Making Programs Memory Safe

Through Program Synthesis

Roland Meyer, **Jakob Tepe**, Sebastian Wolff, **01.03.2024**

Technische Universität Braunschweig

Making Programs Memory Safe

Through Program Synthesis

Roland Meyer, **Jakob Tepe**, Sebastian Wolff, **01.03.2024**

Program Synthesis

$$\models \{pre\} \quad prog \quad \{post\}$$

$$\in Progs$$

Program Synthesis

$$\models \{pre\}\ prog\ \{post\}$$

$$\in Progs$$

$Progs$ given as a Sketch:

Program Synthesis

$\models \{pre\}\ prog\ \{post\}$

$\in Progs$

$Progs$ given as a Sketch:

```
N;
x++;
N;
y = 1;    +    y = 2;
M;
```

Program Synthesis

$\models \{pre\}\ prog\ \{post\}$

$\in Progs$

N ::= x = 1 | x = 2

M ::= y++ | M;M

$Progs$ given as a Sketch:

```
N;
x++;
N;
y = 1;   +   y = 2;
M;
```

Two Problems:

1: Is synthesis possible?

Verification - Realizability Logic

Program Synthesis

$\models \{pre\}\ prog\ \{post\}$

$\in Progs$

N ::= x = 1 | x = 2

M ::= y++ | M

$Progs$ given as a Sketch:

```
x = 0;
N;
x++;
y = 1;   +   y = 2;
M;
```

Two Problems:

1: Is synthesis possible?

Verification - Realizability Logic

2: What does the solution look like?

Synthesis - Realization Logic

Realizability Logic

$$\{true\}$$

$$\{x = 2\}$$

Realizability Logic

$\{true\}$

N;

x++;

$\{x = 2\}$

Realizability Logic

$\{true\}$

N;

x++;

$\{x = 2\}$

N ::= x = 1 | x = 2

Realizability Logic

$\exists$prog $\in$

$$\left\{ \begin{array}{l} \{true\} \\ \text{N;} \\ \\ \text{x++;} \\ \{x = 2\} \end{array} \right.$$

N ::= x = 1 | x = 2

$\vDash \{true\}\text{prog}\{x = 2\}$

Realizability Logic

$\exists$prog $\in$ $\left\{ \begin{array}{l} \{true\} \\ \texttt{x = 1;} \\ \\ \texttt{x++;} \\ \{x = 2\} \end{array} \right.$

$\vDash \{true\}\text{prog}\{x = 2\}$ ✅

N ::= x = 1 | x = 2

Realizability Logic

$\exists$prog $\in$

$$\left\{ \begin{array}{l} \{true\} \\ \texttt{x = 1;} \\ \{x = 1\} \\ \texttt{x++;} \\ \{x = 2\} \end{array} \right.$$

$\models \{true\}$prog$\{x = 2\}$ ✅

N ::= x = 1 | x = 2

Realizability Logic

$\exists$prog $\in$

$\{true\}$

N;

x++;

$\{x = 2\}$

$\vDash \{true\}$prog$\{x = 2\}$ ✅

N ::= x = 1 | x = 2

Realizability Logic

$\langle true \rangle$

$\exists$prog $\in$ $\left\{ \begin{array}{l} \text{N;} \\ \\ \text{x++;} \end{array} \right.$

$\langle x = 2 \rangle$

$\vDash \{true\}\text{prog}\{x = 2\}$ ✅

N ::= x = 1 | x = 2

Realizability Logic

$\exists$prog $\in$ $\left\{ \begin{array}{l} \langle true \rangle \\ \text{N;} \\ \langle x = 1, x = 2 \rangle \\ \text{x++;} \\ \langle x = 2 \rangle \end{array} \right.$

N ::= x = 1 | x = 2

$\vDash \{true\}\text{prog}\{x = 2\}$ ✅

Realizability Logic

$\exists$prog $\in$ $\left\{ \begin{array}{l} \langle true \rangle \\ \text{N;} \\ \langle x = 1, x = 2 \rangle \\ \text{x++;} \\ \langle x = 2, x = 3 \rangle \end{array} \right.$

