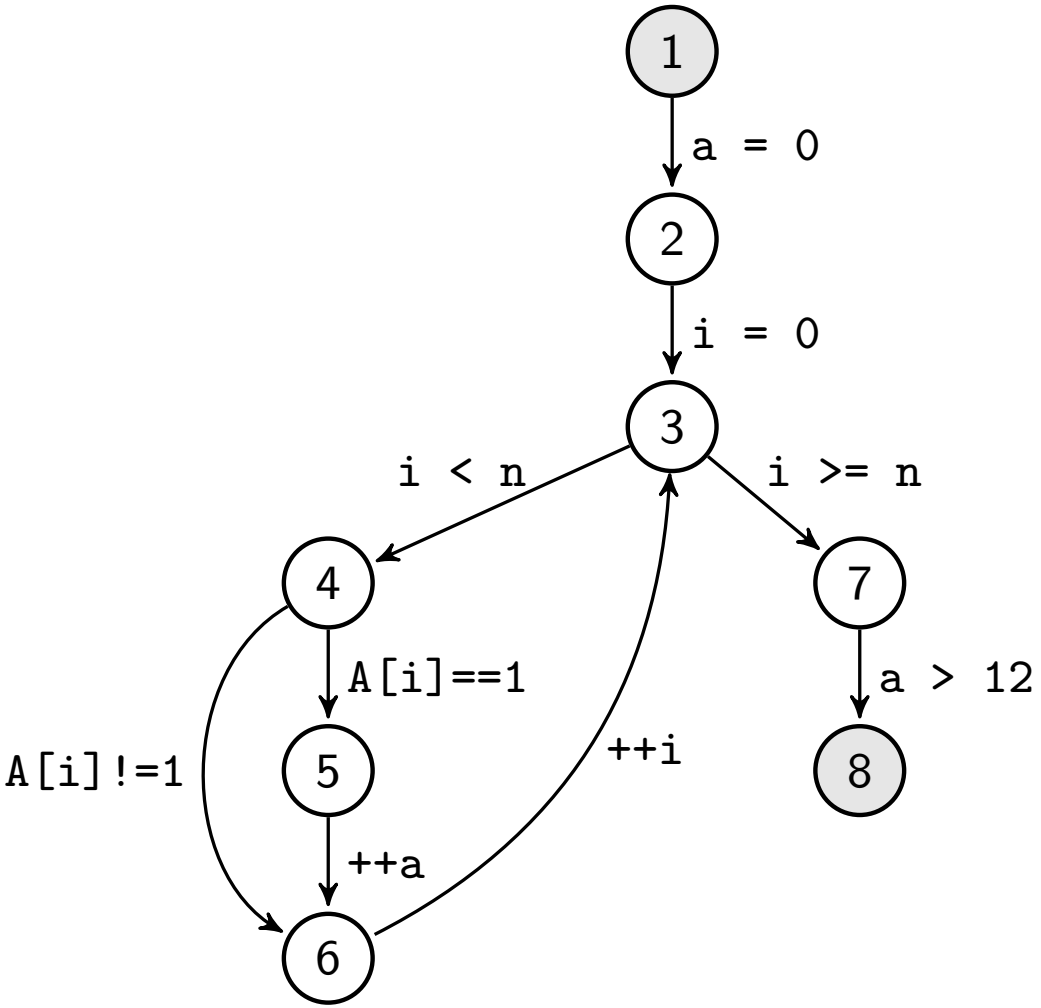
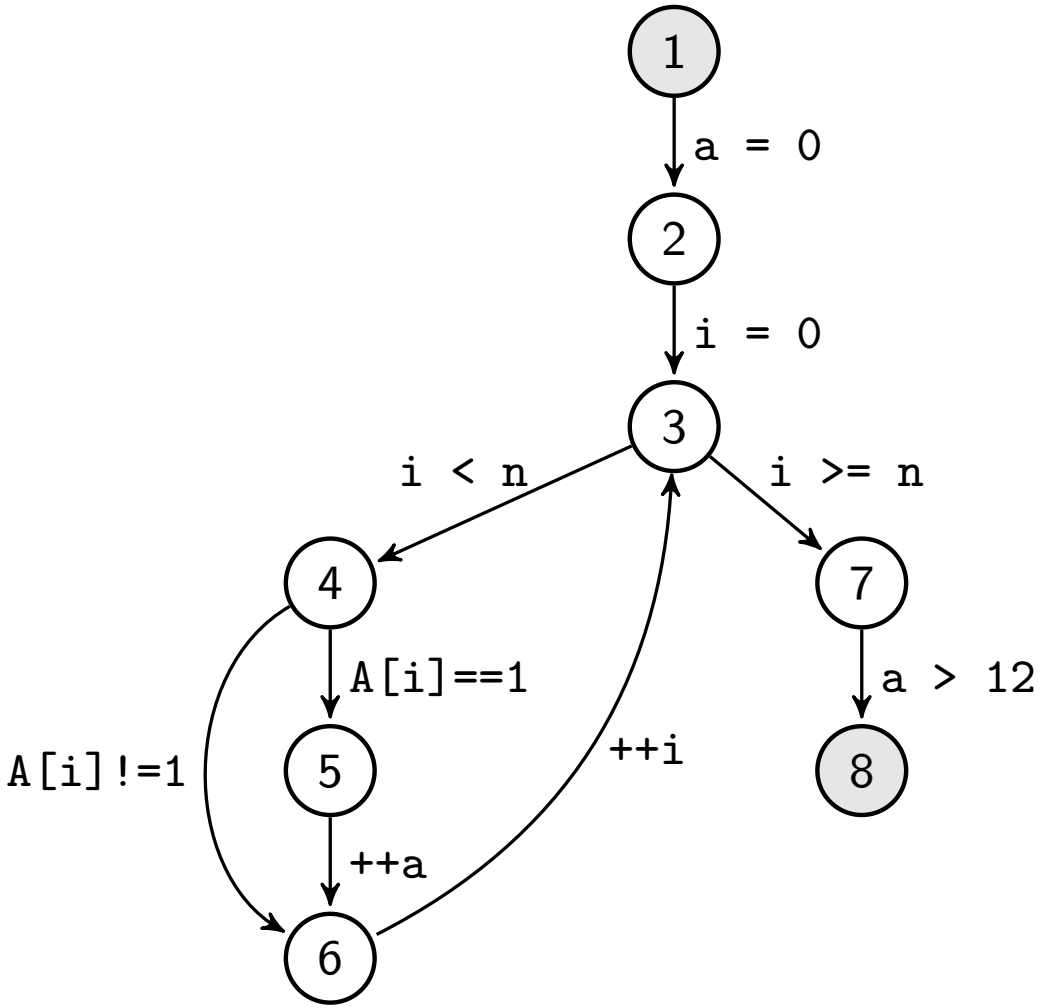
Overapproximating Program Paths using FOL Formula

