Declaration of Independence (1776)

Declaration of the Rights of Man and of the Citizen (1789)


1977

The Declaration of Abstract Interpretation of CC77

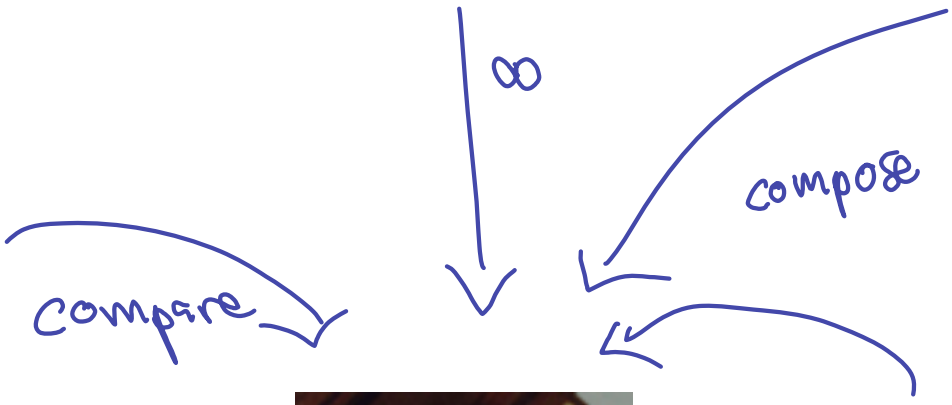
A statement of principles of program analysis:

- compare interpretations
- compose interpretations
- celebrate infinity

A. Turing

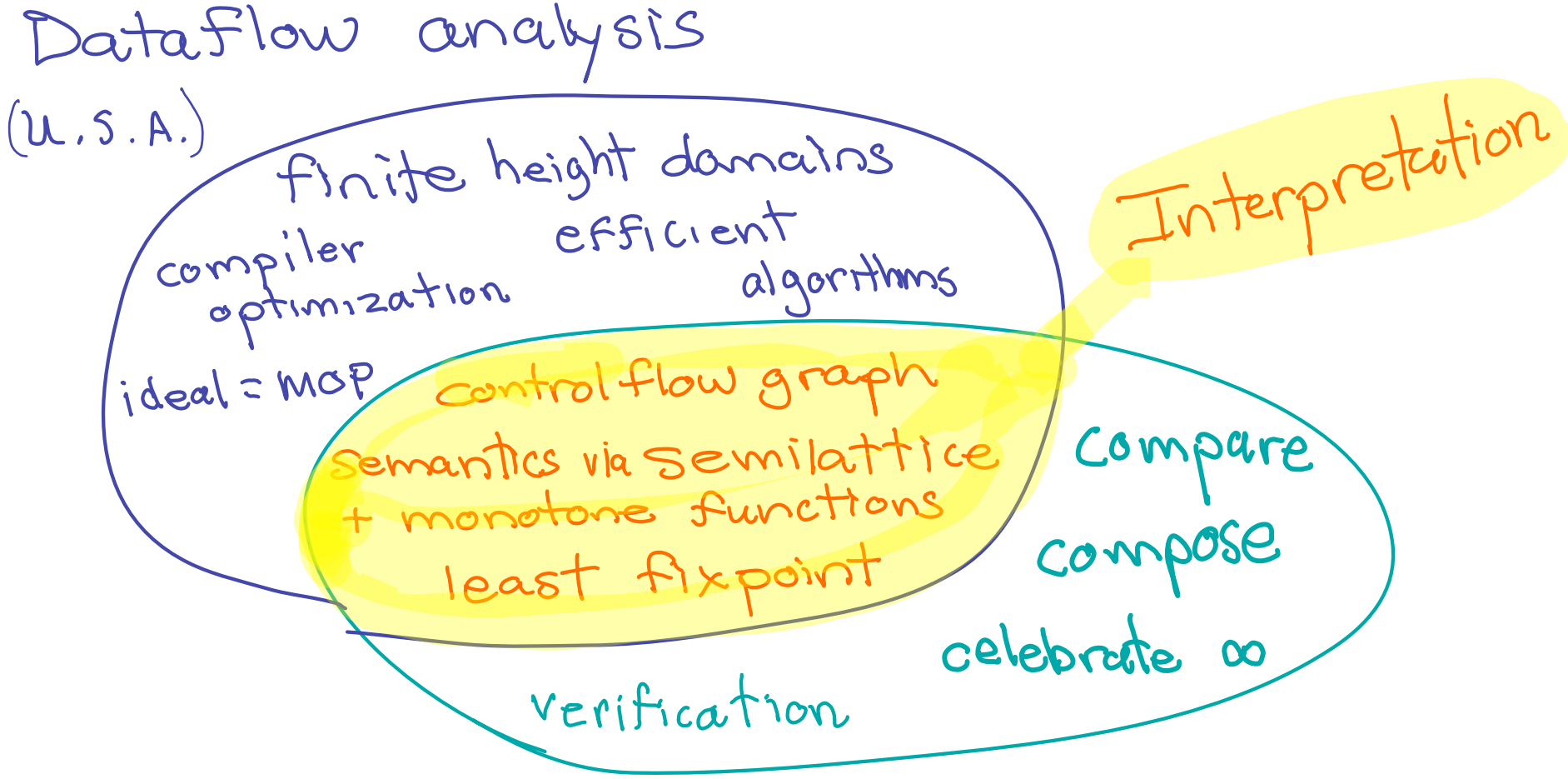
Alfred Tarski (1902-1983)

