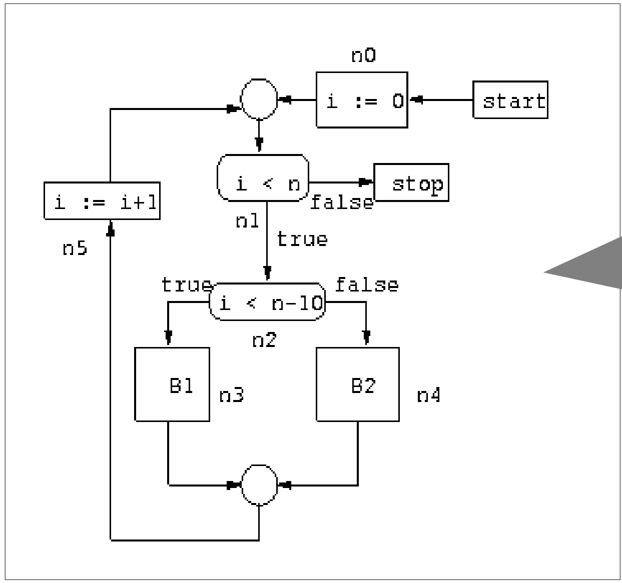
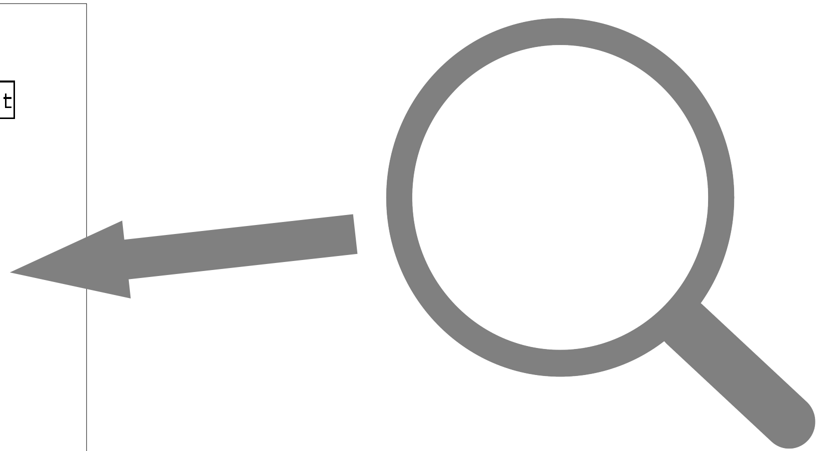
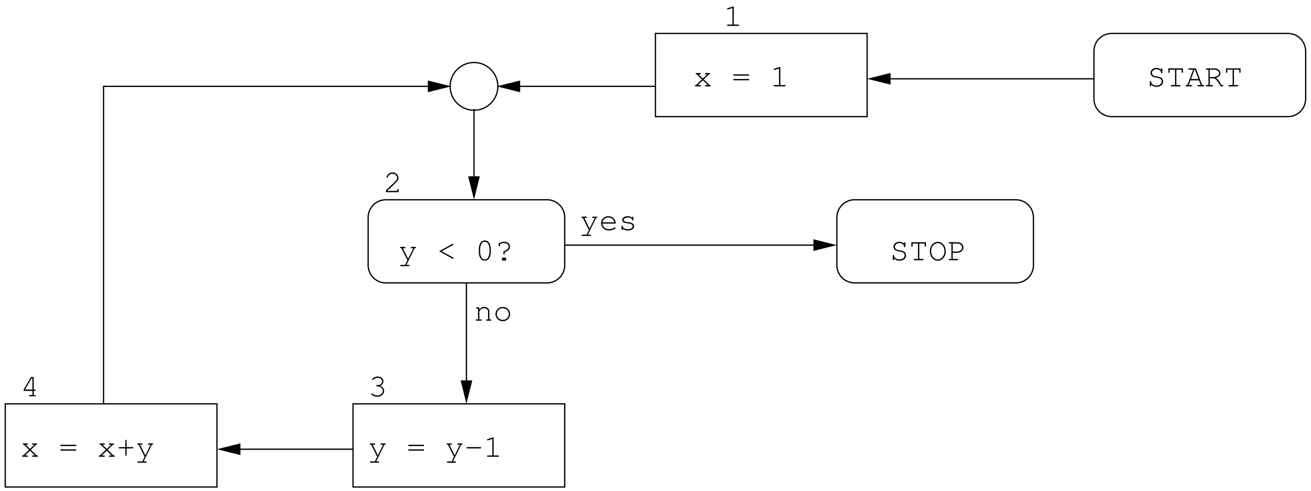
# Static Program Analysis
# Lecture 6: An Interval Analysis Example



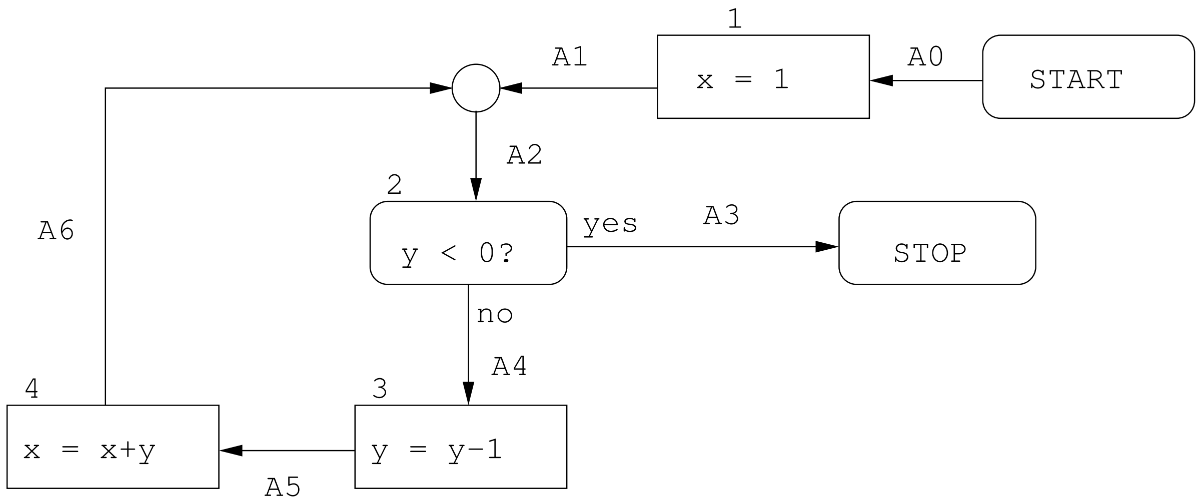



# An Interval Analysis Example




Same example program as for the dataflow analysis example

# Setting up the Equations

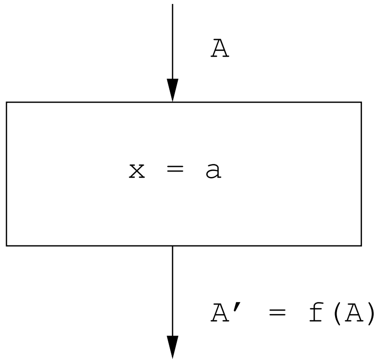



For each program point an abstract state: $A_0, \ldots, A_6$

Related by equations formed from the transfer functions for the CFG nodes

The analysis will compute values for them through fixed-point iteration

# Transfer Functions for Assignments




$f(A) = A[\mathtt{x} \mapsto \mathcal{A}[\![\mathtt{a}]\!]A]$

The abstract state (table) where all entries are the same as for $A$ except for $\mathtt{x}$, where it is $\mathcal{A}[\![\mathtt{a}]\!]A]$

