$$\frac{\vdash \text{Bool} \to \text{Int} \qquad \dfrac{\vdash \text{Int} \to \text{Bool} \qquad \vdash \text{Int}}{\vdash \text{Bool}}}{\vdash \text{Int}}$$

$$\rightsquigarrow$$

$$\frac{\vdash_x \text{Bool} \to \text{Int} \qquad \dfrac{\vdash_y \text{Int} \to \text{Bool} \qquad \vdash_z \text{Int}}{\vdash_{y+z+c} \text{Bool}}}{\vdash_{y+z+c+x+c'} \text{Int}}$$

Computational Complexity

- Sort problem by their difficulty

Computational Complexity

- Sort problem by their difficulty
- Order of magnitude

Computational Complexity

— Sort problem by their difficulty
— Order of magnitude
— Benchmark: Turing Machine

Computational Complexity

- Sort problem by their difficulty
- Order of magnitude
- Benchmark: Turing Machine

Complete Problems

Logarithmic Space (**L**): Acyclicity in undirected graph
Non-Deterministic Logarithmic Space (**NL**): Acyclicity in directed graph
Polynomial Time (**Ptime**): Circuit value problem

Explicit Computational Complexity

- Sort problem by their difficulty
- Order of magnitude
- Benchmark: Turing Machine

Complete Problems

Logarithmic Space (**L**): Acyclicity in undirected graph
Non-Deterministic Logarithmic Space (**NL**): Acyclicity in directed graph
Polynomial Time (**Ptime**): Circuit value problem

- Machine-dependent
- “External” clock and “external” measure on the tape

> classes. By implicit, we here mean that classes are not given by constraining the amount of resources a *machine* is allowed to use, but rather by imposing linguistic constraints on the way *algorithms* are formulated. This idea has de-

(Dal Lago, 2011, p. 90)(lacl.fr/~caubert/ASU/sm.html)

> classes. By implicit, we here mean that classes are not given by constraining the amount of resources a *machine* is allowed to use, but rather by imposing linguistic constraints on the way *algorithms* are formulated. This idea has de-

(Dal Lago, 2011, p. 90)(lacl.fr/~caubert/ASU/sm.html)

Implicit Computational Complexity (ICC)

— Machine-independent

— Without explicit bounds

> classes. By implicit, we here mean that classes are not given by constraining the amount of resources a *machine* is allowed to use, but rather by imposing linguistic constraints on the way *algorithms* are formulated. This idea has de-

(Dal Lago, 2011, p. 90)(lacl.fr/~caubert/ASU/sm.html)

Implicit Computational Complexity (ICC)

— Machine-independent

— Without explicit bounds

Some Achievements

— Fine-grained type systems for **Ptime**, **L**, **NL**, **Pspace**, etc.

— Differential privacy (Gaboardi et al., 2013)

— Computation over the reals (Férée et al., 2015)

Machine-dependent

Turing machine,
Random access machine,
Counter machine, . . .

Machine-dependent	**Machine-independent**
Turing machine, Random access machine, Counter machine, . . .	Bounded recursion on notation (Cobham, 1965), Bounded linear logic (Girard et al., 1992), Bounded arithmetic (Buss, 1986), . . .

Machine-dependent	**Machine-independent**
Turing machine, Random access machine, Counter machine, . . .	Bounded recursion on notation (Cobham, 1965), Bounded linear logic (Girard et al., 1992), Bounded arithmetic (Buss, 1986), . . .

The rules for storage naturally induce polynomials:

Storage $\dfrac{!_{\vec{y}}\Gamma \vdash A}{!_{x\vec{y}}\Gamma \vdash !_x A}$ *Weakening* $\dfrac{\Gamma \vdash B}{\Gamma, !_0 A \vdash B}$

Contraction $\dfrac{\Gamma, !_x A, !_y A \vdash B}{\Gamma, !_{x+y} A \vdash B}$ *Dereliction* $\dfrac{\Gamma, A \vdash B}{\Gamma, !_1 A \vdash B}$.

(Girard et al., 1992, p. 18)

	Machine-dependent	**Machine-independent**
Explicit bounds	Turing machine, Random access machine, Counter machine, . . .	Bounded recursion on notation (Cobham, 1965), Bounded linear logic (Girard et al., 1992), Bounded arithmetic (Buss, 1986), . . .

