Iterative Program Analysis

Mooly Sagiv
http://www.cs.tau.ac.il/~msagiv/courses/pa16.html
Tel Aviv University
640-6706

Textbook: Principles of Program Analysis

Chapter 2.1 (modified)

Subjects

- From programs to equations
- Examples of chaotic iterations
- Why can’t we stop early?
- Why can’t we start from top?
- Incompleteness
- Efficiency issues

Computing Constants

- Construct a control flow graph (CFG)
- Associate transfer functions with control flow graph edges
- Define a system of equations
- Compute the simultaneous least fixed point via Chaotic iterations
- The solution is unique
  - But order of evaluation may affect the number of iterations

A Simple Example

$[z := 3]^1$

$[x := 1]^2$

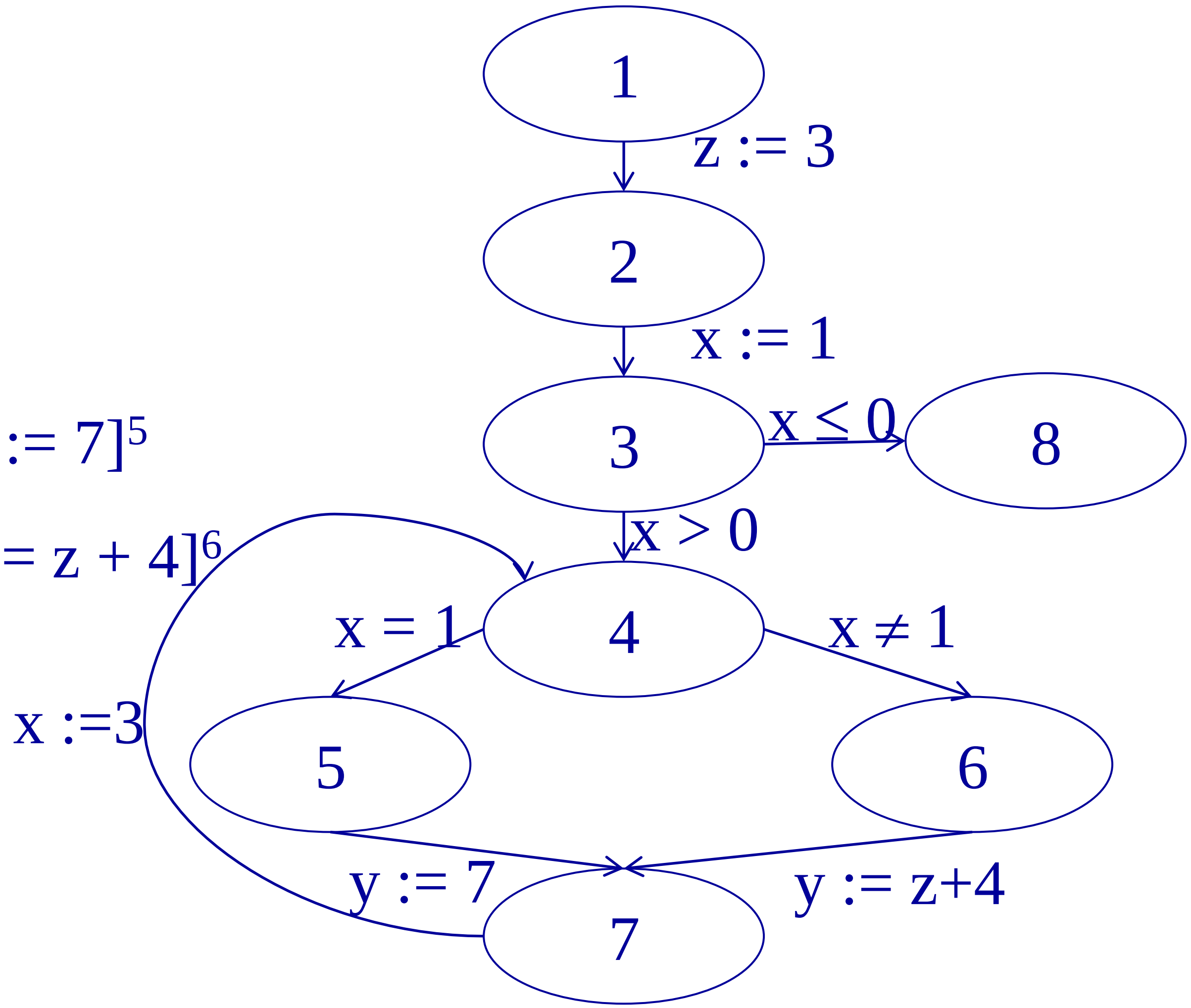
while ($[x > 0]^3$) (

 if $[x = 1]^4$ then $[y := 7]^5$

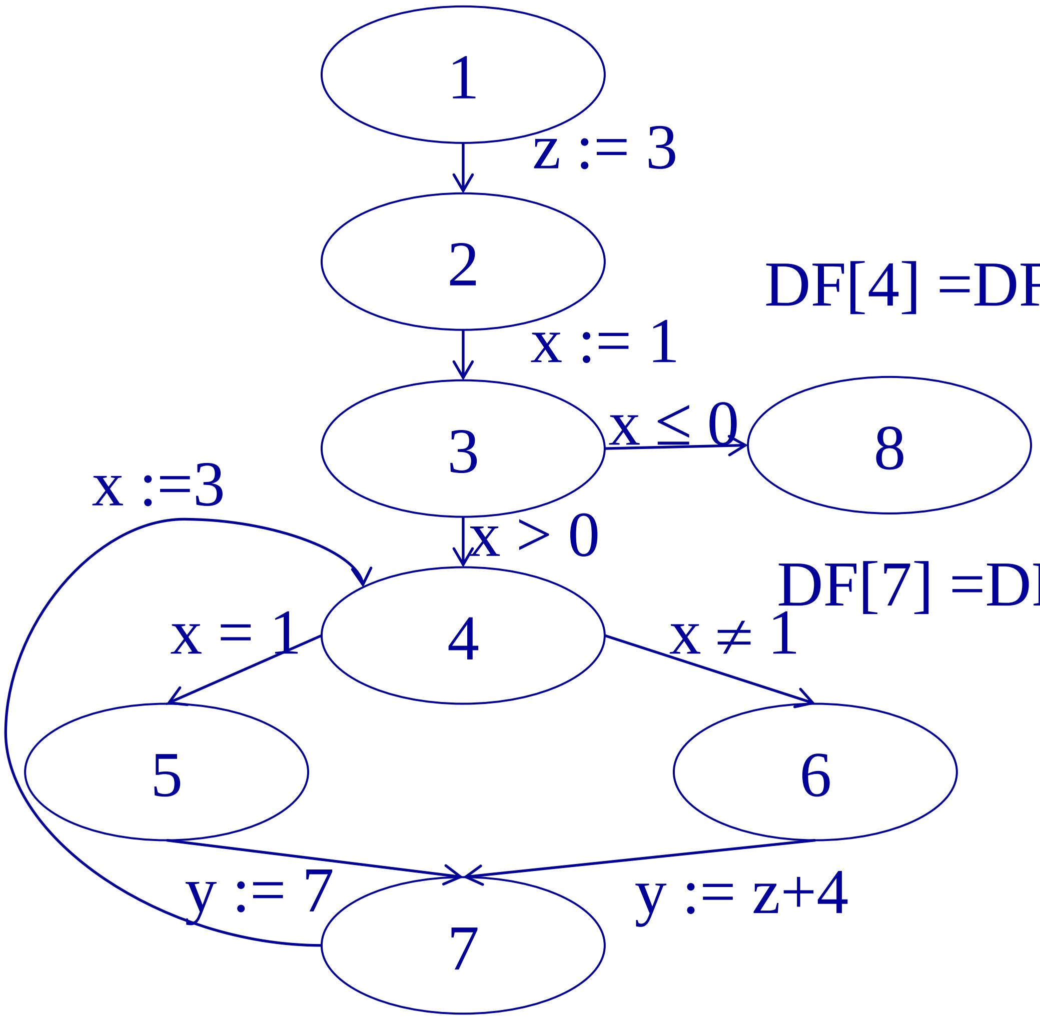
 else $[y := z + 4]^6$

 $[x := 3]^7$

)