$\mathcal{A}[\![\mathtt{a}]\!]$ is the interpretation of $\mathtt{a}$ over intervals rather than numbers

# An Example

Consider the assignment

```
x = x + y
```

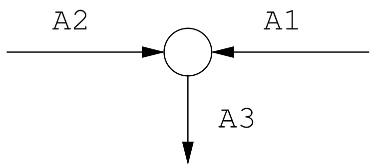
Assume abstract state $A = [\mathrm{x}\colon [1,2], \mathrm{y}\colon [2,5]]$

Then $f(A) = [\mathrm{x}\colon [1,2] + [2,5], \mathrm{y}\colon [2,5]] = [\mathrm{x}\colon [3,7], \mathrm{y}\colon [2,5]]$

Notice:

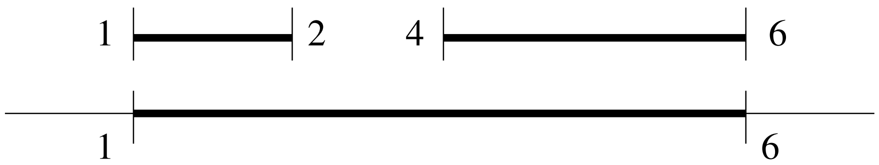
- The entry for `x` is updated, `y` is not touched
- The RHS `x + y` in the assignment is interpreted over intervals. Current intervals for `x` and `y` are inserted, and added

# Transfer Function for Join Nodes




$A_3 = A_1 \sqcup A_2$

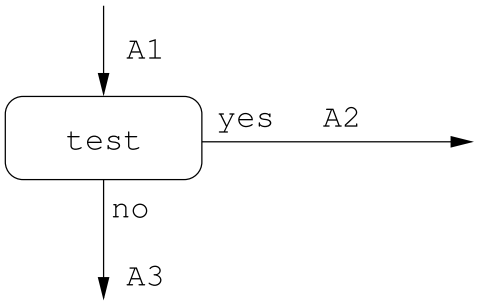
"$\sqcup$" ("join", or "merge") is similar to $\cup$ on sets. First defined on intervals as *smallest enclosing interval*. For instance, $[1, 2] \sqcup [4, 6] = [1, 6]$




Then "lifted" to abstract states entry-wise. Example:

$[\mathrm{x}\colon [1, 2], \mathrm{y}\colon [5, 5]] \sqcup [\mathrm{x}\colon [4, 6], \mathrm{y}\colon [1, 5]] = [\mathrm{x}\colon [1, 2] \sqcup [4, 6], \mathrm{y}\colon [5, 5] \sqcup [1, 5]] =$
$[\mathrm{x}\colon [1, 6], \mathrm{y}\colon [1, 5]]$

# Transfer Function for Test Nodes




$A_2 = b_T(A_1)$, $A_3 = b_F(A_1)$

The form of $b_T$ and $b_F$ depends on `test`

They capture the restriction on the possible states after the test

# An Example

If $\texttt{test} = \texttt{y} < \texttt{0}$, then $b_T$ adds the information that $\mathtt{y} < 0$ and $b_F$ that $\mathtt{y} \geq 0$. Thus,

$$b_T([\mathrm{x}\colon[1,6], \mathrm{y}\colon[-3,5]]) = [\mathrm{x}\colon[1,6], \mathrm{y}\colon[-3,-1]]$$

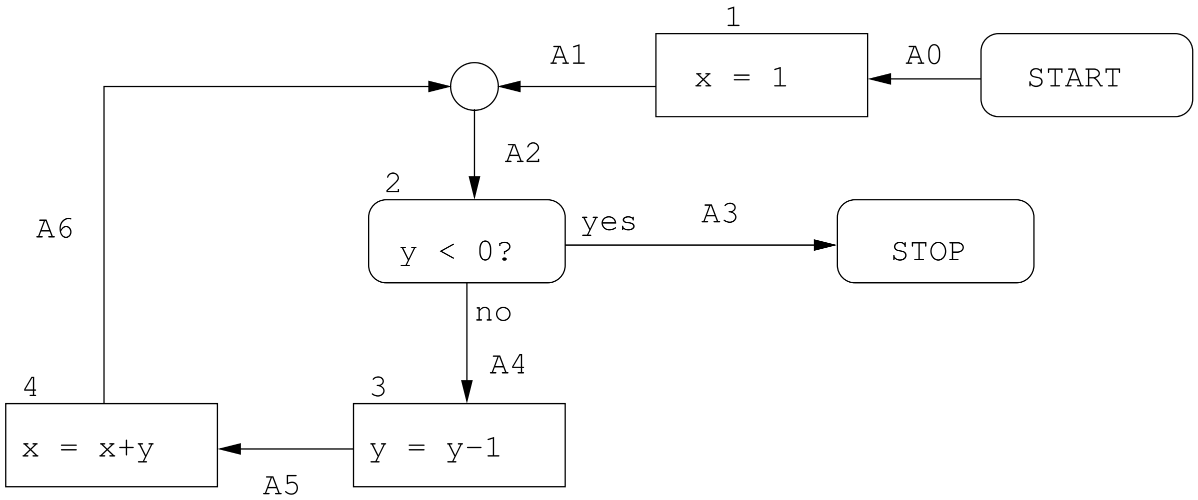
and

$$b_F([\mathrm{x}\colon[1,6], \mathrm{y}\colon[-3,5]]) = [\mathrm{x}\colon[1,6], \mathrm{y}\colon[0,5]]$$

($\mathtt{x}$ is not touched, but the interval for $\mathtt{y}$ is restricted)