	Machine-dependent	**Machine-independent**
Explicit bounds	Turing machine, Random access machine, Counter machine, . . .	Bounded recursion on notation (Cobham, 1965), Bounded linear logic (Girard et al., 1992), Bounded arithmetic (Buss, 1986), . . .
Implicit bounds		Descriptive complexity (Fagin, 1973), Recursion on notation (Bellantoni and Cook, 1992), Tiered recurrence (Leivant, 1993), . . .

	Machine-dependent	**Machine-independent**
Explicit bounds	Turing machine, Random access machine, Counter machine, . . .	Bounded recursion on notation (Cobham, 1965), Bounded linear logic (Girard et al., 1992), Bounded arithmetic (Buss, 1986), . . .
Implicit bounds	Automaton, Auxiliary pushdown machine,. . .	Descriptive complexity (Fagin, 1973), Recursion on notation (Bellantoni and Cook, 1992), Tiered recurrence (Leivant, 1993), . . .

	Machine-dependent	Machine-independent
Explicit bounds	Turing machine, Random access machine, Counter machine, . . .	Bounded recursion on notation (Cobham, 1965), Bounded linear logic (Girard et al., 1992), Bounded arithmetic (Buss, 1986), . . .
ounds	Automaton, Auxiliary pushdown machine,	Descriptive complexity (Fagin, 1973), Recursion on notation (Bellantoni and Cook, 1992),

related to the foregoing question. More specifically, we have attempted to characterize several tape and time complexity classes of Turing machines in terms of devices whose definitions involve only ways in which their infinite memory may be manipulated and no restrictions are imposed on the amount of memory that they use. The basic model

(Ibarra, 1971, p. 88)

$2NFA(k, p)$

— Automata

$2NFA(k, p)$

- Automata
- + Non-Deterministic

$\mathrm{2NFA}(k, p)$

- Automata
- **+** Non-Deterministic
- **+** with $p \geqslant 0$ pushdown stacks

$\mathrm{2NFA}(k, p)$

- Automata
- **+** Non-Deterministic
- **+** with $p \geqslant 0$ pushdown stacks
- **+** 2-ways

2NFA(k, p)

- Automata
- **+** Non-Deterministic
- **+** with $p \geqslant 0$ pushdown stacks
- **+** 2-ways
- **+** with $k \geqslant 1$ heads.

2NFA(k, p)

- Automata
- + Non-Deterministic
- + with $p \geqslant 0$ pushdown stacks
- + 2-ways
- + with $k \geqslant 1$ heads.

Main characterizations

Automata	**Language / Predicate**
2NFA(**1**, **0**)	Regular
2NFA(**1**, **1**)	Context-free
2NFA($*$, **0**)	Non-Deterministic Logarithmic space (**NL**)
2NFA($*$, **1**)	Polynomial time (**Ptime**)
2NFA(**1**, **2**)	Computable

Logic Programming

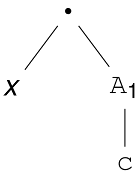
- A programming paradigm
- Computation = unification
- Turing-complete

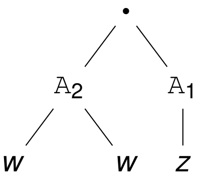
Logic Programming

- A programming paradigm
- Computation = unification
- Turing-complete

Example

$x \bullet \mathtt{A}_1(\mathtt{c})$ $\qquad$ $\mathtt{A}_2(w, w) \bullet \mathtt{A}_1(z)$



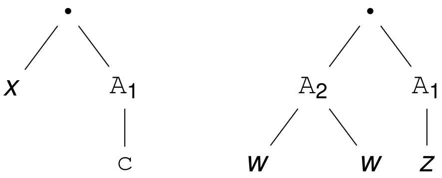


Logic Programming

- A programming paradigm
- Computation = unification
- Turing-complete

Example

$x \bullet \mathtt{A}_1(\mathtt{c})$ $\mathtt{A}_2(w, w) \bullet \mathtt{A}_1(z)$ Unifiable?