A Simple Example: System of Equations



$DF[1] = [x \mapsto 0, z \mapsto 0]$

$DF[2] = DF[1] [\![z \mapsto 3]\!]^{\#}$

$DF[3] = DF[2] [\![x \mapsto 1]\!]^{\#}$

$DF[4] = DF[3] [\![x > 0]\!]^{\#} \sqcup DF[7] [\![y := 7]\!]^{\#}$

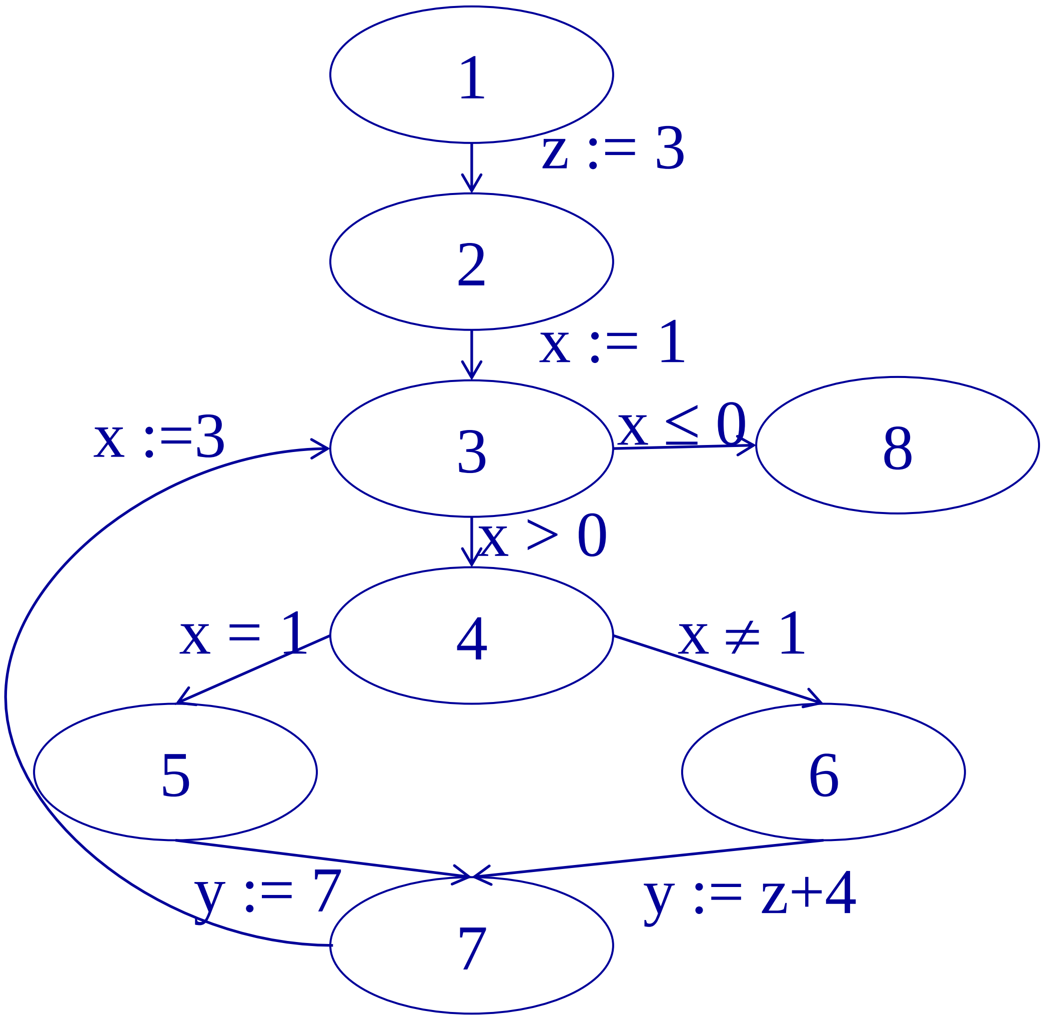
$DF[5] = DF[4] [\![x \neq 1]\!]^{\#}$

$DF[6] = DF[4] [\![x = 1]\!]^{\#}$

$DF[7] = DF[5] [\![y := 7]\!]^{\#} \sqcup DF[7] [\![y := z+4]\!]^{\#}$

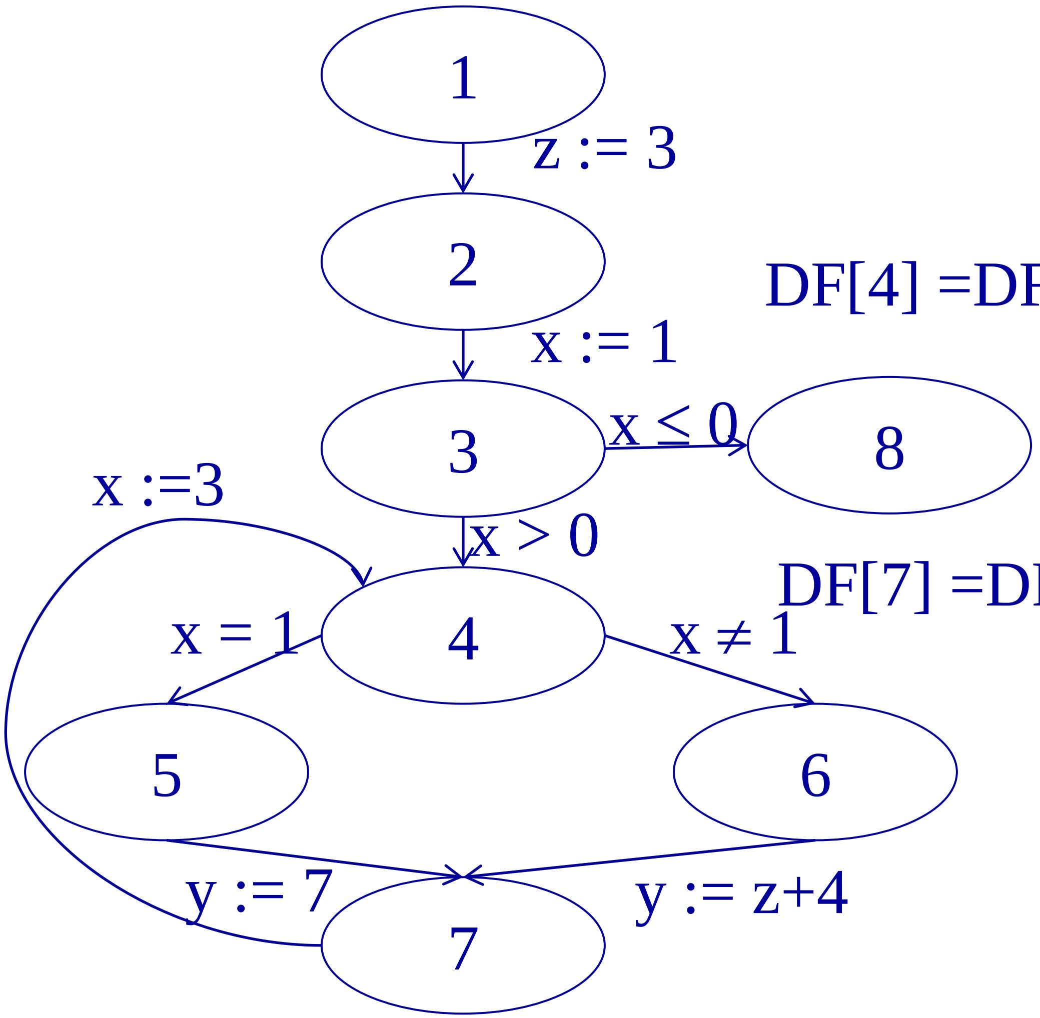
$DF[8] = DF[3] [\![x \leq 1]\!]^{\#}$

A Simple Example: Chaotic Iterations



N	DF[N]	WL
		{1}
1	[x↦0, y↦0, z ↦0]	{2}
2	[x↦0, y↦0, z ↦3]	{3}
3	[x↦1, y↦0, z ↦3]	{4, 8}
4	[x↦1, y↦0, z ↦3]	{5, 6, 8}
5	[x↦1, y↦0, z ↦3]	{6, 7, 8}
6		{7, 8}
7	[x↦1, y↦7, z ↦3]	{3, 8}
3	[x↦⊤, y ↦⊤, z ↦3]	{4, 8}
4	[x↦⊤, y↦⊤, z ↦3]	{5, 6, 8}
5	[x↦1, y↦⊤, z ↦3]	{6, 7, 8}
6	[x↦⊤, y↦⊤, z ↦3]	{7, 8}
7	[x↦⊤, y↦7, z ↦3]	{4, 8}
4		{8}
8	[x↦⊤, y ↦⊤, z ↦3]	{}