# Equations for Interval Analysis

$$
\begin{aligned}
A_0 &= [\mathrm{x}\colon [1,10], \mathrm{y}\colon [-5,5]] \\
A_1 &= f_1(A_0) \\
A_2 &= A_1 \sqcup A_6 \\
A_3 &= b_T(A_2) \\
A_4 &= b_F(A_2) \\
A_5 &= f_3(A_4) \\
A_6 &= f_4(A_5)
\end{aligned}
$$

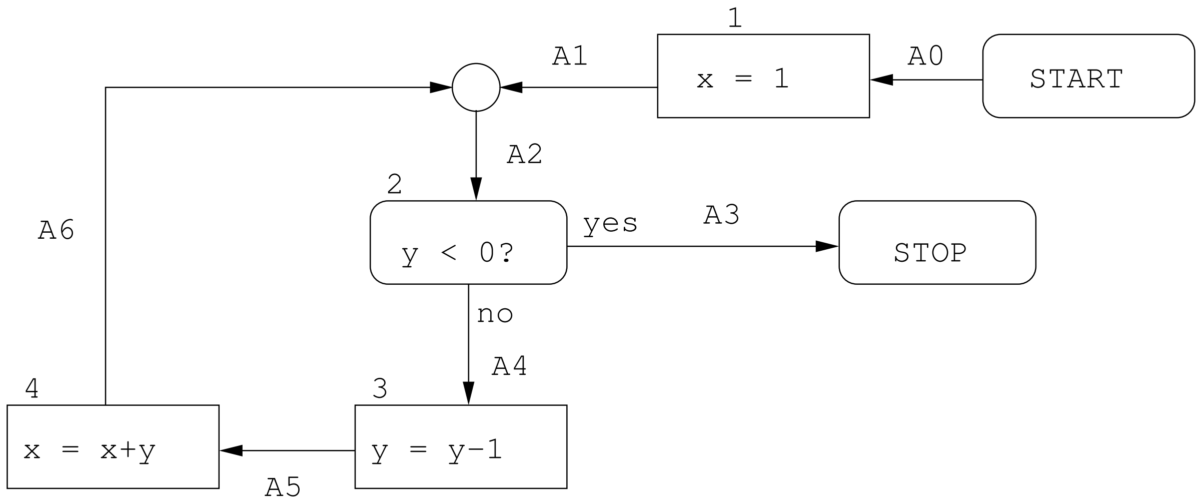



A system of equations relating abstract states $A_0, \ldots, A_6$

We assume that $\mathrm{x} \in [1, 10]$, $\mathrm{y} \in [-5, 5]$ when the program starts. Thus the equation for abstract state $A_0$ above

# Solving the Equations

$$
\begin{aligned}
{\color{red}A_{0,0}} &= [\mathrm{x}: \emptyset, \mathrm{y}: \emptyset] \\
A_{1,0} &= [\mathrm{x}: \emptyset, \mathrm{y}: \emptyset] \\
A_{2,0} &= [\mathrm{x}: \emptyset, \mathrm{y}: \emptyset] \\
A_{3,0} &= [\mathrm{x}: \emptyset, \mathrm{y}: \emptyset] \\
A_{4,0} &= [\mathrm{x}: \emptyset, \mathrm{y}: \emptyset] \\
A_{5,0} &= [\mathrm{x}: \emptyset, \mathrm{y}: \emptyset] \\
A_{6,0} &= [\mathrm{x}: \emptyset, \mathrm{y}: \emptyset]
\end{aligned}
$$

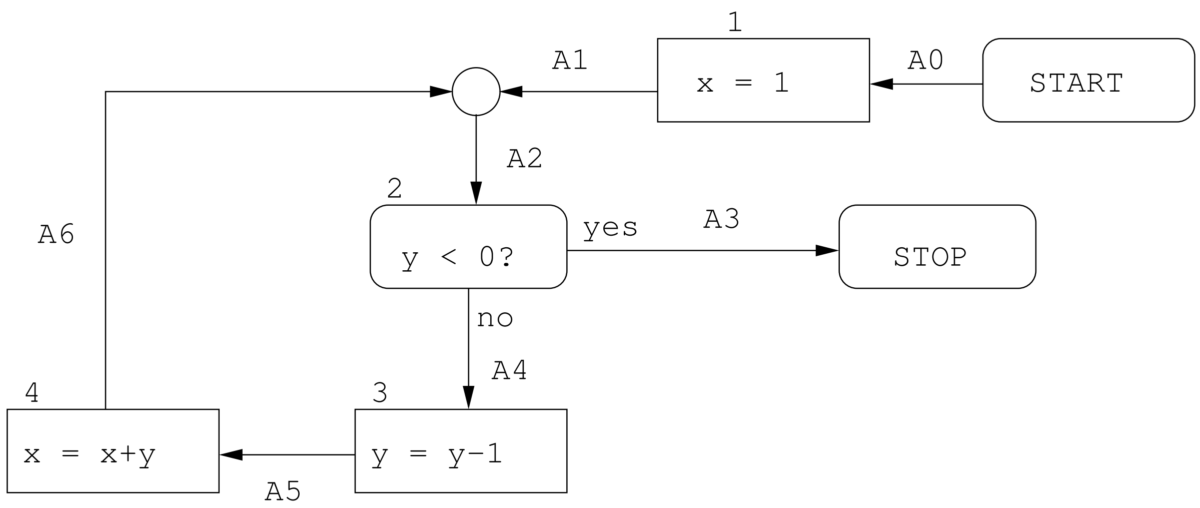



Least fixed-point iteration, as before. Start with least possible intervals ($\emptyset$) as abstract values held by variables

# Iteration 1

Update using equation $A_0 = [\text{x}: [1, 10], \text{y}: [-5, 5]]$:

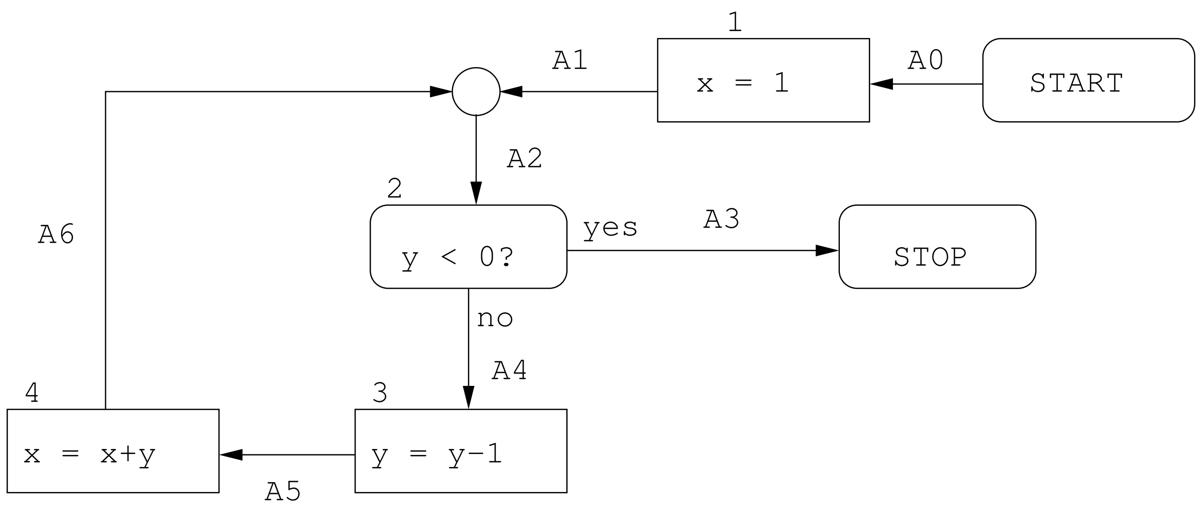
$$
\begin{aligned}
A_{0,1} &= [\text{x}: [1, 10], \text{y}: [-5, 5]] \\
A_{1,0} &= [\text{x}: \emptyset, \text{y}: \emptyset] \\
A_{2,0} &= [\text{x}: \emptyset, \text{y}: \emptyset] \\
A_{3,0} &= [\text{x}: \emptyset, \text{y}: \emptyset] \\
A_{4,0} &= [\text{x}: \emptyset, \text{y}: \emptyset] \\
A_{5,0} &= [\text{x}: \emptyset, \text{y}: \emptyset] \\
A_{6,0} &= [\text{x}: \emptyset, \text{y}: \emptyset]
\end{aligned}
$$



# Iteration 2

Update using equation $A_1 = f_1(A_0)$:

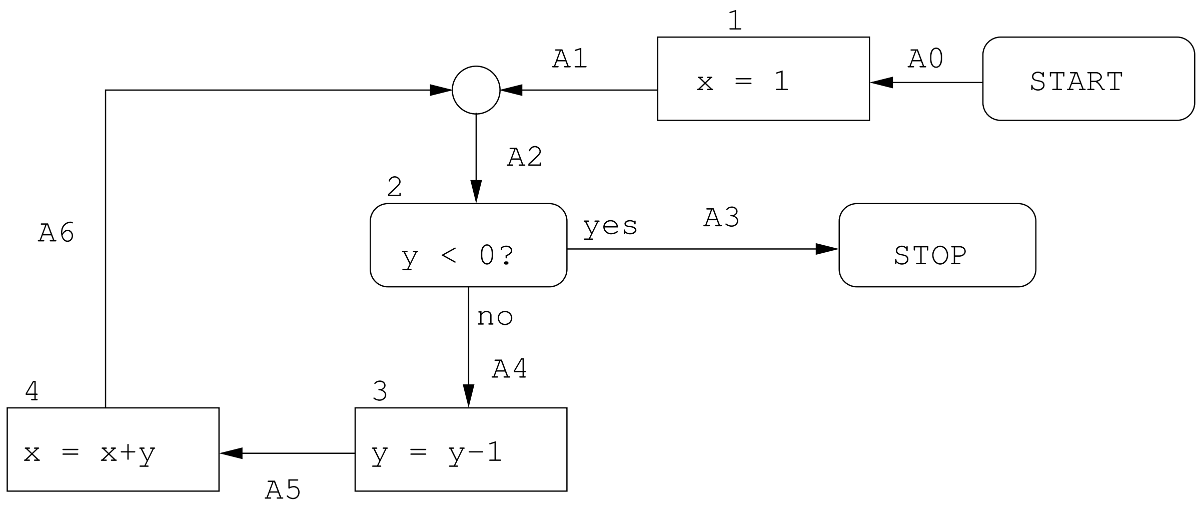
$$
\begin{aligned}
A_{0,1} &= [\mathrm{x}\colon [1, 10], \mathrm{y}\colon [-5, 5]] \\
A_{1,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [-5, 5]] \\
\color{red}{A_{2,0}} &= [\mathrm{x}\colon \emptyset, \mathrm{y}\colon \emptyset] \\
A_{3,0} &= [\mathrm{x}\colon \emptyset, \mathrm{y}\colon \emptyset] \\
A_{4,0} &= [\mathrm{x}\colon \emptyset, \mathrm{y}\colon \emptyset] \\
A_{5,0} &= [\mathrm{x}\colon \emptyset, \mathrm{y}\colon \emptyset] \\
A_{6,0} &= [\mathrm{x}\colon \emptyset, \mathrm{y}\colon \emptyset]
\end{aligned}
$$



# Iteration 3

Update using equation $A_2 = A_1 \sqcup A_6$:

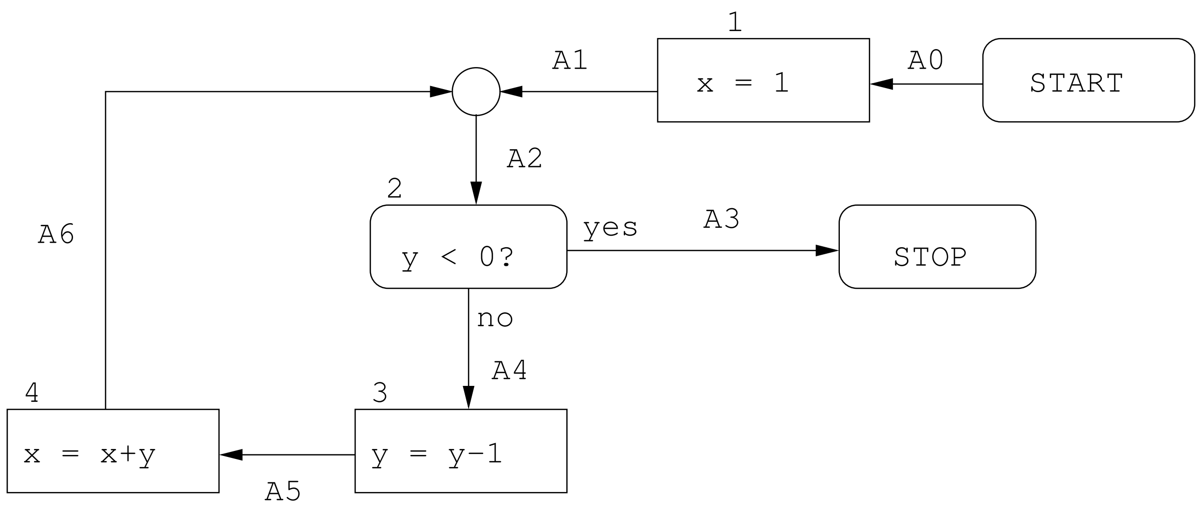
$$
\begin{aligned}
A_{0,1} &= [\mathtt{x}: [1, 10], \mathtt{y}: [-5, 5]] \\
A_{1,1} &= [\mathtt{x}: [1, 1], \mathtt{y}: [-5, 5]] \\
A_{2,1} &= [\mathtt{x}: [1, 1], \mathtt{y}: [-5, 5]] \\
A_{3,0} &= [\mathtt{x}: \emptyset, \mathtt{y}: \emptyset] \\
A_{4,0} &= [\mathtt{x}: \emptyset, \mathtt{y}: \emptyset] \\
A_{5,0} &= [\mathtt{x}: \emptyset, \mathtt{y}: \emptyset] \\
A_{6,0} &= [\mathtt{x}: \emptyset, \mathtt{y}: \emptyset]
\end{aligned}
$$