Jan Strejček and **Marek Trtík**

Motivation

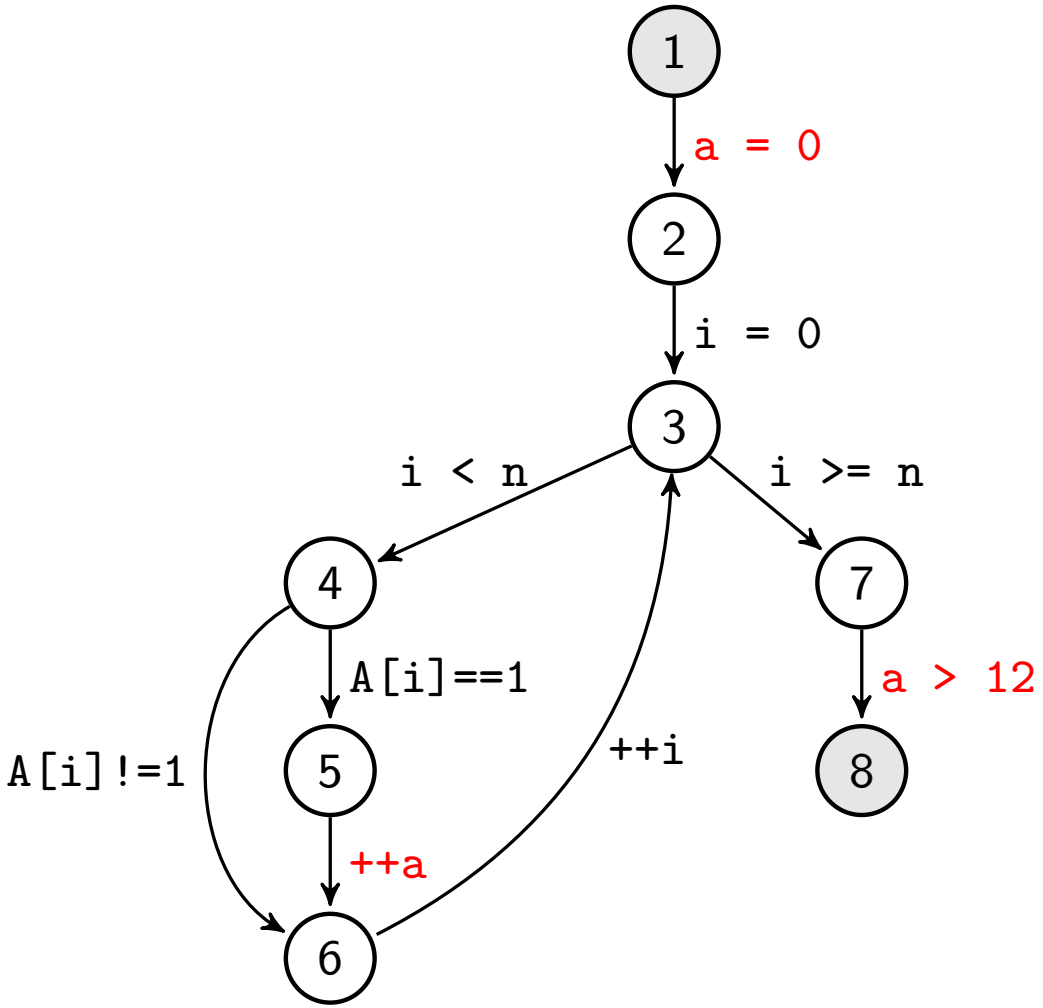


Motivation



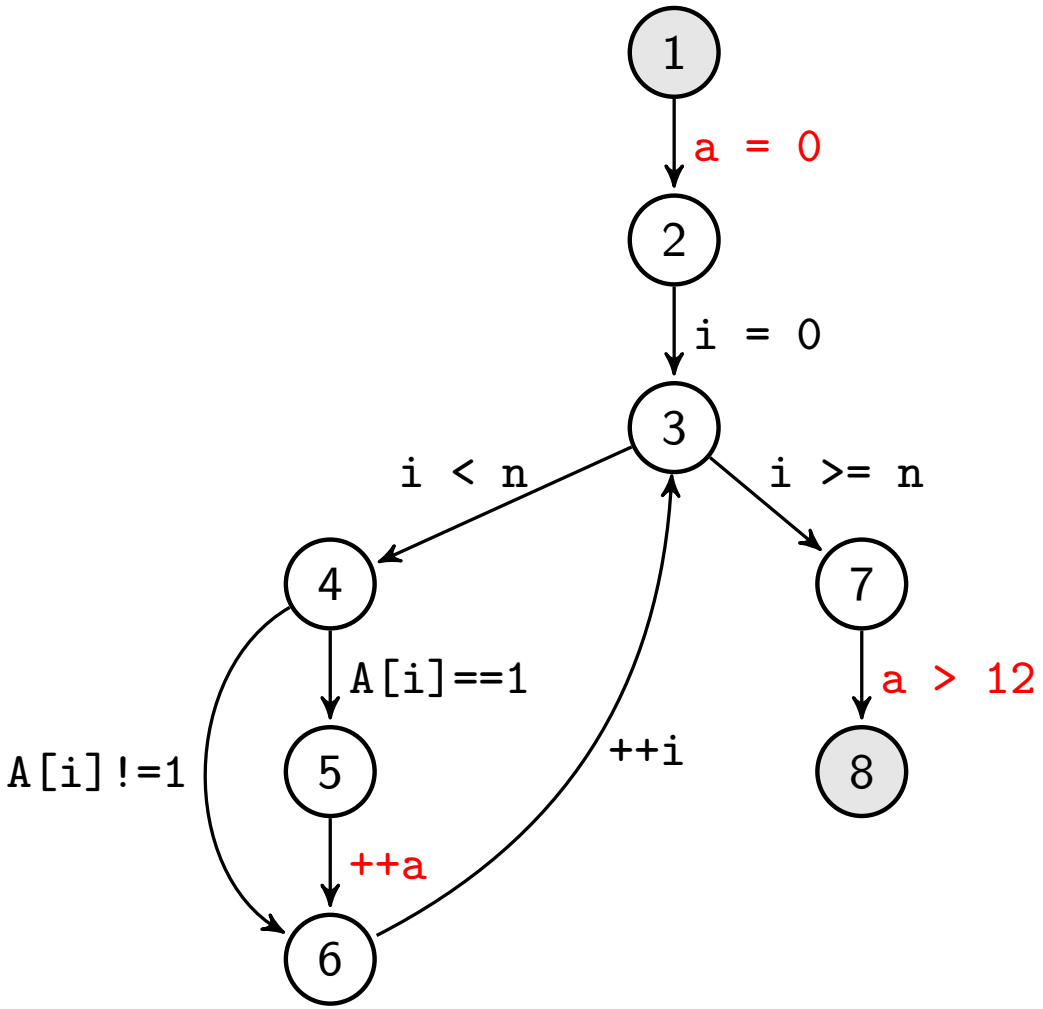
$> 2^{2^{32}}$ paths

Motivation



$> 2^{2^{32}}$ paths

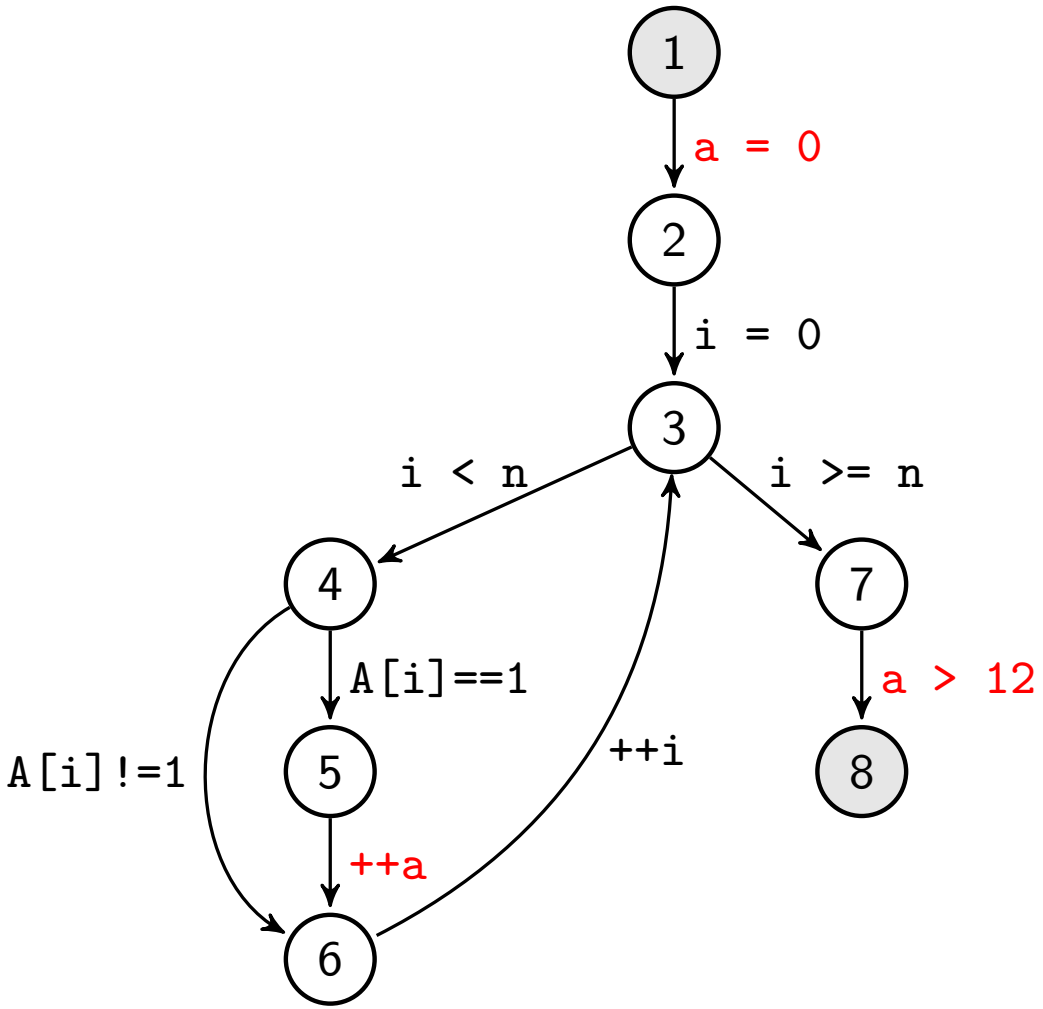
Motivation



$> 2^{2^{32}}$ paths

(1) Relax exact interleaving of paths through a loop.