A Simple Example: System of Equations



$DF[1] = [x \mapsto 0, z \mapsto 0]$

$DF[2] = DF[1][\![z \mapsto 3]\!]^{\#}$

$DF[3] = DF[2][\![x \mapsto 1]\!]^{\#}$

$DF[4] = DF[3][\![x>0]\!]^{\#} \sqcup DF[7][\![y:=7]\!]^{\#}$

$DF[5] = DF[4][\![x \neq 1]\!]^{\#}$

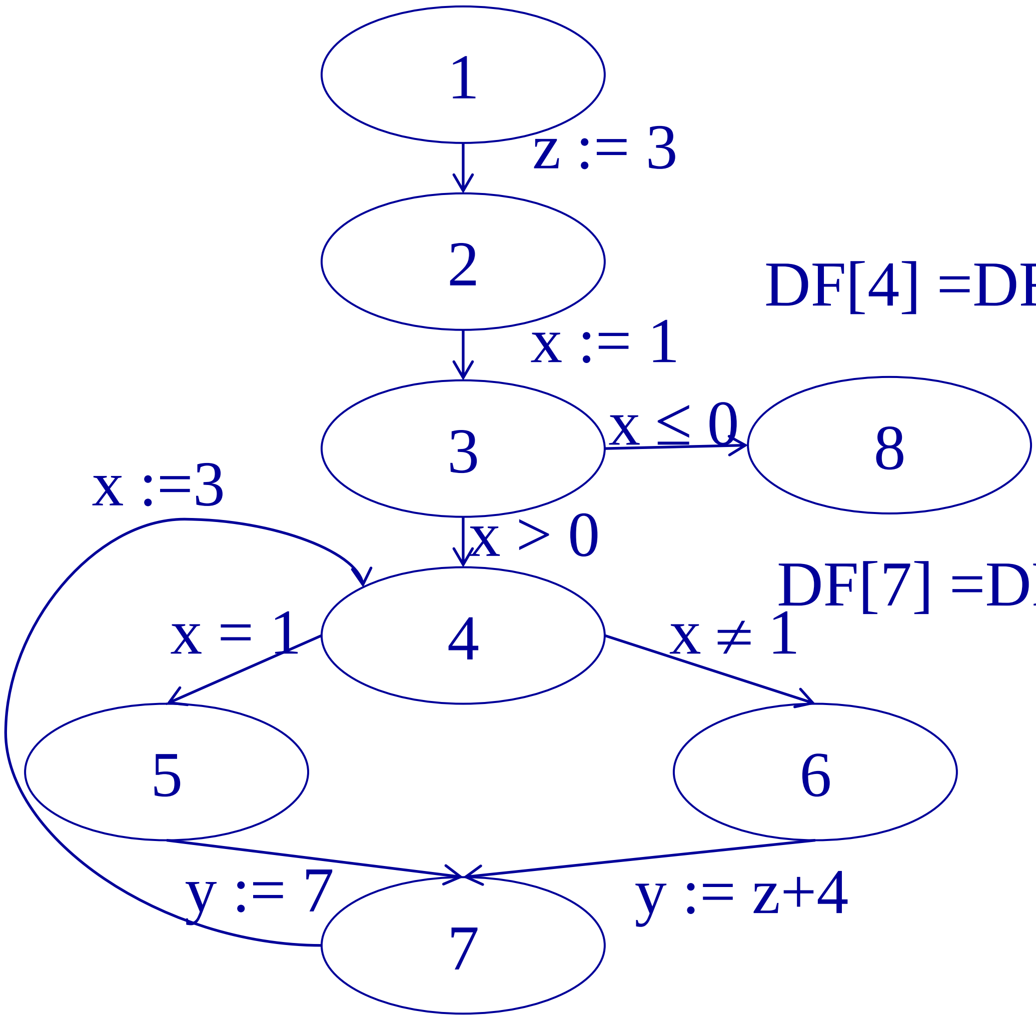
$DF[6] = DF[4][\![x=1]\!]^{\#}$

$DF[7] = DF[5][\![y:=7]\!]^{\#} \sqcup DF[7][\![y:=z+4]\!]^{\#}$

$DF[8] = DF[3][\![x \leq 1]\!]^{\#}$

What happens when values are initialized to $\top$?

A Simple Example: System of Equations



$$DF[1] = [x \mapsto \bot,\ z \mapsto \bot]$$

$$DF[2] = DF[1][\![z \mapsto 3]\!]^{\#}$$

$$DF[3] = DF[2][\![x \mapsto 1]\!]^{\#}$$

$$DF[4] = DF[3][\![x>0]\!]^{\#} \sqcup DF[7][\![y:=7]\!]^{\#}$$

$$DF[5] = DF[4][\![x \neq 1]\!]^{\#}$$

$$DF[6] = DF[4][\![x=1]\!]^{\#}$$

$$DF[7] = DF[5][\![y:=7]\!]^{\#} \sqcup DF[7][\![y:=z+4]\!]^{\#}$$

$$DF[8] = DF[3][\![x \leq 1]\!]^{\#}$$

When do we loose precision

- Dynamic vs. Static values
- Correlated branches