E. Galois



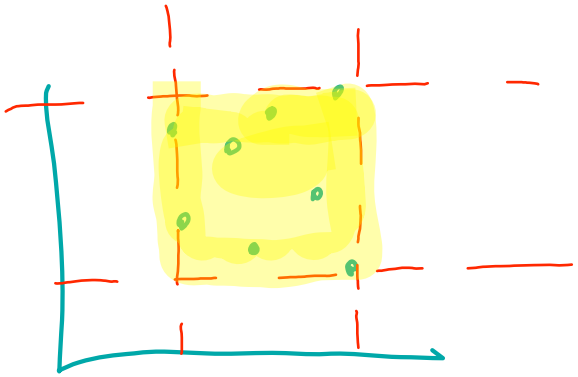
D. Scott

All in the Family (1977)



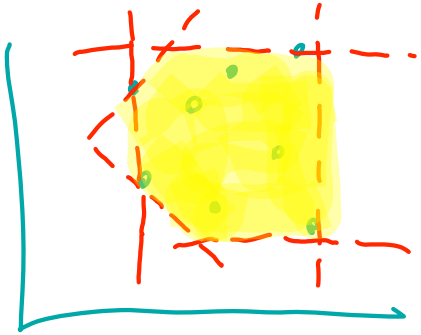
Compare

integer sets



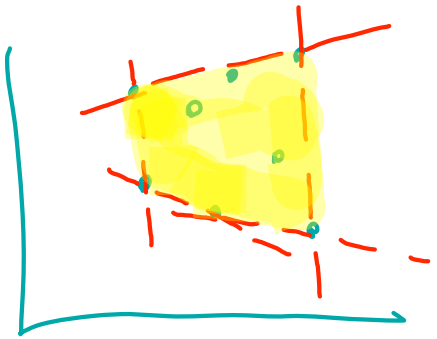
intervals

$c \leq x < d$



octagon

$\pm x \pm y \leq c$



polyhedra

$a_1 x_1 + \dots a_n y_n \leq c$

Diplomacy

webster.2: skill in handling affairs without arousing hostility

Frenchman Charles Maurice de Talleyrand is considered one of the most skilled diplomats of all time

Diplomacy

webster.2: skill in handling affairs without arousing hostility

Frenchman Patrick Cousot
may not be one of the
most skilled diplomats of all time

Patrick's Theme, Take 1

Anything You Can Do, I Can Do Better
Irving Berlin

Anything you can do, I can do better
I can do any thing better than you
No you can't, Yes I can, No you can't, Yes I can
No you can't, Yes I can, yes I can

Patrick's Theme, Take 2

Anything You Can Do, I Can Do Better

Specify

Irving Berlin

Anything you can do, I can specify better
I can specify any thing better than you
No you can't, Yes I can, No you can't, Yes I can
No you can't, Yes I can, yes I can

Compose

Andreas Podelski:

"What abstraction does SLAM compute?"

Sriram & Tom:

"Uh... we implemented c2bp and proved it sound."

Apply Ideal

$P = \{x > 5, x < 5, y = 5\}$ $\quad x := y$

$$\gamma_{bool}(\{\langle 0,0,0\rangle\}) = \{s \mid s \models x = 5 \wedge y \neq 5\}$$

$\downarrow x := y$

$$\alpha_{bool}(\{s \mid s \models x = y \wedge y \neq 5\})$$

$$= \{\langle 1,0,0\rangle, \langle 0,1,0\rangle\}$$

Apply SLAM

S: $x := y$

S_{BP}: $\{x<5\}, \{x>5\}, \{y=5\} := *, *, \{y=5\}$;

$\{\langle 0,0,0\rangle\}$

$\downarrow S_{BP}$

$\{\langle 0\ 0\ 0\rangle,$
$\langle 0\ 1\ 0\rangle,$
$\langle 1\ 0\ 0\rangle,$
$\langle 1\ 1\ 0\rangle\}$

Cartesian Abstraction

Approximate a set of tuples by a tuple of sets

$$\alpha_{cart}(\{\langle 1,0,0\rangle, \langle 0,1,0\rangle\}) = \langle *, *, 0\rangle$$

$$\gamma_{cart}(\langle *, *, 0\rangle) = \{\langle 0,0,0\rangle, \langle 0,1,0\rangle, \langle 1,0,0\rangle, \langle 1,1,0\rangle\}$$