$\vDash \{true\}\text{prog}\{x = 2\}$ ✅

N ::= x = 1 | x = 2

Realizability Logic

$\langle \mathit{true} \rangle$

∃prog ∈ $\left\{ \begin{array}{l} \texttt{x = 1;} \quad + \quad \texttt{x = 2;} \\ \\ \texttt{x++;} \end{array} \right.$

N ::= x = 1 | x = 2

$\models \{\mathit{true}\}\mathrm{prog}\{x = 2\}$

Realizability Logic

$\exists$prog $\in$ $\left\{ \begin{array}{l} \langle true \rangle \\ \texttt{x = 1;} \quad + \quad \texttt{x = 2;} \\ \langle x = 1 \lor x = 2 \rangle \\ \texttt{x++;} \end{array} \right.$

N ::= x = 1 | x = 2

$\models \{true\}\text{prog}\{x = 2\}$

Realizability Logic

$\exists$prog $\in$ $\left\{ \begin{array}{l} \langle true \rangle \\ \texttt{x = 1;} \quad + \quad \texttt{x = 2;} \\ \langle x = 1 \lor x = 2 \rangle \\ \texttt{x++;} \\ \langle x = 2 \lor x = 3 \rangle \end{array} \right.$

N ::= x = 1 | x = 2

$\models \{true\}$prog$\{x = 2\}$

Realizability Logic

$\exists$prog $\in$ $\left\{ \begin{array}{l} \langle true \rangle \\ \texttt{x = 1;} \quad + \quad \texttt{x = 2;} \\ \langle x = 1 \lor x = 2 \rangle \\ \texttt{x++;} \\ \langle x = 2 \lor x = 3 \rangle \end{array} \right.$

$\vDash \{true\}\text{prog}\{x = 2\}$ ✗

N ::= x = 1 | x = 2

Realizability Logic

$\langle true \rangle$

$\exists$prog $\in$ $\left\{ \begin{array}{l} \text{N;} \\ \\ \text{x++;} \quad + \quad \text{skip;} \end{array} \right.$

N ::= x = 1 | x = 2

$\models \{true\}\text{prog}\{x = 2\}$

Realizability Logic

$\exists$prog $\in$ $\left\{ \begin{array}{l} \langle true \rangle \\ \text{N;} \\ \langle x = 1, x = 2 \rangle \\ \text{x++;} \quad + \quad \text{skip;} \end{array} \right.$

N ::= x = 1 | x = 2

$\vDash \{true\}\text{prog}\{x = 2\}$

Realizability Logic

$\exists \text{prog} \in \left\{ \begin{array}{l} \langle true \rangle \\ \text{N}; \\ \langle x = 1, x = 2 \rangle \\ \text{x++;} \quad + \quad \text{skip;} \\ \langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle \end{array} \right.$

$\vDash \{true\}\text{prog}\{x = 2\}$

N ::= x = 1 | x = 2

Realizability Logic

$\exists$prog $\in$

$\vDash \{true\}\mathrm{prog}\{x = 2\}$ ✗

$$\left\{\begin{array}{l}\langle true \rangle \\ \mathsf{N}; \\ \langle x = 1, x = 2 \rangle \\ \mathsf{x{+}{+};} \quad + \quad \mathsf{skip;} \\ \langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle\end{array}\right.$$

N ::= x = 1 | x = 2

Realizability Logic

$\exists$prog $\in$ $\left\{ \begin{array}{l} \langle true \rangle \\ \text{x = 1;} \quad + \quad \text{x = 2;} \\ \\ \text{N;} \end{array} \right.$

N ::= x++ | skip

$\models \{true\}\text{prog}\{x = 2\}$

Realizability Logic

$$\exists \text{prog} \in \left\{ \begin{array}{l} \langle true \rangle \\ \text{x = 1;} \quad + \quad \text{x = 2;} \\ \langle x = 1 \vee x = 2 \rangle \\ \text{N;} \end{array} \right.$$

N ::= x++ | skip

$$\vDash \{true\}\text{prog}\{x = 2\}$$

Realizability Logic

$\exists$prog $\in$

$\models \{true\}\text{prog}\{x = 2\}$

$\langle true \rangle$

x = 1; **+** x = 2;

$\langle x = 1 \vee x = 2 \rangle$

N;

$\langle x = 2 \vee x = 3, x = 1 \vee x = 2 \rangle$

N ::= x++ | skip

Realizability Logic

$\exists$prog $\in$

$\models \{true\}\text{prog}\{x = 2\}$ ❌

$\langle true \rangle$

x = 1; **+** x = 2;