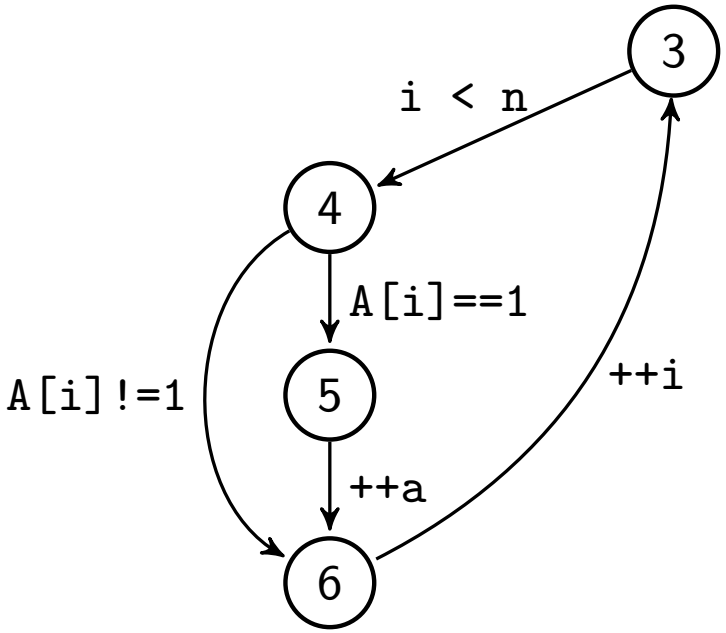
Motivation



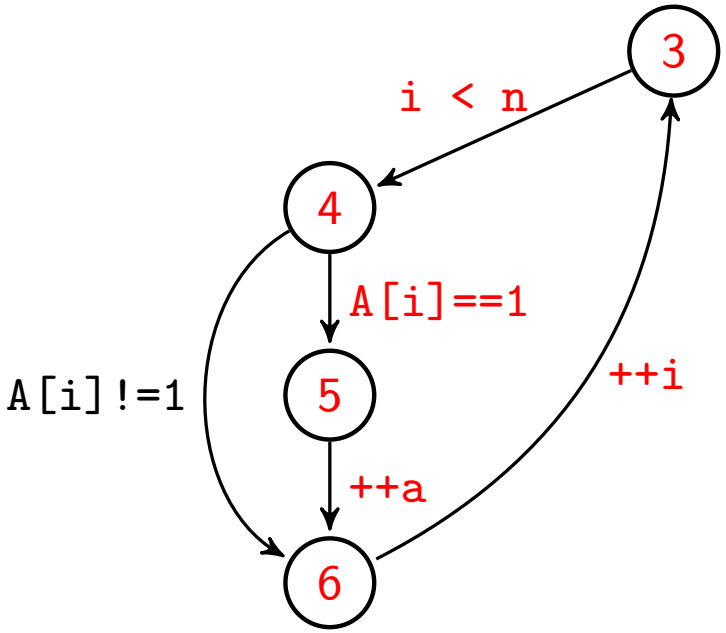
$> 2^{2^{32}}$ paths

(1) Relax exact interleaving of paths through a loop.
(2) Express variables as functions of path counters.

Our heuristic

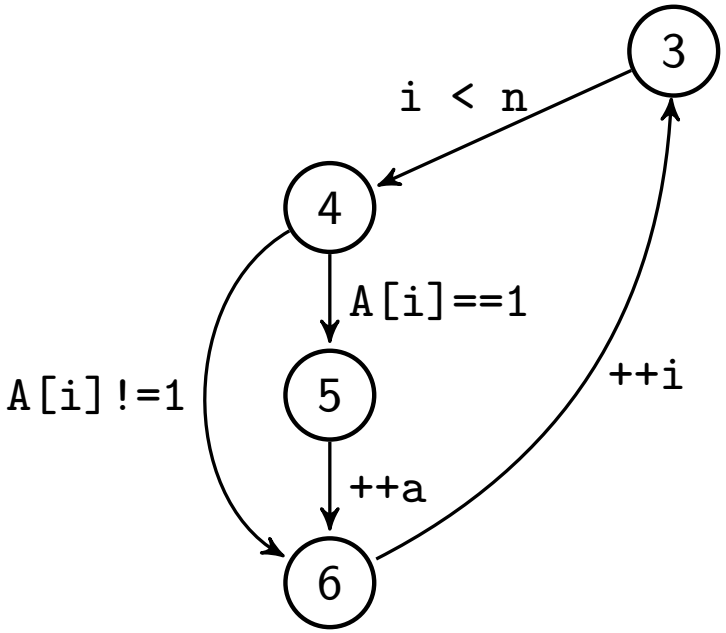


Our heuristic



$$\texttt{i} \to \underline{i} \rightsquigarrow \texttt{i} \to \underline{i} + 1$$
$$\texttt{a} \to \underline{a} \rightsquigarrow \texttt{a} \to \underline{a} + 1$$

Our heuristic

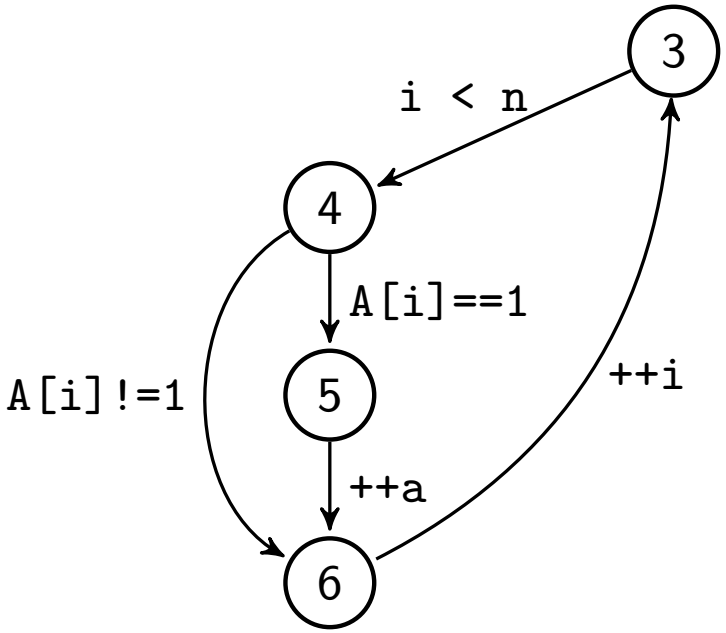


$$\mathtt{i} \to \underline{i} \rightsquigarrow \mathtt{i} \to \underline{i} + 1$$

$$\mathtt{a} \to \underline{a} \rightsquigarrow \mathtt{a} \to \underline{a} + 1$$

$$i(\kappa_1) = \kappa_1 + \underline{i}$$

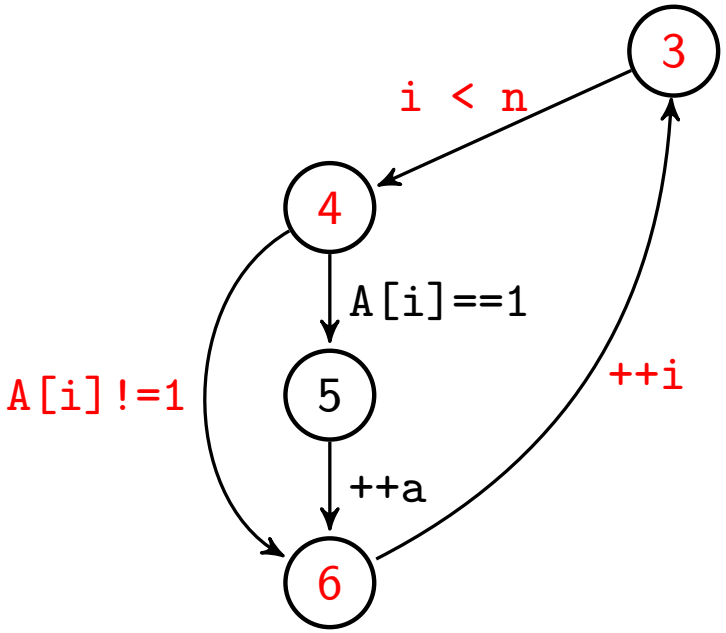
Our heuristic



$$\texttt{i} \to \underline{i} \rightsquigarrow \texttt{i} \to \underline{i} + 1$$
$$\texttt{a} \to \underline{a} \rightsquigarrow \texttt{a} \to \underline{a} + 1$$

$$i(\kappa_1) = \kappa_1 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$

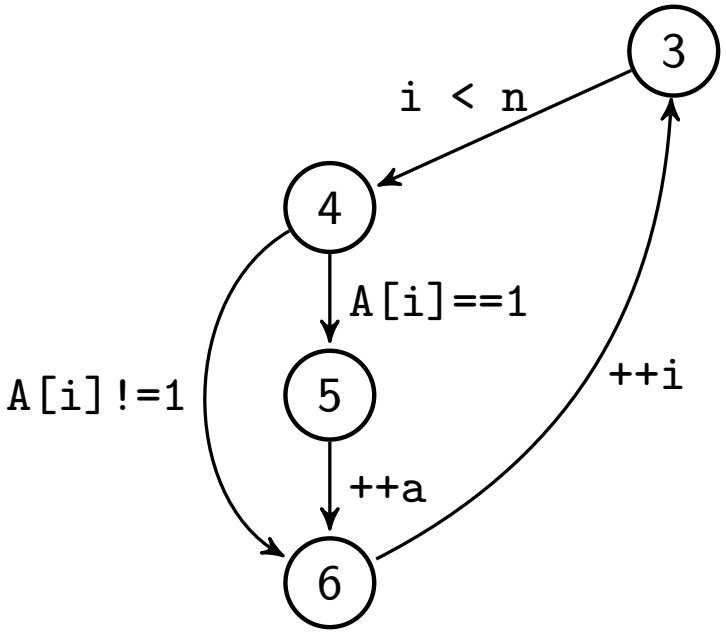
Our heuristic



$$\texttt{i} \to \underline{i} \rightsquigarrow \texttt{i} \to \underline{i} + 1$$
$$\texttt{a} \to \underline{a} \rightsquigarrow \texttt{a} \to \underline{a}$$

$$i(\kappa_1) = \kappa_1 + \underline{i} \qquad i(\kappa_2) = \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a} \qquad a(\kappa_2) = \underline{a}$$