SLAM Abstraction

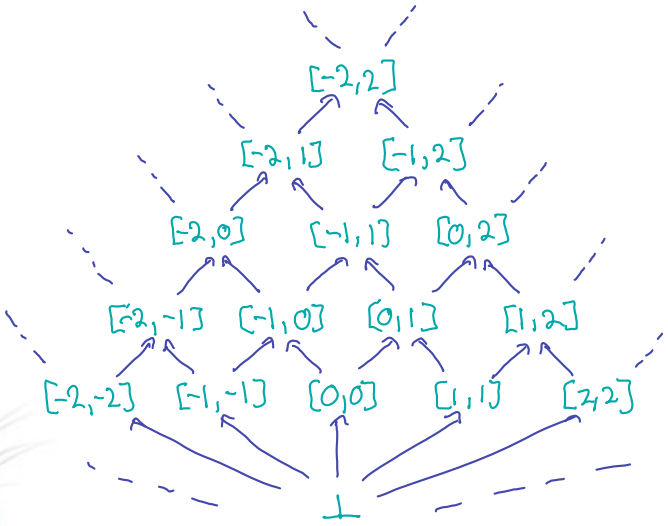
Not

$$\alpha_{bool} \circ SP \circ \gamma_{bool}$$

Rather

$$\alpha_{cart} \circ \alpha_{bool} \circ SP \circ \gamma_{bool} \circ \gamma_{cart}$$

Celebrate ∞!



A recipe for tasty abstractions!

Cousot, Halbwachs (1978)

Discovering liner equalities

- Wegbreit '75, Karr '76
- required finite ascending chains

Discovering linear inequalities, CH78

- convex polyhedra
- infinite ascending chains

$(X=1)\ (1 \leq X \leq 2)\ \ldots\ (1 \leq X \leq n)\ \ldots$

- widening, narrowing

Impact

Theory (precision, fixpoint with ∞ domains)

CC77, ...

Algorithms, Data structures

CH78, ...

Application

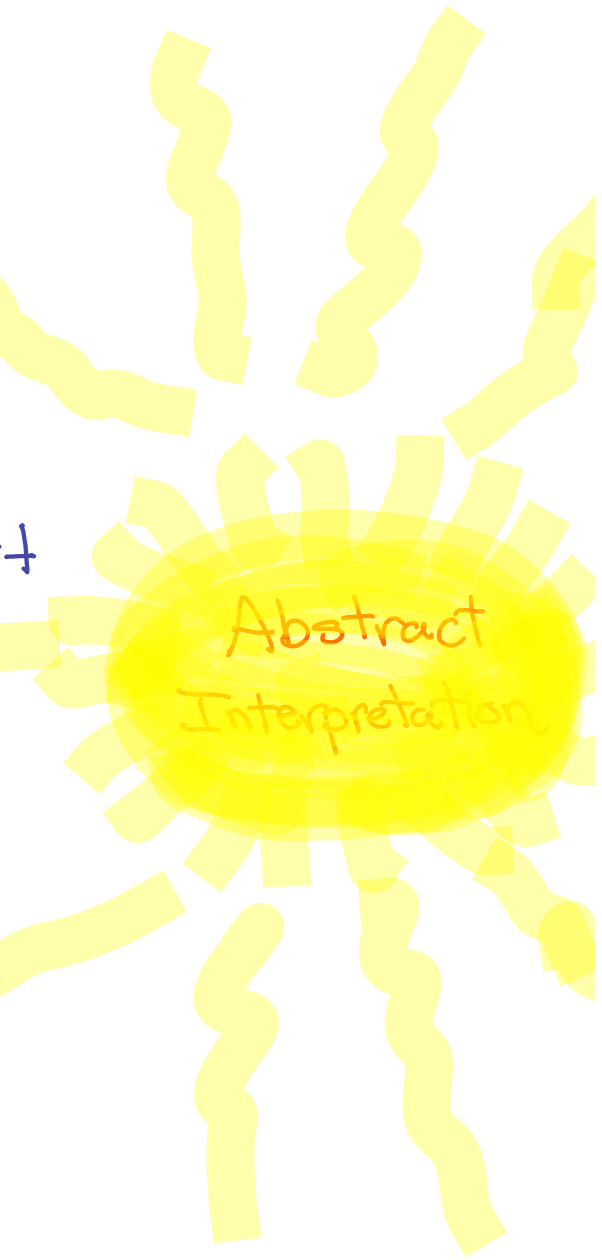
..., ASTREE, ...

Software Tools from Microsoft (2007)

- Windows device drivers
  - Static Driver Verifier (SLAM)
  - part of Windows Vista DDK
- Buffer overflow checking for C/C++
  - SAL + ESPx
  - 1000s of defects fixed
- .NET (managed) code
  - Clousot checker

Software Tools from Microsoft (2007)

- Windows device drivers
  - Static Driver Verifier (SLAM)
  - part of Windows Vista DDK
- Buffer overflow checking for C/C++
  - SAL + ESPx
  - 1000s of defects fixed
- .NET (managed) code
  - Clousot checker




Abstract
Interpretation