$\langle x = 1 \vee x = 2 \rangle$

N;

$\langle x = 2 \vee x = 3, x = 1 \vee x = 2 \rangle$

N ::= x++ | skip

Realizability Logic

$\langle true \rangle$

$\exists$prog $\in$ $\left\{ \begin{array}{l} \text{M;} \\ \\ \text{N;} \end{array} \right.$

M ::= x = 1 | x = 2

N ::= x++ | skip

$\vDash \{true\}\text{prog}\{x = 2\}$

Realizability Logic

$$\exists \text{prog} \in \left\{ \begin{array}{l} \langle true \rangle \\ \text{M;} \\ \langle x = 1, x = 2 \rangle \\ \text{N;} \end{array} \right.$$

$$\vDash \{true\}\text{prog}\{x = 2\}$$

M ::= x = 1 | x = 2

N ::= x++ | skip

Realizability Logic

$\exists$prog $\in$

$\langle \mathit{true} \rangle$

M;

$\langle x = 1, x = 2 \rangle$

N;

$\langle x = 1, x = 2, x = 3 \rangle$

$\vDash \{\mathit{true}\}\text{prog}\{x = 2\}$

M ::= x = 1 | x = 2

N ::= x++ | skip

Realizability Logic

$\exists$prog $\in$

$\langle \mathit{true} \rangle$
M;
$\langle x = 1, x = 2 \rangle$
N;
$\langle x = 1, x = 2, x = 3 \rangle$

$\vDash \{\mathit{true}\}\mathrm{prog}\{x = 2\}$ ✅

M ::= x = 1 | x = 2

N ::= x++ | skip

Realizability Logic

$\exists$prog $\in$

$$\left\{ \begin{array}{l} \langle true \rangle \\ \text{M;} \\ \langle x = 1, x = 2 \rangle \\ \text{N;} \\ \langle x = 1, x = 2, x = 3 \rangle \end{array} \right.$$

M ::= x = 1 | x = 2

N ::= x++ | skip

$\models \{true\}$prog$\{x = 2\}$ ✅

What semantics?

Realizability Logic

Set of predicates

$$\models_a \langle R \rangle \text{sketch} \langle S \rangle \qquad \Leftrightarrow$$

Realizability Logic

Set of predicates

$\vDash_a \langle R \rangle \text{sketch} \langle S \rangle \quad \Leftrightarrow$

$\vDash_a \langle true \rangle$ M;N $\langle x = 1, x = 2, x = 3 \rangle$

M ::= x = 1 | x = 2

N ::= x++ | skip

Realizability Logic

Set of predicates

$\vDash_a \langle R \rangle \text{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.$

$\vDash_a \langle true \rangle$ M;N $\langle x = 1, x = 2, x = 3 \rangle$

M ::= x = 1 | x = 2

N ::= x++ | skip

Realizability Logic

Set of predicates

$\vDash_a \langle R \rangle \text{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S . \exists r \in R . \exists \text{prog} \in drv(\text{sketch}) .$

$\vDash_a \langle true \rangle$ M;N $\langle x = 1, x = 2, x = 3 \rangle$

M ::= x = 1 | x = 2

N ::= x++ | skip

Realizability Logic

Set of predicates

$\vDash_a \langle R \rangle \text{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \text{prog} \in drv(\text{sketch}).\ \vDash_d \{r\}\text{prog}\{s\}$

$\vDash_a \langle true \rangle$ M;N $\langle x = 1, x = 2, x = 3 \rangle$

M ::= x = 1 | x = 2

N ::= x++ | skip

Realizability Logic

Set of predicates

$\vDash_a \langle R \rangle \text{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S . \exists r \in R . \exists \text{prog} \in drv(\text{sketch}) . \vDash_d \{r\} \text{prog} \{s\}$

demonic (standard Hoare)

$\vDash_a \langle true \rangle$ M;N $\langle x = 1, x = 2, x = 3 \rangle$

M ::= x = 1 | x = 2

N ::= x++ | skip

Realizability Logic

Set of predicates

$$\vDash_a \langle R \rangle \text{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \text{prog} \in drv(\text{sketch}).\ \vDash_d \{r\}\text{prog}\{s\}$$

angelic

demonic (standard Hoare)

$$\vDash_a \langle true \rangle \quad \text{M;N} \quad \langle x = 1, x = 2, x = 3 \rangle$$