Our heuristic

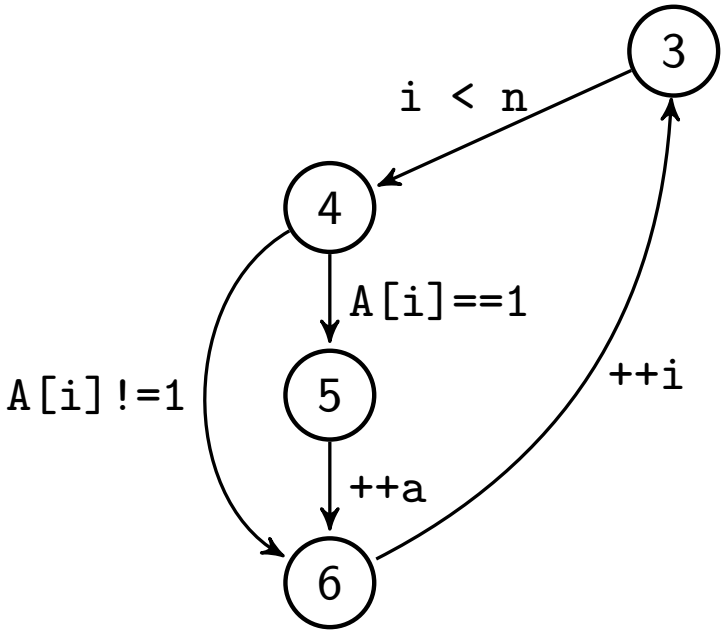


Merging counter functions.

$$i(\kappa_1) = \kappa_1 + \underline{i} \qquad i(\kappa_2) = \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a} \qquad a(\kappa_2) = \underline{a}$$

$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2 + \underline{i}$$

Our heuristic

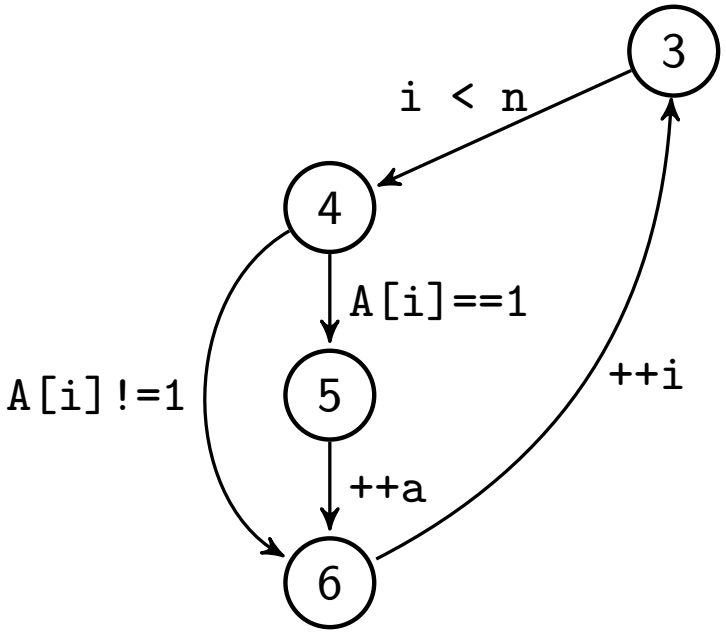


Merging counter functions.

$$i(\kappa_1) = \kappa_1 + \underline{i} \qquad i(\kappa_2) = \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a} \qquad a(\kappa_2) = \underline{a}$$

$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$

Our heuristic

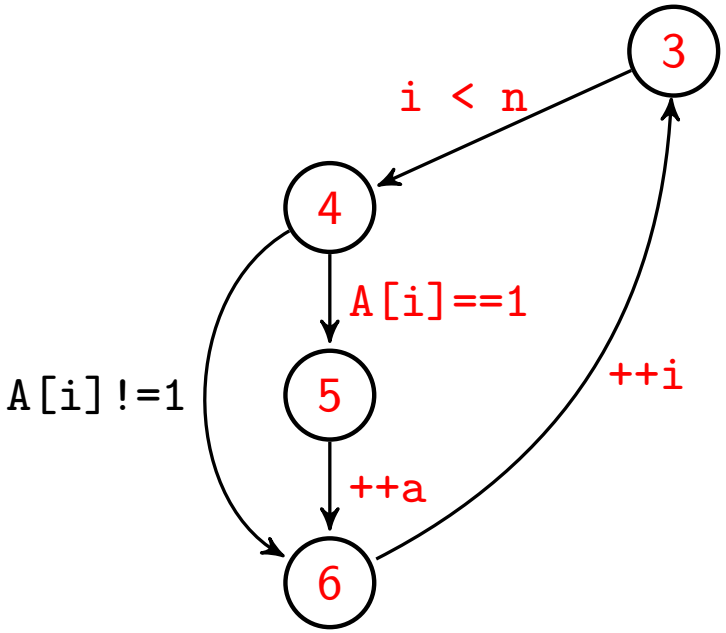


$$i(\kappa_1) = \kappa_1 + \underline{i} \qquad i(\kappa_2) = \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a} \qquad a(\kappa_2) = \underline{a}$$

$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$

$$\begin{aligned}
\varphi^{\vec{\kappa}} \equiv\ & \forall \tau_1\ (0 \le \tau_1 < \kappa_1 \rightarrow \\
& \quad \exists \tau_2\ (0 \le \tau_2 \le \kappa_2\ \wedge \\
& \qquad \tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) = 1))\ \wedge \\
& \forall \tau_2\ (0 \le \tau_2 < \kappa_2 \rightarrow \\
& \quad \exists \tau_1\ (0 \le \tau_1 \le \kappa_1\ \wedge \\
& \qquad \tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) \neq 1))
\end{aligned}$$

Our heuristic

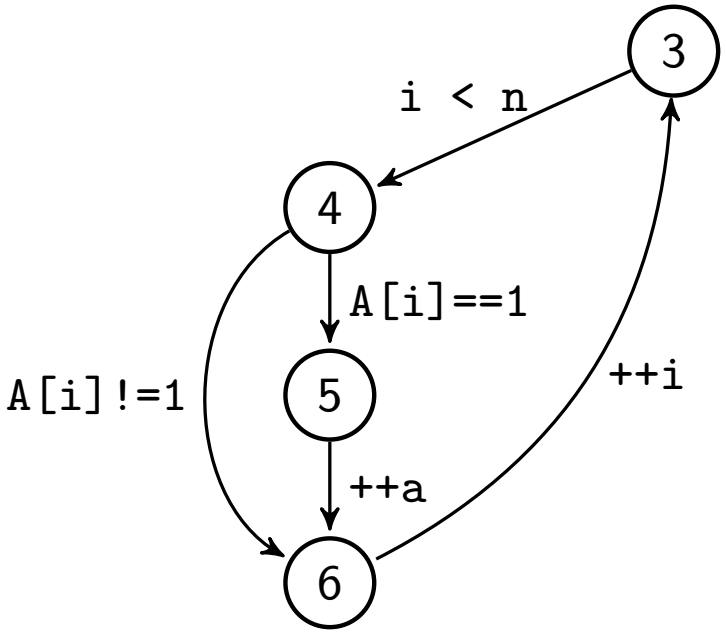


$$i(\kappa_1) = \kappa_1 + \underline{i} \qquad i(\kappa_2) = \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a} \qquad a(\kappa_2) = \underline{a}$$

$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$

$$\begin{aligned}
\varphi^{\vec{\kappa}} \equiv\ & \forall \tau_1\ (0 \le \tau_1 < \kappa_1 \rightarrow \\
& \quad \exists \tau_2\ (0 \le \tau_2 \le \kappa_2 \wedge \\
& \qquad \tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) = 1)) \wedge \\
& \forall \tau_2\ (0 \le \tau_2 < \kappa_2 \rightarrow \\
& \quad \exists \tau_1\ (0 \le \tau_1 \le \kappa_1 \wedge \\
& \qquad \tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) \neq 1))
\end{aligned}$$

Our heuristic

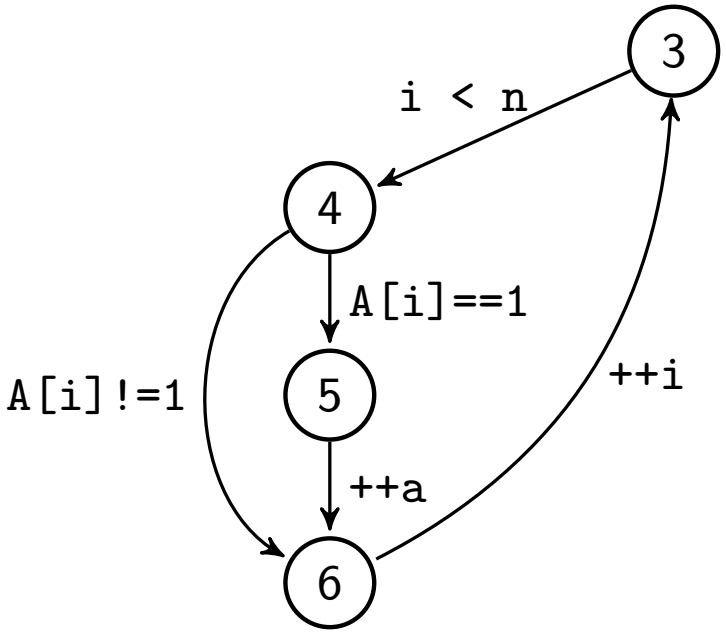


$$i(\kappa_1) = \kappa_1 + \underline{i} \qquad i(\kappa_2) = \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a} \qquad a(\kappa_2) = \underline{a}$$