# Iteration 4

Update using equation $A_3 = b_T(A_2)$:

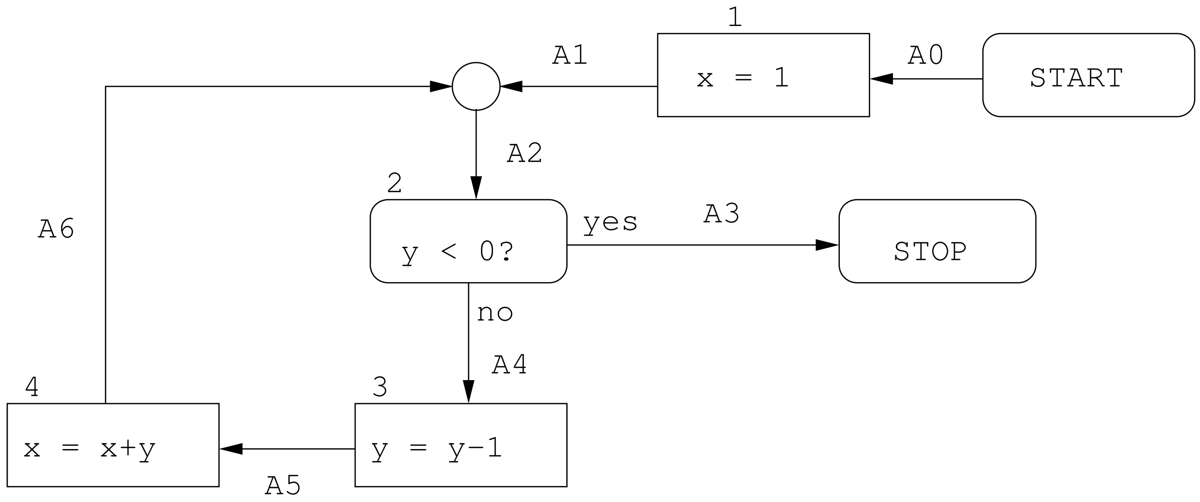
$$
\begin{aligned}
A_{0,1} &= [\text{x}: [1, 10], \text{y}: [-5, 5]] \\
A_{1,1} &= [\text{x}: [1, 1], \text{y}: [-5, 5]] \\
A_{2,1} &= [\text{x}: [1, 1], \text{y}: [-5, 5]] \\
A_{3,1} &= [\text{x}: [1, 1], \text{y}: [-5, -1]] \\
A_{4,0} &= [\text{x}: \emptyset, \text{y}: \emptyset] \\
A_{5,0} &= [\text{x}: \emptyset, \text{y}: \emptyset] \\
A_{6,0} &= [\text{x}: \emptyset, \text{y}: \emptyset]
\end{aligned}
$$



# Iteration 5

Update using equation $A_4 = b_F(A_2)$:

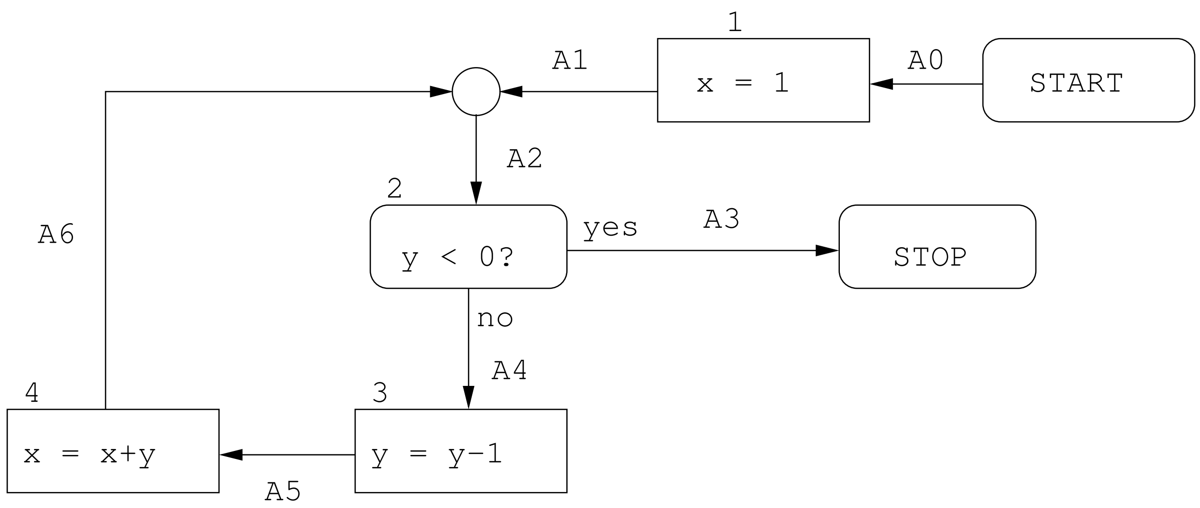
$$
\begin{aligned}
A_{0,1} &= [\mathrm{x}\colon [1, 10], \mathrm{y}\colon [-5, 5]] \\
A_{1,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [-5, 5]] \\
A_{2,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [-5, 5]] \\
A_{3,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [-5, -1]] \\
A_{4,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [0, 5]] \\
{\color{red}A_{5,0}} &= [\mathrm{x}\colon \emptyset, \mathrm{y}\colon \emptyset] \\
A_{6,0} &= [\mathrm{x}\colon \emptyset, \mathrm{y}\colon \emptyset]
\end{aligned}
$$



# Iteration 6

Update using equation $A_5 = f_3(A_4)$:

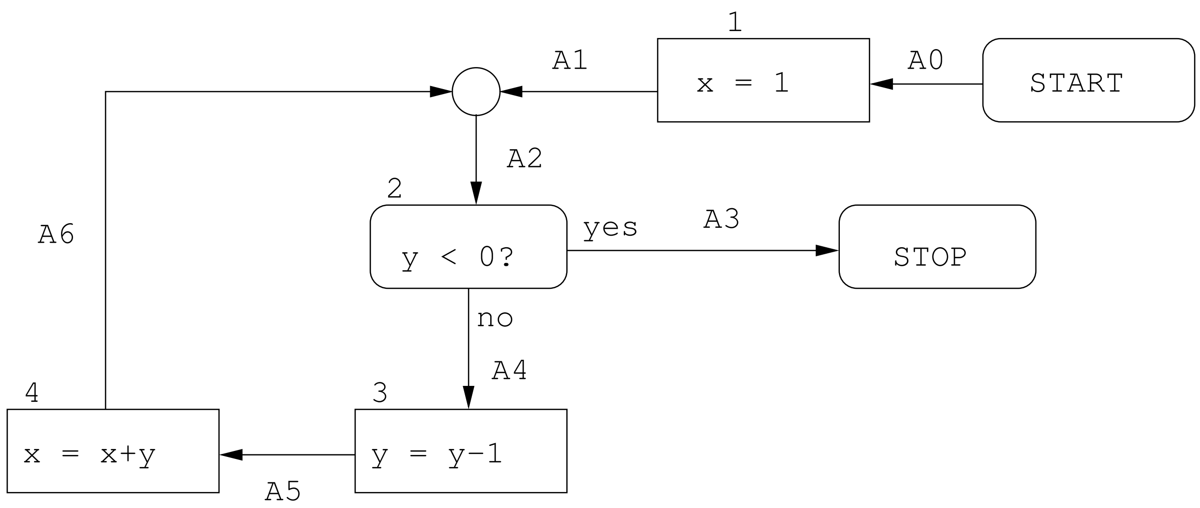
$$
\begin{aligned}
A_{0,1} &= [\mathrm{x}\colon [1, 10], \mathrm{y}\colon [-5, 5]] \\
A_{1,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [-5, 5]] \\
A_{2,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [-5, 5]] \\
A_{3,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [-5, -1]] \\
A_{4,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [0, 5]] \\
A_{5,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [-1, 4]] \\
{\color{red}A_{6,0}} &= [\mathrm{x}\colon \emptyset, \mathrm{y}\colon \emptyset]
\end{aligned}
$$



# Iteration 7

Update using equation $A_6 = f_4(A_5)$:

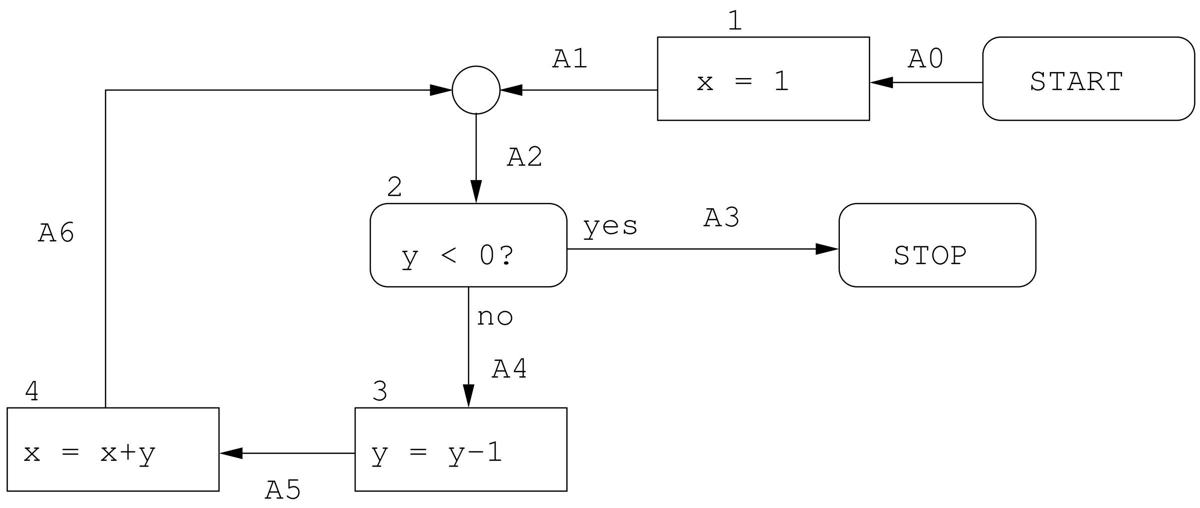
$$
\begin{aligned}
A_{0,1} &= [\text{x}: [1, 10], \text{y}: [-5, 5]] \\
A_{1,1} &= [\text{x}: [1, 1], \text{y}: [-5, 5]] \\
A_{2,1} &= [\text{x}: [1, 1], \text{y}: [-5, 5]] \\
A_{3,1} &= [\text{x}: [1, 1], \text{y}: [-5, -1]] \\
A_{4,1} &= [\text{x}: [1, 1], \text{y}: [0, 5]] \\
A_{5,1} &= [\text{x}: [1, 1], \text{y}: [-1, 4]] \\
A_{6,1} &= [\text{x}: [0, 5], \text{y}: [-1, 4]]
\end{aligned}
$$



# Iteration 8

Update using equation $A_2 = A_1 \sqcup A_6$:

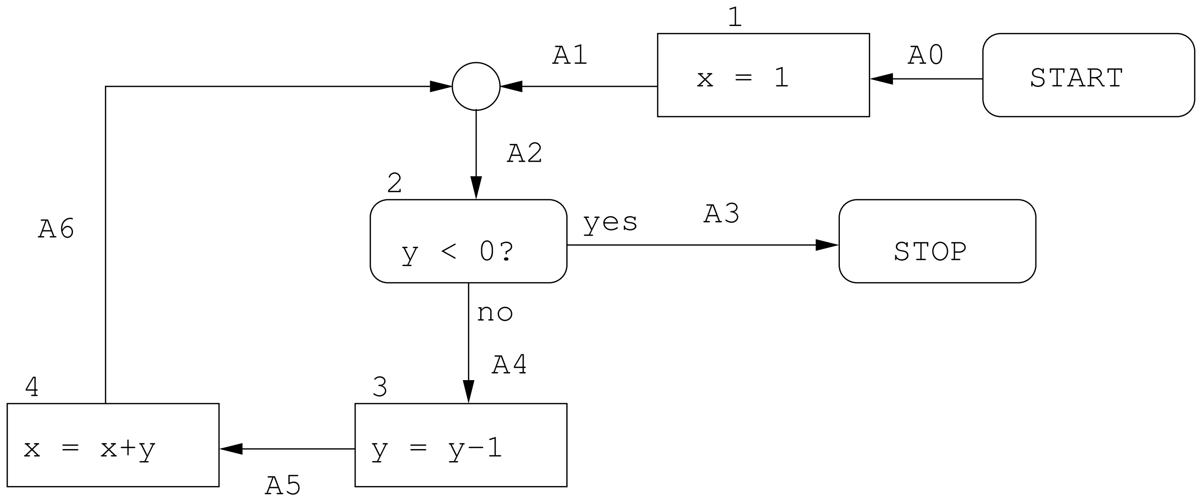
$$
\begin{aligned}
A_{0,1} &= [\mathrm{x}\colon [1, 10], \mathrm{y}\colon [-5, 5]] \\
A_{1,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [-5, 5]] \\
A_{2,2} &= [\mathrm{x}\colon [0, 5], \mathrm{y}\colon [-5, 5]] \\
A_{3,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [-5, -1]] \\
A_{4,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [0, 5]] \\
A_{5,1} &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [-1, 4]] \\
A_{6,1} &= [\mathrm{x}\colon [0, 5], \mathrm{y}\colon [-1, 4]]
\end{aligned}
$$