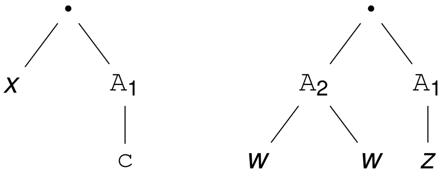


Logic Programming

- A programming paradigm
- Computation = unification
- Turing-complete

Example

$x \bullet \mathtt{A}_1(\mathtt{c})$ $\mathtt{A}_2(w, w) \bullet \mathtt{A}_1(z)$ Unifiable?



✓

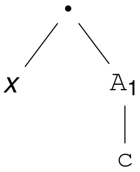
$\theta = [x \leftarrow \mathtt{A}_2(w, w); z \leftarrow c]$

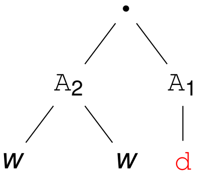
Logic Programming

- A programming paradigm
- Computation = unification
- Turing-complete

Example

$x \bullet \mathtt{A}_1(\mathtt{c})$ $\mathtt{A}_2(w, w) \bullet \mathtt{A}_1(\mathtt{d})$ Unifiable?





$\mathtt{c} \neq \mathtt{d}$

Logic Programming

- A programming paradigm
- Computation = unification
- Turing-complete

Used in . . .

- `Prolog`, `Datalog`
- Type-inference in `Haskell` and `ML`
- Models of Linear Logic (Baillot and Pedicini, 2001; Girard, 2013)

Flows

A *flow* is a pair of terms $t \leftharpoonup u$ with $\mathtt{Var}(t) \subseteq \mathtt{Var}(u)$.

Flows

A *flow* is a pair of terms $t \leftharpoondown u$ with $\texttt{Var}(t) \subseteq \texttt{Var}(u)$.

Balanced

A flow $t \leftharpoondown u$ is *balanced* if for any $x \in \texttt{Var}(t) \cup \texttt{Var}(u)$, all occurrences of x in both t and u have the same height.

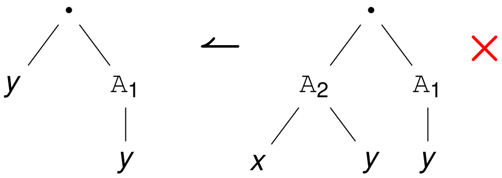
Flows

A *flow* is a pair of terms $t \leftharpoondown u$ with $\mathtt{Var}(t) \subseteq \mathtt{Var}(u)$.

Balanced

A flow $t \leftharpoondown u$ is *balanced* if for any $x \in \mathtt{Var}(t) \cup \mathtt{Var}(u)$, all occurrences of x in both t and u have the same height.

Examples



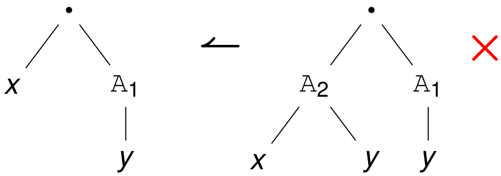
Flows

A *flow* is a pair of terms $t \leftharpoonup u$ with $\mathtt{Var}(t) \subseteq \mathtt{Var}(u)$.

Balanced

A flow $t \leftharpoonup u$ is *balanced* if for any $x \in \mathtt{Var}(t) \cup \mathtt{Var}(u)$, all occurrences of x in both t and u have the same height.

Examples



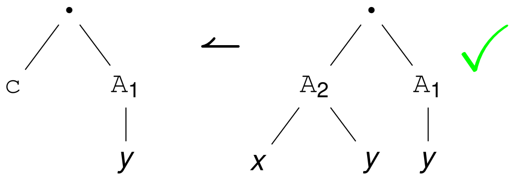
Flows

A *flow* is a pair of terms $t \leftharpoonup u$ with $\mathtt{Var}(t) \subseteq \mathtt{Var}(u)$.

Balanced

A flow $t \leftharpoonup u$ is *balanced* if for any $x \in \mathtt{Var}(t) \cup \mathtt{Var}(u)$, all occurrences of x in both t and u have the same height.

Examples



Flows

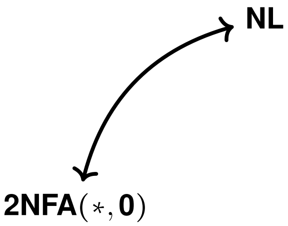
A *flow* is a pair of terms $t \leftharpoondown u$ with $\mathtt{Var}(t) \subseteq \mathtt{Var}(u)$.