$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$

$$\begin{aligned}
\varphi^{\vec{\kappa}} \equiv\ & \forall \tau_1\ (0 \leq \tau_1 < \kappa_1 \rightarrow \\
& \exists \tau_2\ (0 \leq \tau_2 \leq \kappa_2\ \wedge \\
& \qquad \tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) = 1))\ \wedge \\
& \forall \tau_2\ (0 \leq \tau_2 < \kappa_2 \rightarrow \\
& \exists \tau_1\ (0 \leq \tau_1 \leq \kappa_1\ \wedge \\
& \qquad \tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) \neq 1))
\end{aligned}$$

Our heuristic

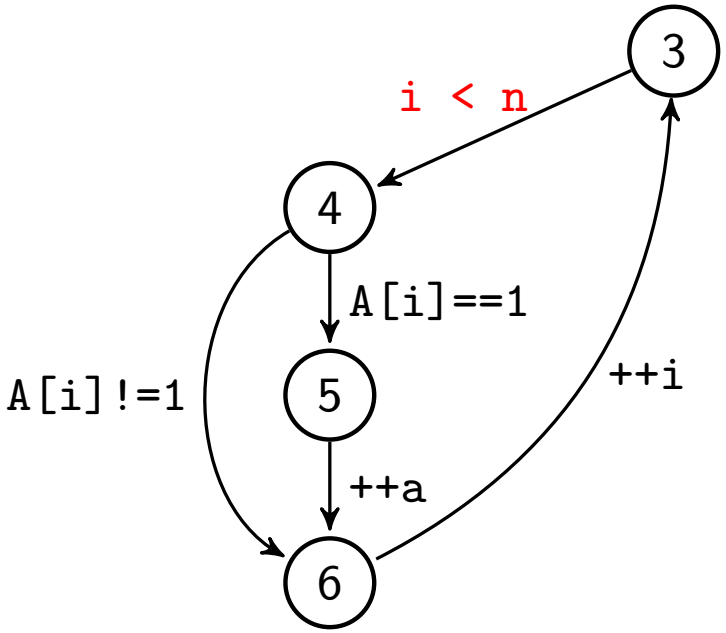


$$i(\kappa_1) = \kappa_1 + \underline{i} \qquad i(\kappa_2) = \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a} \qquad a(\kappa_2) = \underline{a}$$

$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$

$$\begin{aligned}
\varphi^{\vec{\kappa}} \equiv \forall\tau_1\ (0 \le \tau_1 < \kappa_1 \rightarrow\ & \\
& \exists\tau_2\ (0 \le \tau_2 \le \kappa_2 \wedge \\
& \qquad \tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) = 1)) \wedge \\
\forall\tau_2\ (0 \le \tau_2 < \kappa_2 \rightarrow\ & \\
& \exists\tau_1\ (0 \le \tau_1 \le \kappa_1 \wedge \\
& \qquad \tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) \neq 1))
\end{aligned}$$

Our heuristic

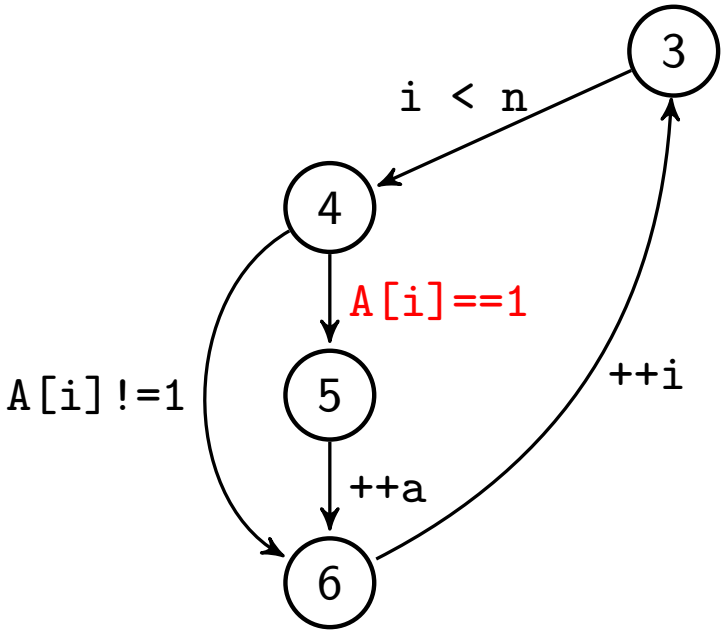


$$i(\kappa_1) = \kappa_1 + \underline{i} \qquad i(\kappa_2) = \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a} \qquad a(\kappa_2) = \underline{a}$$

$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$

$$\begin{aligned}
\varphi^{\vec{\kappa}} \equiv \forall\tau_1\ (0 \le \tau_1 < \kappa_1 \rightarrow\ & \\
& \exists\tau_2\ (0 \le \tau_2 \le \kappa_2\ \wedge \\
& \qquad \tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) = 1)) \wedge \\
\forall\tau_2\ (0 \le \tau_2 < \kappa_2 \rightarrow\ & \\
& \exists\tau_1\ (0 \le \tau_1 \le \kappa_1\ \wedge \\
& \qquad \tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) \neq 1))
\end{aligned}$$

Our heuristic

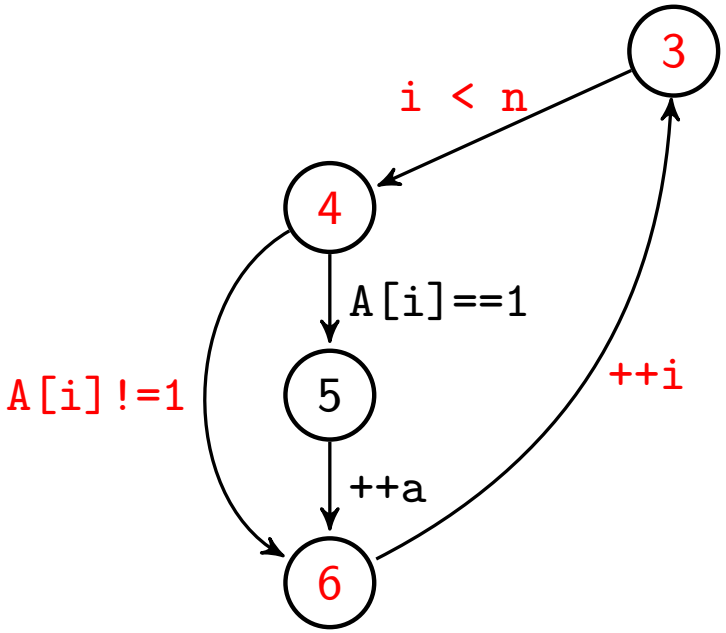


$$i(\kappa_1) = \kappa_1 + \underline{i} \qquad i(\kappa_2) = \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a} \qquad a(\kappa_2) = \underline{a}$$

$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$

$$\begin{aligned}
\varphi^{\vec{\kappa}} \equiv \forall\tau_1\ (0 \le \tau_1 < \kappa_1 \rightarrow\ & \\
\exists\tau_2\ (0 \le \tau_2 \le \kappa_2 \wedge\ & \\
\tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) = 1)) \wedge\ & \\
\forall\tau_2\ (0 \le \tau_2 < \kappa_2 \rightarrow\ & \\
\exists\tau_1\ (0 \le \tau_1 \le \kappa_1 \wedge\ & \\
\tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) \neq 1))\ &
\end{aligned}$$

Our heuristic

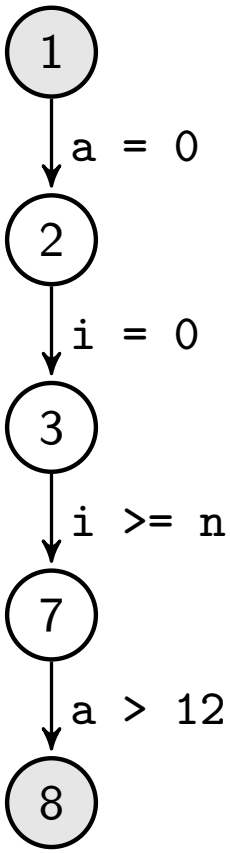


$$i(\kappa_1) = \kappa_1 + \underline{i} \qquad i(\kappa_2) = \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a} \qquad a(\kappa_2) = \underline{a}$$