M ::= x = 1 | x = 2

N ::= x++ | skip

Realizability Logic

$\langle true \rangle$

N

x++; **+** skip;

N ::= x = 1 | x = 2

Realizability Logic

$$(\textbf{COM})\ \frac{}{\vdash_a \langle \mathit{true} \rangle \texttt{x = 1;} \langle x = 1 \rangle}$$

$\langle \mathit{true} \rangle$

N

x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\text{(ANG)}\ \dfrac{\text{(COM)}\ \dfrac{}{\vdash_a \langle true \rangle \mathtt{x\ =\ 1;} \langle x = 1 \rangle}}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1 \rangle}$$

$\langle true \rangle$

N

x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\text{(ANG)}\ \dfrac{\text{(COM)}\ \dfrac{}{\vdash_a \langle true \rangle \texttt{x = 1;} \langle x = 1 \rangle} \qquad \dfrac{}{\vdash_a \langle true \rangle \texttt{x = 2;} \langle x = 2 \rangle}\ \text{(COM)}}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1 \rangle}$$

$\langle true \rangle$

N

x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\text{(ANG)}\ \dfrac{\text{(COM)}\ \dfrac{}{\vdash_a \langle true \rangle \texttt{x = 1;} \langle x = 1 \rangle}}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1 \rangle} \qquad \dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 2;} \langle x = 2 \rangle}\ \text{(COM)}}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 2 \rangle}\ \text{(ANG)}$$

$\langle true \rangle$

N

x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$(\text{ANG})\ \dfrac{(\text{COM})\ \dfrac{}{\vdash_a \langle true \rangle \texttt{x = 1;} \langle x = 1 \rangle}}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1 \rangle} \qquad \dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 2;} \langle x = 2 \rangle}\ (\text{COM})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 2 \rangle}\ (\text{ANG})$$

$\langle true \rangle$

N

x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 1;} \langle x = 1 \rangle}\ (\text{COM})}{\vdash_a \langle true \rangle \, \mathsf{N} \, \langle x = 1 \rangle}\ (\text{ANG}) \qquad \dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 2;} \langle x = 2 \rangle}\ (\text{COM})}{\vdash_a \langle true \rangle \, \mathsf{N} \, \langle x = 2 \rangle}\ (\text{ANG})$$

$$\dfrac{\vdash_a \langle true \rangle \, \mathsf{N} \, \langle x = 1 \rangle \qquad \vdash_a \langle true \rangle \, \mathsf{N} \, \langle x = 2 \rangle}{\vdash_a \langle true \rangle \, \mathsf{N} \, \langle x = 1 \underline{,}\ x = 2 \rangle}\ (\text{GATHER})$$

1️⃣

$\langle true \rangle$

N

$\langle x = 1 \underline{,}\ x = 2 \rangle$

x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{}{\vdash_a \langle true\rangle \texttt{x = 1;} \langle x = 1\rangle}\ (\text{COM})}{\vdash_a \langle true\rangle \, N \, \langle x = 1\rangle}\ (\text{ANG}) \qquad \dfrac{\dfrac{}{\vdash_a \langle true\rangle \texttt{x = 2;} \langle x = 2\rangle}\ (\text{COM})}{\vdash_a \langle true\rangle \, N \, \langle x = 2\rangle}\ (\text{ANG})$$

$$\text{(GATHER)}\ \ \vdash_a \langle true\rangle \, N \, \langle x = 1, x = 2\rangle$$

1

$\langle true\rangle$

N

$\langle x = 1, x = 2\rangle$

x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 1;} \langle x = 1 \rangle}\,(\text{COM})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1 \rangle}\,(\text{ANG}) \qquad \dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 2;} \langle x = 2 \rangle}\,(\text{COM})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 2 \rangle}\,(\text{ANG})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1, x = 2 \rangle}\,(\text{GATHER})$$

1

$$(\text{COM})\ \dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{x++;} \langle x = 2 \rangle}$$