Balanced

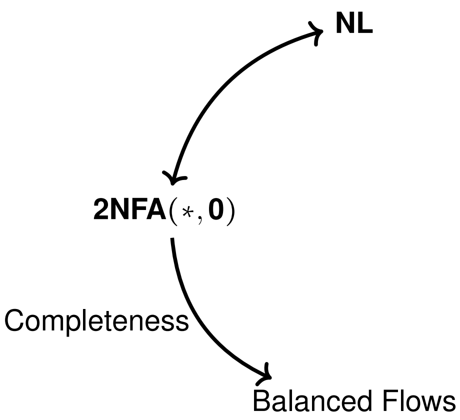
A flow $t \leftharpoondown u$ is *balanced* if for any $x \in \mathtt{Var}(t) \cup \mathtt{Var}(u)$, all occurrences of x in both t and u have the same height.

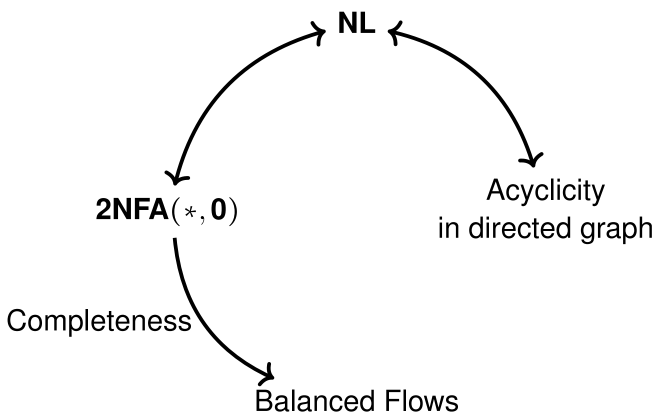
Unary

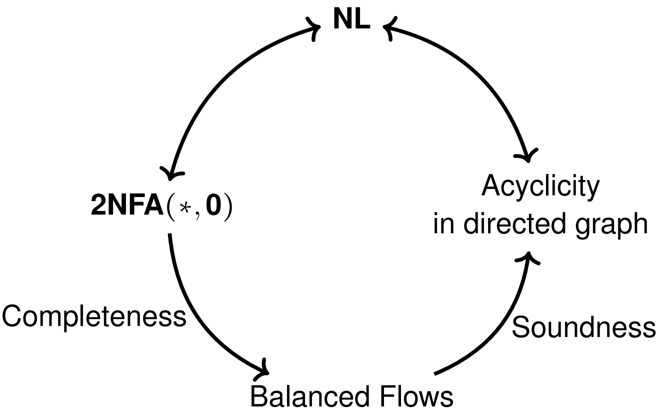
A flow is *unary* if it is built using only unary function symbols and a variable.



Balanced Flows


NL
2NFA$(*, \mathbf{0})$
Completeness
Balanced Flows

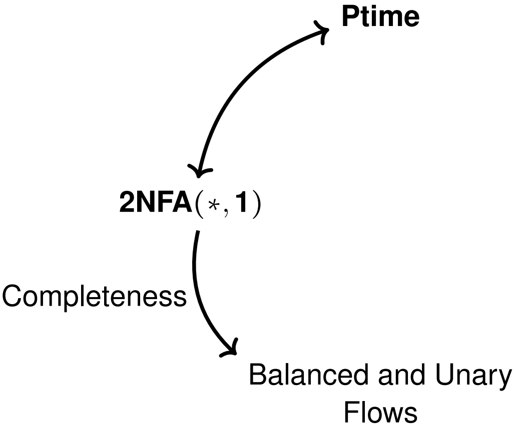

NL
$\mathbf{2NFA}(*, \mathbf{0})$
Acyclicity
in directed graph
Completeness
Balanced Flows