# Iteration 9

Update using equation $A_3 = b_T(A_2)$:

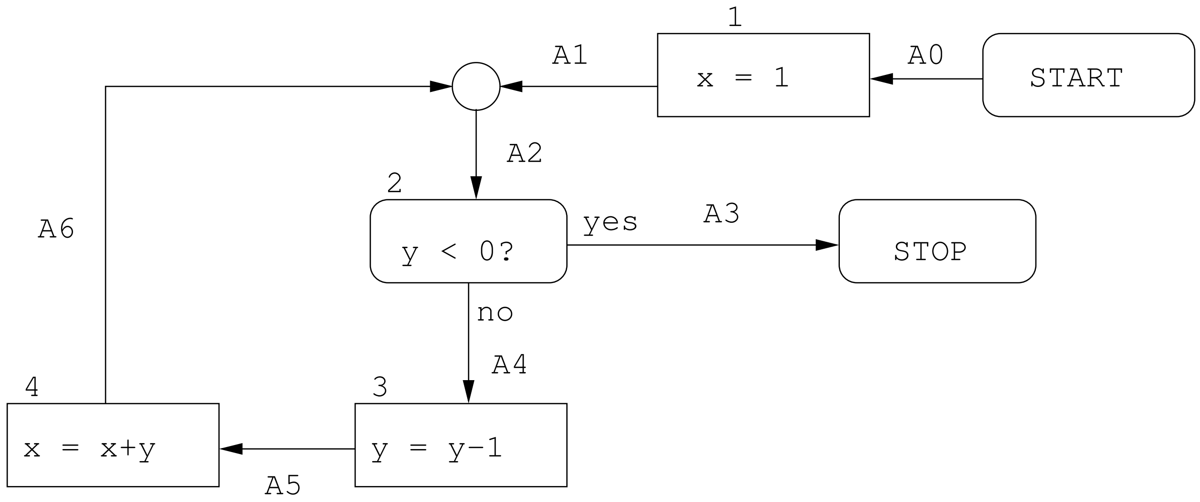
$$
\begin{aligned}
A_{0,1} &= [\text{x}: [1, 10], \text{y}: [-5, 5]] \\
A_{1,1} &= [\text{x}: [1, 1], \text{y}: [-5, 5]] \\
A_{2,2} &= [\text{x}: [0, 5], \text{y}: [-5, 5]] \\
A_{3,2} &= [\text{x}: [0, 5], \text{y}: [-5, -1]] \\
A_{4,1} &= [\text{x}: [1, 1], \text{y}: [0, 5]] \\
A_{5,1} &= [\text{x}: [1, 1], \text{y}: [-1, 4]] \\
A_{6,1} &= [\text{x}: [0, 5], \text{y}: [-1, 4]]
\end{aligned}
$$



# Iteration 10

Update using equation $A_4 = b_F(A_2)$:

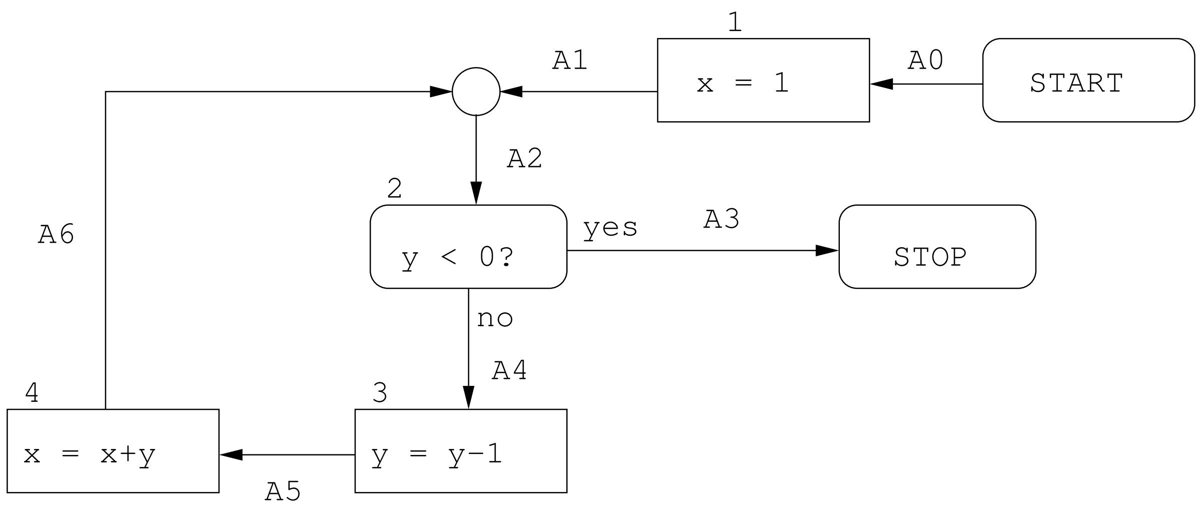
$$
\begin{aligned}
A_{0,1} &= [\text{x}: [1, 10], \text{y}: [-5, 5]] \\
A_{1,1} &= [\text{x}: [1, 1], \text{y}: [-5, 5]] \\
A_{2,2} &= [\text{x}: [0, 5], \text{y}: [-5, 5]] \\
A_{3,2} &= [\text{x}: [0, 5], \text{y}: [-5, -1]] \\
A_{4,2} &= [\text{x}: [0, 5], \text{y}: [0, 5]] \\
A_{5,1} &= [\text{x}: [1, 1], \text{y}: [-1, 4]] \\
A_{6,1} &= [\text{x}: [0, 5], \text{y}: [-1, 4]]
\end{aligned}
$$



# Iteration 11

Update using equation $A_5 = f_3(A_4)$:

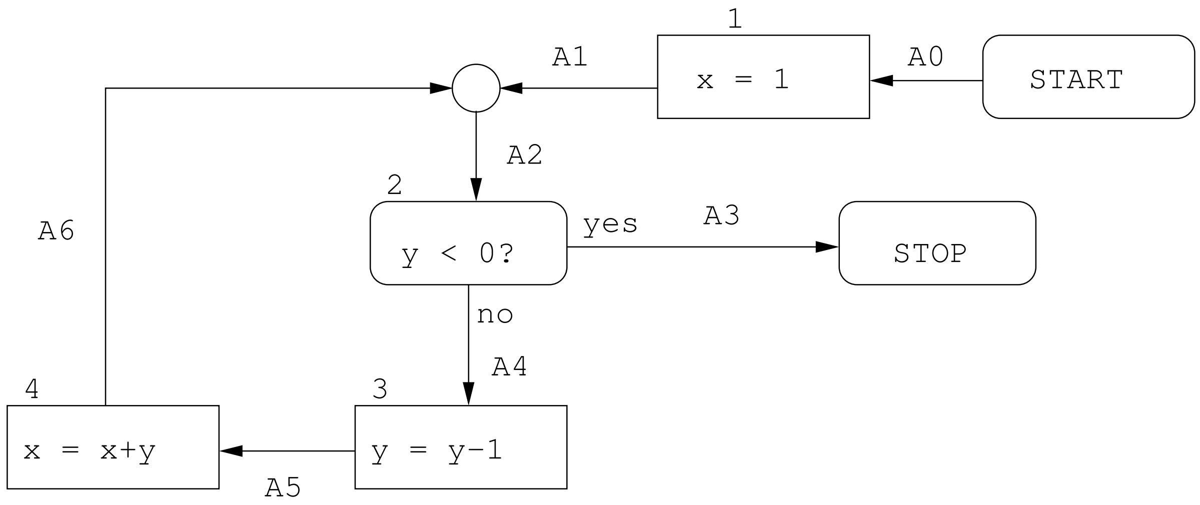
$$
\begin{aligned}
A_{0,1} &= [\text{x}: [1, 10], \text{y}: [-5, 5]] \\
A_{1,1} &= [\text{x}: [1, 1], \text{y}: [-5, 5]] \\
A_{2,2} &= [\text{x}: [0, 5], \text{y}: [-5, 5]] \\
A_{3,2} &= [\text{x}: [0, 5], \text{y}: [-5, -1]] \\
A_{4,2} &= [\text{x}: [0, 5], \text{y}: [0, 5]] \\
A_{5,2} &= [\text{x}: [0, 5], \text{y}: [-1, 4]] \\
\color{red}{A_{6,1}} &= [\text{x}: [0, 5], \text{y}: [-1, 4]]
\end{aligned}
$$



# Iteration 12

Update using equation $A_6 = f_4(A_5)$:

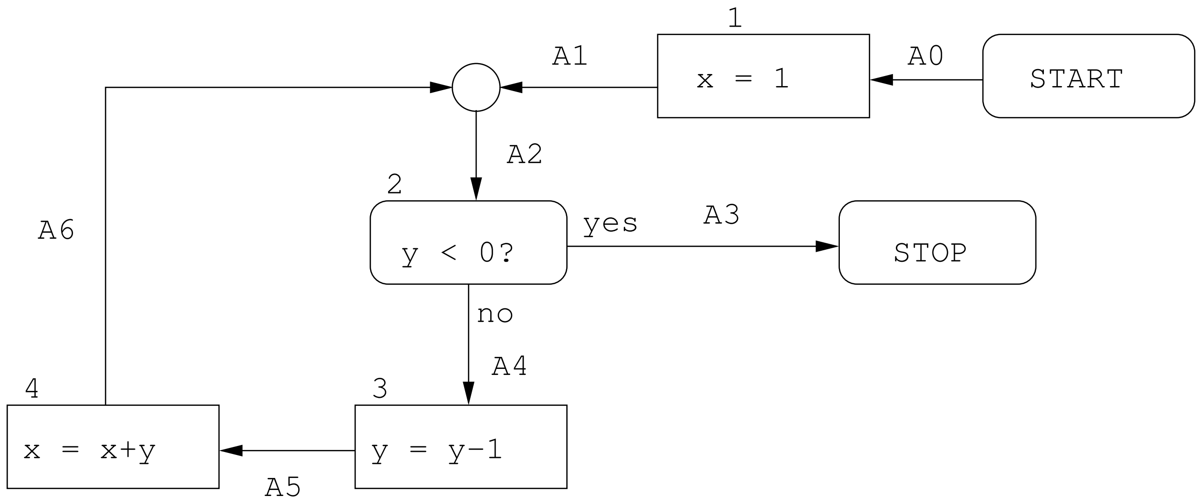
$A_{0,1} = [\mathrm{x}: [1, 10], \mathrm{y}: [-5, 5]]$
$A_{1,1} = [\mathrm{x}: [1, 1], \mathrm{y}: [-5, 5]]$
$A_{2,2} = [\mathrm{x}: [0, 5], \mathrm{y}: [-5, 5]]$
$A_{3,2} = [\mathrm{x}: [0, 5], \mathrm{y}: [-5, -1]]$
$A_{4,2} = [\mathrm{x}: [0, 5], \mathrm{y}: [0, 5]]$
$A_{5,2} = [\mathrm{x}: [0, 5], \mathrm{y}: [-1, 4]]$
$A_{6,2} = [\mathrm{x}: [-1, 9], \mathrm{y}: [-1, 4]]$




Etc. This iteration does not converge in a finite number of steps. However, a convergence acceleration technique called **widening** can be applied which ensures termination (at cost of some overapproximation)

# A Solution

$$
\begin{aligned}
A_0 &= [\mathrm{x}\colon [1, 10], \mathrm{y}\colon [-5, 5]] \\
A_1 &= [\mathrm{x}\colon [1, 1], \mathrm{y}\colon [-5, 5]] \\
A_2 &= [\mathrm{x}\colon [-\infty, \infty], \mathrm{y}\colon [-5, 5]] \\
A_3 &= [\mathrm{x}\colon [-\infty, \infty], \mathrm{y}\colon [-5, -1]] \\
A_4 &= [\mathrm{x}\colon [-\infty, \infty], \mathrm{y}\colon [0, 5]] \\
A_5 &= [\mathrm{x}\colon [-\infty, \infty], \mathrm{y}\colon [-1, 4]] \\
A_6 &= [\mathrm{x}\colon [-\infty, \infty], \mathrm{y}\colon [-1, 4]]
\end{aligned}
$$




Obtained by widening

Notice that the value range of `x` is overapproximated in the loop