- Locality of transformers (Join over all path)
- Initial value

Low Level View

- Explicitly represent the program counter
- Create an abstract transition system which represents the analysis
- Execute transitions in arbitrary order

Low Level View (Example)

State : PC → (Var → Val)

Transformer: State → State

1: z = 3

2: x = 1

while 3: (x > 0) (

4: if (x = 1) then 5: y = 7

else 6: y =z + 4

7: x = 3

8: print y

)

$$\lambda S.\ \lambda pc.\ \lambda v:$$

$$\begin{cases}
0 & pc = 1 \\
S\ 1\ [z \mapsto 3]\ v & pc = 2 \\
(S\ 2\ [x \mapsto 1] \sqcup S\ 8)\ v & pc = 3 \\
S\ 3\ \ v & pc = 4 \\
(S\ 4 \sqcap [x \longmapsto 1,\ y \longmapsto \top,\ z \longmapsto \top])\ v & pc = 5 \\
S\ 4\ v & pc = 6 \\
(S\ 5\ [y \mapsto 7] \sqcup (S\ 6\ [y \mapsto (S\ 6\ z) + 4] & pc = 7 \\
S\ 7\ [x \mapsto 3]\ v & pc = 8
\end{cases}$$

Summary

- Chaotic iterations is a powerful technique
- Easy to implement
- Rather precise
- But expensive
  - More efficient methods exist for structured programs