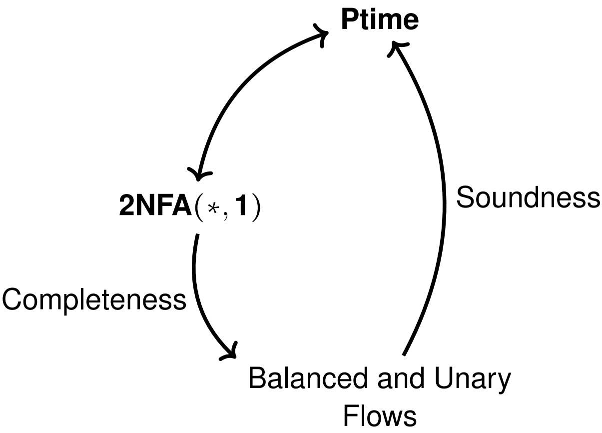

NL
2NFA$(*, \mathbf{0})$
Acyclicity
in directed graph
Completeness
Soundness
Balanced Flows

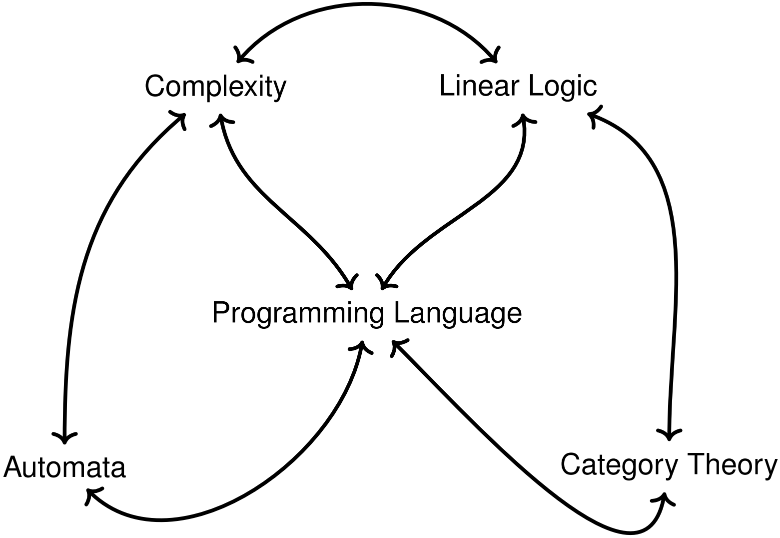
Ptime

2NFA$(*, 1)$

Balanced and Unary
Flows


Ptime
2NFA$(*, 1)$
Completeness
Balanced and Unary Flows


Ptime
2NFA$(*, \mathbf{1})$
Soundness
Completeness
Balanced and Unary Flows


Complexity
Linear Logic
Programming Language
Automata
Category Theory

In increasing order of complexity:

- Write an intepreter for Automata (Chakraborty, Saxena, and Katti, 2011)

In increasing order of complexity:

- Write an intepreter for Automata (Chakraborty, Saxena, and Katti, 2011)
- The odd status of inputs

In increasing order of complexity:

- Write an intepreter for Automata (Chakraborty, Saxena, and Katti, 2011)
- The odd status of inputs
- Knowledge transfers

In increasing order of complexity:

- Write an intepreter for Automata (Chakraborty, Saxena, and Katti, 2011)
- The odd status of inputs
- Knowledge transfers
- Encode other variations of automata

Classroom Presentation lacl.fr/~caubert/ASU/cp.html

Classroom Presentation lacl.fr/~caubert/ASU/cp.html

Reversibility is in embryonic stage:

- Interpreter for reversible automata
- Extending `Janus`' datatypes and datastructures
- Reversible algorithms 101
- Software engineering on research code
- New programming languages

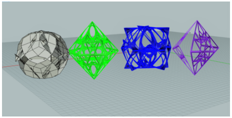
Classroom Presentation lacl.fr/~caubert/ASU/cp.html
Reversibility is in embryonic stage:

- Interpreter for reversible automata
- Extending `Janus`' datatypes and datastructures
- Reversible algorithms 101
- Software engineering on research code
- New programming languages

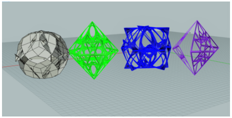
Benefits:

- Re-usable skills
- Small community = strong (international) impact
- So much to be done!