$\langle true \rangle$

N

$\langle x = 1, x = 2 \rangle$

x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 1;} \langle x = 1 \rangle}\,(\text{COM})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1 \rangle}\,(\text{ANG}) \qquad \dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 2;} \langle x = 2 \rangle}\,(\text{COM})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 2 \rangle}\,(\text{ANG})$$

$$\dfrac{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1 \rangle \qquad \vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 2 \rangle}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1, x = 2 \rangle}\,(\text{GATHER})$$

1

$$(\text{COM})\,\dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{x++;} \langle x = 2 \rangle} \qquad \dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{skip;} \langle x = 1 \rangle}\,(\text{COM})$$

$\langle true \rangle$

N

$\langle x = 1, x = 2 \rangle$

x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 1;} \langle x = 1 \rangle}\ (\text{COM})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1 \rangle}\ (\text{ANG}) \qquad \dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 2;} \langle x = 2 \rangle}\ (\text{COM})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 2 \rangle}\ (\text{ANG})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1, x = 2 \rangle}\ (\text{GATHER}) \quad 1$$

$$\dfrac{\dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{x++;} \langle x = 2 \rangle}\ (\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{skip;} \langle x = 1 \rangle}\ (\text{COM})}{\vdash_a \langle x = 1 \rangle \texttt{x++;} \ + \ \texttt{skip;} \langle x = 1 \lor x = 2 \rangle}\ (\text{DEM}) \quad 2$$

$\langle true \rangle$

N

$\langle x = 1, x = 2 \rangle$

x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 1;} \langle x = 1 \rangle}\ (\text{COM})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1 \rangle}\ (\text{ANG}) \qquad \dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 2;} \langle x = 2 \rangle}\ (\text{COM})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 2 \rangle}\ (\text{ANG})$$

$$\dfrac{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1 \rangle \qquad \vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 2 \rangle}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1, x = 2 \rangle}\ (\text{GATHER}) \quad \boxed{1}$$

$$\dfrac{\dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{x++;} \langle x = 2 \rangle}\ (\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{skip;} \langle x = 1 \rangle}\ (\text{COM})}{\vdash_a \langle x = 1 \rangle \texttt{x++;} + \texttt{skip;} \langle x = 1 \vee x = 2 \rangle}\ (\text{DEM}) \quad \boxed{2}$$

$\langle true \rangle$

N

$\langle x = 1, x = 2 \rangle$

x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 1;} \langle x = 1 \rangle}\ (\text{COM})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1 \rangle}\ (\text{ANG}) \qquad \dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 2;} \langle x = 2 \rangle}\ (\text{COM})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 2 \rangle}\ (\text{ANG})}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1,\ x = 2 \rangle}\ (\text{GATHER}) \quad 1$$

$$\dfrac{\dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{x++;} \langle x = 2 \rangle}\ (\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{skip;} \langle x = 1 \rangle}\ (\text{COM})}{\vdash_a \langle x = 1 \rangle \texttt{x++;} + \texttt{skip;} \langle x = 1 \lor x = 2 \rangle}\ (\text{DEM}) \quad 2$$

$$\dfrac{}{\vdash_a \langle x = 2 \rangle \texttt{x++;} \langle x = 3 \rangle}\ (\text{COM})$$

$\langle true \rangle$
N
$\langle x = 1,\ x = 2 \rangle$
x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{\dfrac{}{\vdash_a \langle true\rangle \texttt{x = 1;} \langle x = 1\rangle}\,(\text{COM})}{\vdash_a \langle true\rangle\, \mathsf{N}\, \langle x = 1\rangle}\,(\text{ANG}) \qquad \dfrac{\dfrac{}{\vdash_a \langle true\rangle \texttt{x = 2;} \langle x = 2\rangle}\,(\text{COM})}{\vdash_a \langle true\rangle\, \mathsf{N}\, \langle x = 2\rangle}\,(\text{ANG})}{\vdash_a \langle true\rangle\, \mathsf{N}\, \langle x = 1, x = 2\rangle}\,(\text{GATHER})$$

1

$$\dfrac{\dfrac{}{\vdash_a \langle x = 1\rangle \texttt{x++;} \langle x = 2\rangle}\,(\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 1\rangle \texttt{skip;} \langle x = 1\rangle}\,(\text{COM})}{\vdash_a \langle x = 1\rangle \texttt{x++;} + \texttt{skip;} \langle x = 1 \vee x = 2\rangle}\,(\text{DEM})$$