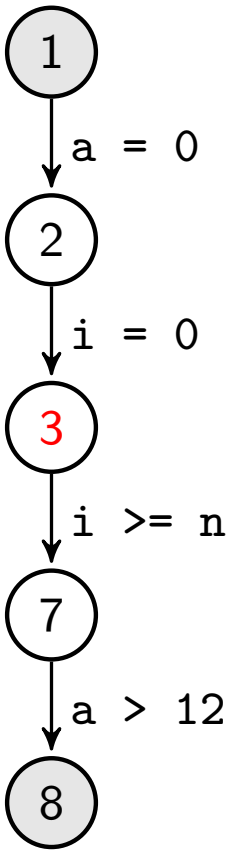
$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$

$$\begin{aligned}
\varphi^{\vec{\kappa}} \equiv \forall\tau_1\ (0 \le \tau_1 < \kappa_1 \rightarrow\ & \\
& \exists\tau_2\ (0 \le \tau_2 \le \kappa_2 \wedge \\
& \quad \tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) = 1)) \wedge \\
\forall\tau_2\ (0 \le \tau_2 < \kappa_2 \rightarrow\ & \\
& \exists\tau_1\ (0 \le \tau_1 \le \kappa_1 \wedge \\
& \quad \tau_1 + \tau_2 + \underline{i} < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2 + \underline{i}) \neq 1))
\end{aligned}$$

Our heuristic

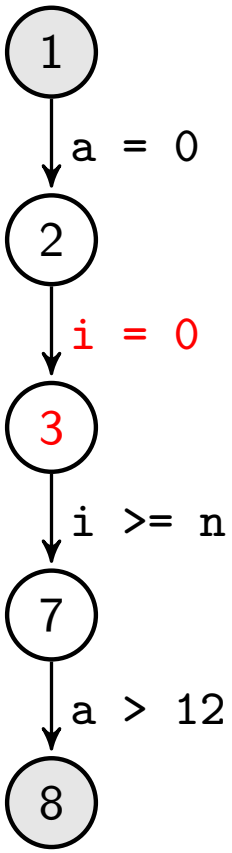


Our heuristic



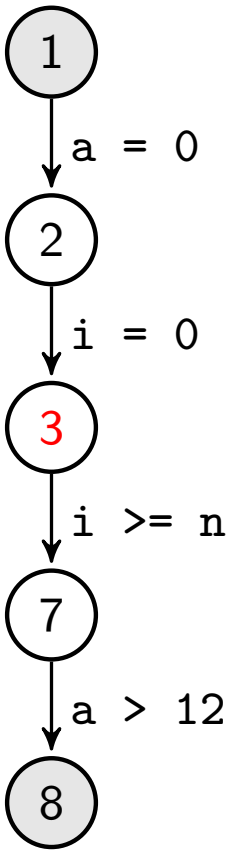
$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$
$$\varphi^{\vec{\kappa}}$$

Our heuristic



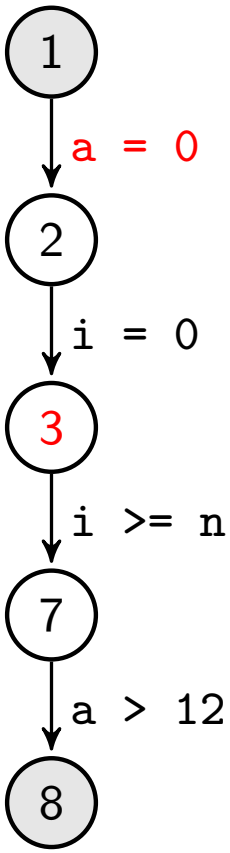
$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2 + \underline{i}$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$
$$\varphi^{\vec{\kappa}}$$

Our heuristic



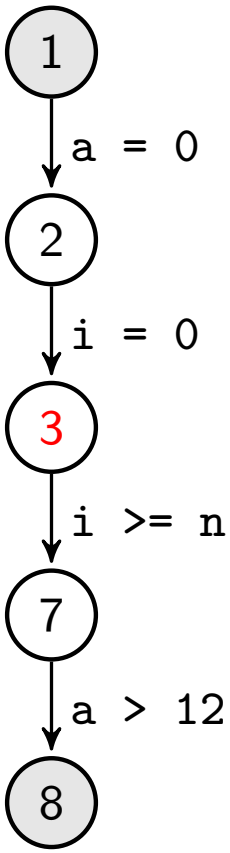
$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$
$$\varphi^{\vec{\kappa}}$$

Our heuristic



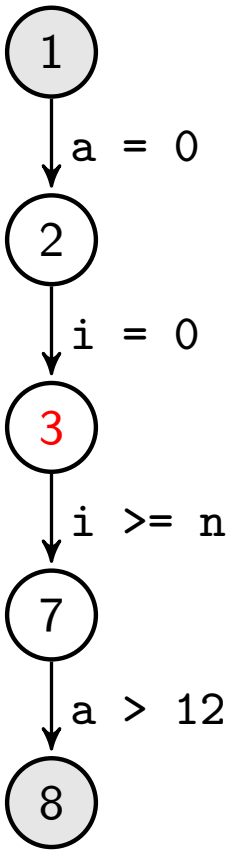
$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2$$
$$a(\kappa_1) = \kappa_1 + \underline{a}$$
$$\varphi^{\vec{\kappa}}$$

Our heuristic



$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2$$
$$a(\kappa_1) = \kappa_1$$
$$\varphi^{\vec{\kappa}}$$

Our heuristic

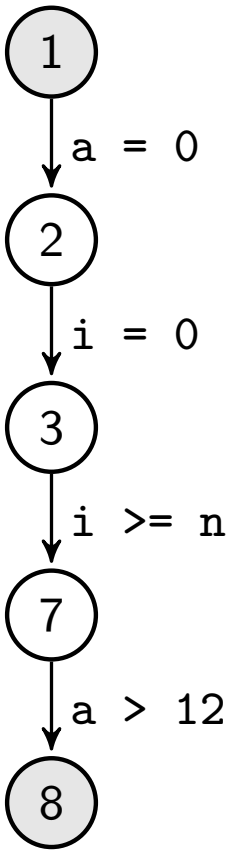


$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2$

$a(\kappa_1) = \kappa_1$

$\varphi^{\vec{\kappa}}[\underline{i}/0, \underline{a}/0]$

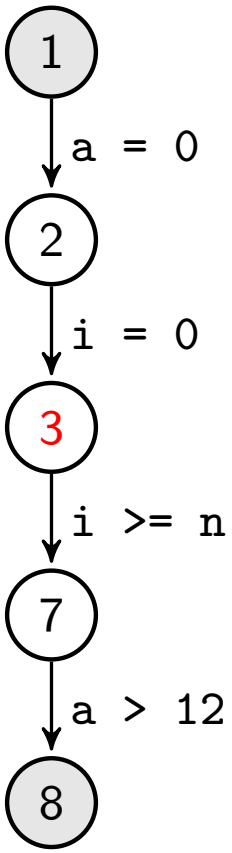
Our heuristic



$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2$$
$$a(\kappa_1) = \kappa_1$$
$$\varphi^{\vec{\kappa}}[\underline{i}/0, \underline{a}/0]$$

$$\hat{\varphi} \equiv \exists \kappa_1 \, (\kappa_1 \geq 0 \wedge \exists \kappa_2 \, (\kappa_2 \geq 0 \wedge \varphi^{\vec{\kappa}}[\underline{i}/0, \underline{a}/0] \wedge \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))$$

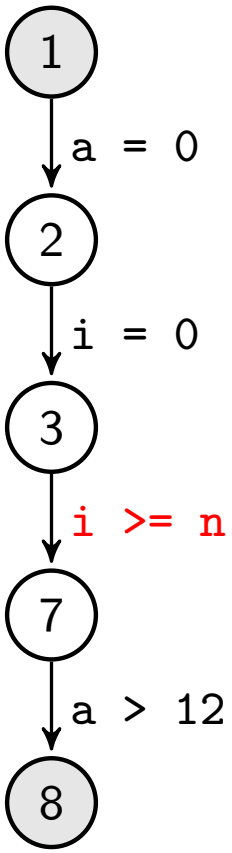
Our heuristic



$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2$$
$$a(\kappa_1) = \kappa_1$$
$$\varphi^{\vec{\kappa}}[\underline{i}/0, \underline{a}/0]$$

$$\hat{\varphi} \equiv \exists \kappa_1 \, (\kappa_1 \geq 0 \wedge \exists \kappa_2 \, (\kappa_2 \geq 0 \wedge \varphi^{\vec{\kappa}}[\underline{i}/0, \underline{a}/0] \wedge \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))$$

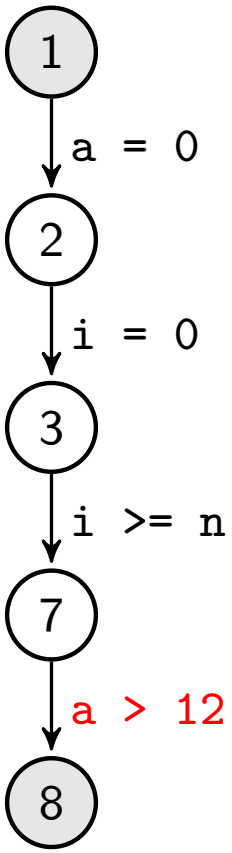
Our heuristic



$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2$$
$$a(\kappa_1) = \kappa_1$$
$$\varphi^{\vec{\kappa}}[\underline{i}/0, \underline{a}/0]$$

$$\hat{\varphi} \equiv \exists \kappa_1 \, (\kappa_1 \geq 0 \wedge \exists \kappa_2 \, (\kappa_2 \geq 0 \wedge \varphi^{\vec{\kappa}}[\underline{i}/0, \underline{a}/0] \wedge \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))$$