- Alisha Sprinkle + Richard Elaver (Assistant Professor of Industrial Design) =

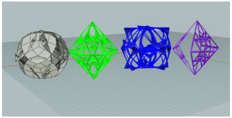


- Alisha Sprinkle + Richard Elaver (Assistant Professor of Industrial Design) =



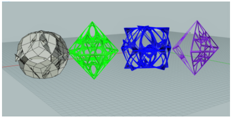
- ? + Richard Elaver = `Python` to design

- Alisha Sprinkle + Richard Elaver (Assistant Professor of Industrial Design) =



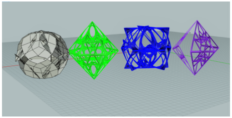
- ? + Richard Elaver = `Python` to design
- ? + Mark Nystrom (Associate Professor in the Art department) = Artistic Coding!

- Alisha Sprinkle + Richard Elaver (Assistant Professor of Industrial Design) =



- ? + Richard Elaver = `Python` to design
- ? + Mark Nystrom (Associate Professor in the Art department) = Artistic Coding!
- ? + ? = Web design

- Alisha Sprinkle + Richard Elaver (Assistant Professor of Industrial Design) =



- ? + Richard Elaver = `Python` to design
- ? + Mark Nystrom (Associate Professor in the Art department) = Artistic Coding!
- ? + ? = Web design

Thanks!

- Baillot, Patrick and Marco Pedicini (2001). "Elementary Complexity and Geometry of Interaction". In: *Fund. Inform.* 45.1–2, pp. 1–31.
- Bellantoni, Stephen J. and Stephen Arthur Cook (1992). "A New Recursion-Theoretic Characterization of the Polytime Functions (Extended Abstract)". In: *STOC*. Ed. by S. Rao Kosaraju, Mike Fellows, Avi Wigderson, and John A. Ellis. ACM, pp. 283–93.
- Buss, Samuel R. (1986). *Bounded Arithmetic*. Vol. 3. Studies in Proof Theory. Lecture Notes. Bibliopolis.
- Chakraborty, Pinaki, Prem Chandra Saxena, and Chittaranjan Padmanabha Katti (2011). "Fifty years of automata simulation: a review". In: *Inroads* 2.4, pp. 59–70.

- Cobham, Alan (1965). “The intrinsic computational difficulty of functions”. In: *Logic, methodology and philosophy of science: Proceedings of the 1964 international congress held at the Hebrew university of Jerusalem, Israel, from August 26 to September 2, 1964*. Ed. by Yehoshua Bar-Hillel. Studies in Logic and the foundations of mathematics. North-Holland Publishing Company, pp. 24–30.
- Dal Lago, Ugo (2011). “A Short Introduction to Implicit Computational Complexity”. In: *ESSLLI*. Ed. by Nick Bezhanishvili and Valentin Goranko. Vol. 7388. LNCS. Springer, pp. 89–109.
- Fagin, Ronald (1973). “Contributions to the Model Theory of Finite Structures”. PhD thesis. University of California, Berkeley.

- Férée, Hugo, Emmanuel Hainry, Mathieu Hoyrup, and Romain Péchoux (2015). "Characterizing polynomial time complexity of stream programs using interpretations". In: *Theoret. Comput. Sci.* 585, pp. 41–54.
- Gaboardi, Marco, Andreas Haeberlen, Justin Hsu, Arjun Narayan, and Benjamin C. Pierce (2013). "Linear dependent types for differential privacy". In: *POPL*. Ed. by Roberto Giacobazzi and Radhia Cousot. ACM, pp. 357–370.
- Girard, Jean-Yves (2013). "Three lightings of logic". In: *CSL*. Ed. by Simona Ronchi Della Rocca. Vol. 23. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, pp. 11–23.
- Girard, Jean-Yves, Andre Scedrov, and Philip J. Scott (1992). "Bounded linear logic: a modular approach to polynomial-time computability". In: *Theoret. Comput. Sci.* 97.1, pp. 1–66.

Ibarra, Oscar H. (1971). “Characterizations of Some Tape and Time Complexity Classes of Turing Machines in Terms of Multihead and Auxiliary Stack Automata”. In: *J. Comput. Syst. Sci.* 5.2, pp. 88–117.

Leivant, Daniel (1993). “Stratified Functional Programs and Computational Complexity”. In: *POPL*. Ed. by Mary S. Van Deusen and Bernard Lang. ACM Press, pp. 325–333.