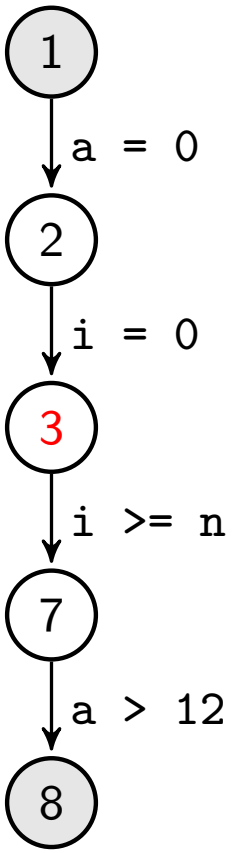
Our heuristic



$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2$$
$$a(\kappa_1) = \kappa_1$$
$$\varphi^{\vec{\kappa}}[\underline{i}/0, \underline{a}/0]$$

$$\hat{\varphi} \equiv \exists \kappa_1 \, (\kappa_1 \geq 0 \wedge \exists \kappa_2 \, (\kappa_2 \geq 0 \wedge \varphi^{\vec{\kappa}}[\underline{i}/0, \underline{a}/0] \wedge \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))$$

Our heuristic



$$i(\kappa_1, \kappa_2) = \kappa_1 + \kappa_2$$
$$a(\kappa_1) = \kappa_1$$
$$\varphi^{\vec{\kappa}}[\underline{i}/0, \underline{a}/0]$$

$$\hat{\varphi} \equiv \exists \kappa_1 \ (\kappa_1 \geq 0 \wedge \exists \kappa_2 \ (\kappa_2 \geq 0 \wedge \varphi^{\vec{\kappa}}[\underline{i}/0, \underline{a}/0] \wedge \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))$$

Usage of the heuristic

- Symbolic execution:
  - PC $\leftarrow$ *true*

Usage of the heuristic

- Symbolic execution:
  - PC $\leftarrow \hat{\varphi}$

Usage of the heuristic

- Symbolic execution:
  - PC $\leftarrow \hat{\varphi}$
- DART:
  - Initialization = random

Usage of the heuristic

- Symbolic execution:
  - PC $\leftarrow \hat{\varphi}$
- DART:
  - Initialization = model of $\hat{\varphi}$

Usage of the heuristic

- Symbolic execution:
  - PC $\leftarrow \hat{\varphi}$
- DART:
  - Initialization = model of $\hat{\varphi}$
  - Next input = model of φ

Usage of the heuristic

- Symbolic execution:
  - PC $\leftarrow \hat{\varphi}$
- DART:
  - Initialization = model of $\hat{\varphi}$
  - Next input = model of $\varphi \wedge \hat{\varphi}$

Usage of the heuristic

- Symbolic execution:
  - PC $\leftarrow \hat{\varphi}$
- DART:
  - Initialization = model of $\hat{\varphi}$
  - Next input = model of $\varphi \wedge \hat{\varphi}$
- Tools:
  - KLEE, EXE, PEX, SAGE

Z3 performance

$$
\begin{aligned}
&\exists \kappa_1 \ (\kappa_1 \geq 0 \wedge \\
&\qquad \exists \kappa_2 \ (\kappa_2 \geq 0 \wedge \\
&\qquad\qquad \forall \tau_1 \ (0 \leq \tau_1 < \kappa_1 \rightarrow \\
&\qquad\qquad\qquad \exists \tau_2 \ (0 \leq \tau_2 \leq \kappa_2 \wedge \tau_1 + \tau_2 < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2) = 1)) \wedge \\
&\qquad\qquad \forall \tau_2 \ (0 \leq \tau_2 < \kappa_2 \rightarrow \\
&\qquad\qquad\qquad \exists \tau_1 \ (0 \leq \tau_1 \leq \kappa_1 \wedge \tau_1 + \tau_2 < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2) \neq 1)) \wedge \\
&\qquad\qquad \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))
\end{aligned}
$$

Z3 performance

$$
\begin{aligned}
&\exists \kappa_1\ (\kappa_1 \geq 0 \wedge \\
&\quad \exists \kappa_2\ (\kappa_2 \geq 0 \wedge \\
&\quad\quad \forall \tau_1\ (0 \leq \tau_1 < \kappa_1 \rightarrow \\
&\quad\quad\quad \exists \tau_2\ (0 \leq \tau_2 \leq \kappa_2 \wedge \tau_1 + \tau_2 < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2) = 1)) \wedge \\
&\quad\quad \forall \tau_2\ (0 \leq \tau_2 < \kappa_2 \rightarrow \\
&\quad\quad\quad \exists \tau_1\ (0 \leq \tau_1 \leq \kappa_1 \wedge \tau_1 + \tau_2 < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2) \neq 1)) \wedge \\
&\quad\quad \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))
\end{aligned}
$$

(1) $\hat{\varphi} \longrightarrow \mathit{true} \mid \varphi(\emptyset) \vee \hat{\varphi}$

(2) $\varphi(V) \longrightarrow \gamma(V) \mid \exists x\ (0 \leq x \wedge \psi(V \cup \{x\}) \wedge \varphi(V \cup \{x\}))$

(3) $\psi(V \cup \{y\}) \longrightarrow \mathit{true} \mid \forall x\ (0 \leq x < y \rightarrow \rho(V \cup \{x, y\})) \wedge \psi(V \cup \{y\})$

(4) $\rho(V \cup \{y\}) \longrightarrow \varphi(V \cup \{y\}) \mid \exists x\ (0 \leq x \leq y \wedge \rho(V \cup \{x, y\}))$

Z3 performance

$$
\begin{aligned}
&\exists \kappa_1\ (\kappa_1 \geq 0 \wedge \\
&\quad \exists \kappa_2\ (\kappa_2 \geq 0 \wedge \\
&\qquad \forall \tau_1\ (0 \leq \tau_1 < \kappa_1 \rightarrow \\
&\qquad\quad \exists \tau_2\ (0 \leq \tau_2 \leq \kappa_2 \wedge \tau_1 + \tau_2 < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2) = 1)) \wedge \\
&\qquad \forall \tau_2\ (0 \leq \tau_2 < \kappa_2 \rightarrow \\
&\qquad\quad \exists \tau_1\ (0 \leq \tau_1 \leq \kappa_1 \wedge \tau_1 + \tau_2 < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2) \neq 1)) \wedge \\
&\qquad \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))
\end{aligned}
$$

(1) $\hat{\varphi} \longrightarrow \mathit{true} \mid \varphi(\emptyset) \vee \hat{\varphi}$

(2) $\varphi(V) \longrightarrow \gamma(V) \mid \exists x\ (0 \leq x \wedge \psi(V \cup \{x\}) \wedge \varphi(V \cup \{x\}))$

(3) $\psi(V \cup \{y\}) \longrightarrow \mathit{true} \mid \forall x\ (0 \leq x < y \rightarrow \rho(V \cup \{x, y\})) \wedge \psi(V \cup \{y\})$

(4) $\rho(V \cup \{y\}) \longrightarrow \varphi(V \cup \{y\}) \mid \exists x\ (0 \leq x \leq y \wedge \rho(V \cup \{x, y\}))$

Z3 performance

$$
\begin{aligned}
&\exists \kappa_1\ (\kappa_1 \geq 0 \wedge \\
&\quad \exists \kappa_2\ (\kappa_2 \geq 0 \wedge \\
&\quad\quad \forall \tau_1\ (0 \leq \tau_1 < \kappa_1 \rightarrow \\
&\quad\quad\quad \exists \tau_2\ (0 \leq \tau_2 \leq \kappa_2 \wedge \tau_1 + \tau_2 < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2) = 1)) \wedge \\
&\quad\quad \forall \tau_2\ (0 \leq \tau_2 < \kappa_2 \rightarrow \\
&\quad\quad\quad \exists \tau_1\ (0 \leq \tau_1 \leq \kappa_1 \wedge \tau_1 + \tau_2 < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2) \neq 1)) \wedge \\
&\quad\quad \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))
\end{aligned}
$$

(1) $\hat{\varphi} \longrightarrow \mathit{true} \mid \varphi(\emptyset) \vee \hat{\varphi}$

(2) $\varphi(V) \longrightarrow \gamma(V) \mid \exists x\ (0 \leq x \wedge \psi(V \cup \{x\}) \wedge \varphi(V \cup \{x\}))$

(3) $\psi(V \cup \{y\}) \longrightarrow \mathit{true} \mid \forall x\ (0 \leq x < y \rightarrow \rho(V \cup \{x, y\})) \wedge \psi(V \cup \{y\})$

(4) $\rho(V \cup \{y\}) \longrightarrow \varphi(V \cup \{y\}) \mid \exists x\ (0 \leq x \leq y \wedge \rho(V \cup \{x, y\}))$

Z3 performance

$$
\begin{aligned}
&\exists \kappa_1\ (\kappa_1 \geq 0 \wedge \\
&\quad \exists \kappa_2\ (\kappa_2 \geq 0 \wedge \\
&\quad\quad \forall \tau_1\ (0 \leq \tau_1 < \kappa_1 \rightarrow \\
&\quad\quad\quad \exists \tau_2\ (0 \leq \tau_2 \leq \kappa_2 \wedge \tau_1 + \tau_2 < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2) = 1)) \wedge \\
&\quad\quad \forall \tau_2\ (0 \leq \tau_2 < \kappa_2 \rightarrow \\
&\quad\quad\quad \exists \tau_1\ (0 \leq \tau_1 \leq \kappa_1 \wedge \tau_1 + \tau_2 < \underline{n} \wedge \underline{A}(\tau_1 + \tau_2) \neq 1)) \wedge \\
&\quad\quad \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))
\end{aligned}
$$

(1) $\hat{\varphi} \longrightarrow \mathit{true} \mid \varphi(\emptyset) \vee \hat{\varphi}$

(2) $\varphi(V) \longrightarrow \gamma(V) \mid \exists x\ (0 \leq x \wedge \psi(V \cup \{x\}) \wedge \varphi(V \cup \{x\}))$

(3) $\psi(V \cup \{y\}) \longrightarrow \mathit{true} \mid \forall x\ (0 \leq x < y \rightarrow \rho(V \cup \{x, y\})) \wedge \psi(V \cup \{y\})$

(4) $\rho(V \cup \{y\}) \longrightarrow \varphi(V \cup \{y\}) \mid \exists x\ (0 \leq x \leq y \wedge \rho(V \cup \{x, y\}))$

Z3 performance

$$
\begin{aligned}
&(\kappa_1 \geq 0 \wedge \kappa_1 \leq 25 \wedge \\
&\quad (\kappa_2 \geq 0 \wedge \kappa_2 \leq 25 \wedge \\
&\qquad (0 \leq 0 < \kappa_1) \rightarrow \\
&\qquad\quad (0 \leq \tau_{2,0} \leq \kappa_2 \wedge 0 + \tau_{2,0} < \underline{n} \wedge \underline{A}(0 + \tau_{2,0}) = 1)) \wedge \\
&\qquad \ldots \\
&\qquad (0 \leq 24 < \kappa_1) \rightarrow \\
&\qquad\quad (0 \leq \tau_{2,24} \leq \kappa_2 \wedge 24 + \tau_{2,24} < \underline{n} \wedge \underline{A}(24 + \tau_{2,24}) = 1)) \wedge \\
&\qquad (0 \leq 0 < \kappa_2) \rightarrow \\
&\qquad\quad (0 \leq \tau_{1,0} \leq \kappa_1 \wedge \tau_{1,0} + 0 < \underline{n} \wedge \underline{A}(\tau_{1,0} + 0) \neq 1)) \wedge \\
&\qquad \ldots \\
&\qquad (0 \leq 24 < \kappa_2) \rightarrow \\
&\qquad\quad (0 \leq \tau_{1,24} \leq \kappa_1 \wedge \tau_{1,24} + 24 < \underline{n} \wedge \underline{A}(\tau_{1,24} + 24) \neq 1)) \wedge \\
&\qquad \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))
\end{aligned}
$$

Z3 performance

$$
\begin{aligned}
&(\kappa_1 \geq 0 \wedge \kappa_1 \leq 25 \wedge \\
&\quad (\kappa_2 \geq 0 \wedge \kappa_2 \leq 25 \wedge \\
&\qquad (0 \leq 0 < \kappa_1) \rightarrow \\
&\qquad\quad (0 \leq \tau_{2,0} \leq \kappa_2 \wedge 0 + \tau_{2,0} < \underline{n} \wedge \underline{A}(0 + \tau_{2,0}) = 1)) \wedge \\
&\qquad \ldots \\
&\qquad (0 \leq 24 < \kappa_1) \rightarrow \\
&\qquad\quad (0 \leq \tau_{2,24} \leq \kappa_2 \wedge 24 + \tau_{2,24} < \underline{n} \wedge \underline{A}(24 + \tau_{2,24}) = 1)) \wedge \\
&\qquad (0 \leq 0 < \kappa_2) \rightarrow \\
&\qquad\quad (0 \leq \tau_{1,0} \leq \kappa_1 \wedge \tau_{1,0} + 0 < \underline{n} \wedge \underline{A}(\tau_{1,0} + 0) \neq 1)) \wedge \\
&\qquad \ldots \\
&\qquad (0 \leq 24 < \kappa_2) \rightarrow \\
&\qquad\quad (0 \leq \tau_{1,24} \leq \kappa_1 \wedge \tau_{1,24} + 24 < \underline{n} \wedge \underline{A}(\tau_{1,24} + 24) \neq 1)) \wedge \\
&\qquad \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))
\end{aligned}
$$

Z3 performance

$$
\begin{aligned}
&(\kappa_1 \geq 0 \wedge \kappa_1 \leq 25 \wedge \\
&\quad (\kappa_2 \geq 0 \wedge \kappa_2 \leq 25 \wedge \\
&\qquad (0 \leq 0 < \kappa_1) \rightarrow \\
&\qquad\quad (0 \leq \tau_{2,0} \leq \kappa_2 \wedge 0 + \tau_{2,0} < \underline{n} \wedge \underline{A}(0 + \tau_{2,0}) = 1)) \wedge \\
&\qquad \ldots \\
&\qquad (0 \leq 24 < \kappa_1) \rightarrow \\
&\qquad\quad (0 \leq \tau_{2,24} \leq \kappa_2 \wedge 24 + \tau_{2,24} < \underline{n} \wedge \underline{A}(24 + \tau_{2,24}) = 1)) \wedge \\
&\qquad (0 \leq 0 < \kappa_2) \rightarrow \\
&\qquad\quad (0 \leq \tau_{1,0} \leq \kappa_1 \wedge \tau_{1,0} + 0 < \underline{n} \wedge \underline{A}(\tau_{1,0} + 0) \neq 1)) \wedge \\
&\qquad \ldots \\
&\qquad (0 \leq 24 < \kappa_2) \rightarrow \\
&\qquad\quad (0 \leq \tau_{1,24} \leq \kappa_1 \wedge \tau_{1,24} + 24 < \underline{n} \wedge \underline{A}(\tau_{1,24} + 24) \neq 1)) \wedge \\
&\qquad \kappa_1 + \kappa_2 \geq \underline{n} \wedge \kappa_1 > 12))
\end{aligned}
$$

Experimental Results

Test	Pex	APC			
		Total	Build	Full	QF
Hello	5.257	0.614	0.091	0.433	0.09
HW	25.05	1.608	0.400	0.998	0.21
HWM	fail	11.00	7.338	2.748	0.92
MatrIR	95.00	1.435	0.105	1.330	-
WinDriver	35.53	0.382	0.089	0.143	0.150

- Intel® Core™ i7 CPU 920 @ 2.67GHz 2.67GHz, 6GB RAM, Windows 7 Professional 64-bit
- MS Pex 0.92.50603.1, MS Moles 1.0.0.0, MS Visual Studio 2008, MS .NET Framework v3.5 SP1
- MS Z3 SMT solver v3.2, and boost v1.42.0.

Conclusion

- The heuristic computes a formula that is a necessary condition for reaching the target. We build the formula according to the following two relaxations:
  - We relax an exact interleaving of paths through a loop.
  - And we expresses variables as functions of path counters.

Conclusion

- The heuristic computes a formula that is a necessary condition for reaching the target. We build the formula according to the following two relaxations:
  - We relax an exact interleaving of paths through a loop.
  - And we expresses variables as functions of path counters.
- Computed formulae belong to a fragment of FOL expressible by a simple grammar. In this fragment each universally quantified variable is bound to an interval with a path counter as the upper bound.

Conclusion

- The heuristic computes a formula that is a necessary condition for reaching the target. We build the formula according to the following two relaxations:
  - We relax an exact interleaving of paths through a loop.
  - And we expresses variables as functions of path counters.
- Computed formulae belong to a fragment of FOL expressible by a simple grammar. In this fragment each universally quantified variable is bound to an interval with a path counter as the upper bound.
- Z3 often performs purely on computed formulae, because of quantifiers. But structure of formulae allows to generate bounded quantifier free formulae, where Z3 performs very well.

Conclusion

- The heuristic computes a formula that is a necessary condition for reaching the target. We build the formula according to the following two relaxations:
  - We relax an exact interleaving of paths through a loop.
  - And we expresses variables as functions of path counters.
- Computed formulae belong to a fragment of FOL expressible by a simple grammar. In this fragment each universally quantified variable is bound to an interval with a path counter as the upper bound.
- Z3 often performs purely on computed formulae, because of quantifiers. But structure of formulae allows to generate bounded quantifier free formulae, where Z3 performs very well.
- We showed that results of the heuristic can be easily and directly used in tools based on either original symbolic execution or DART algorithm. And experimental results show a potential to improve performance of such tools.