2

$$\dfrac{}{\vdash_a \langle x = 2\rangle \texttt{x++;} \langle x = 3\rangle}\,(\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 2\rangle \texttt{skip;} \langle x = 2\rangle}\,(\text{COM})$$

$\langle true\rangle$
N
$\langle x = 1, x = 2\rangle$
x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{\overline{\vdash_a \langle true\rangle \texttt{x = 1;} \langle x = 1\rangle}\ (\text{COM})}{\vdash_a \langle true\rangle\, \mathsf{N}\, \langle x = 1\rangle}\ (\text{ANG}) \qquad \dfrac{\overline{\vdash_a \langle true\rangle \texttt{x = 2;} \langle x = 2\rangle}\ (\text{COM})}{\vdash_a \langle true\rangle\, \mathsf{N}\, \langle x = 2\rangle}\ (\text{ANG})}{\vdash_a \langle true\rangle\, \mathsf{N}\, \langle x = 1, x = 2\rangle}\ (\text{GATHER}) \quad 1$$

$$\dfrac{\overline{\vdash_a \langle x = 1\rangle \texttt{x++;} \langle x = 2\rangle}\ (\text{COM}) \qquad \overline{\vdash_a \langle x = 1\rangle \texttt{skip;} \langle x = 1\rangle}\ (\text{COM})}{\vdash_a \langle x = 1\rangle \texttt{x++;} + \texttt{skip;} \langle x = 1 \vee x = 2\rangle}\ (\text{DEM}) \quad 2$$

$$\dfrac{\overline{\vdash_a \langle x = 2\rangle \texttt{x++;} \langle x = 3\rangle}\ (\text{COM}) \qquad \overline{\vdash_a \langle x = 2\rangle \texttt{skip;} \langle x = 2\rangle}\ (\text{COM})}{\vdash_a \langle x = 2\rangle \texttt{x++;} + \texttt{skip;} \langle x = 2 \vee x = 3\rangle}\ (\text{DEM}) \quad 3$$

$\langle true\rangle$
N
$\langle x = 1, x = 2\rangle$
x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{}{\vdash_a \langle true\rangle \texttt{x = 1;} \langle x = 1\rangle}\ \text{(COM)}}{\vdash_a \langle true\rangle\ \mathsf{N}\ \langle x = 1\rangle}\ \text{(ANG)} \qquad \dfrac{\dfrac{}{\vdash_a \langle true\rangle \texttt{x = 2;} \langle x = 2\rangle}\ \text{(COM)}}{\vdash_a \langle true\rangle\ \mathsf{N}\ \langle x = 2\rangle}\ \text{(ANG)}$$

$$\text{(GATHER)}\ \vdash_a \langle true\rangle\ \mathsf{N}\ \langle x = 1, x = 2\rangle \quad \boxed{1}$$

$$\text{(DEM)}\ \dfrac{\dfrac{}{\vdash_a \langle x = 1\rangle \texttt{x++;} \langle x = 2\rangle}\ \text{(COM)} \qquad \dfrac{}{\vdash_a \langle x = 1\rangle \texttt{skip;} \langle x = 1\rangle}\ \text{(COM)}}{\vdash_a \langle x = 1\rangle \texttt{x++;} + \texttt{skip;} \langle x = 1 \lor x = 2\rangle} \quad \boxed{2}$$

$$\text{(DEM)}\ \dfrac{\dfrac{}{\vdash_a \langle x = 2\rangle \texttt{x++;} \langle x = 3\rangle}\ \text{(COM)} \qquad \dfrac{}{\vdash_a \langle x = 2\rangle \texttt{skip;} \langle x = 2\rangle}\ \text{(COM)}}{\vdash_a \langle x = 2\rangle \texttt{x++;} + \texttt{skip;} \langle x = 2 \lor x = 3\rangle} \quad \boxed{3}$$

$\langle true\rangle$
N
$\langle x = 1, x = 2\rangle$
x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{\dfrac{}{\vdash_a \langle true\rangle \texttt{x = 1;} \langle x = 1\rangle}\ (\text{COM})}{\vdash_a \langle true\rangle\ \mathsf{N}\ \langle x = 1\rangle}\ (\text{ANG}) \qquad \dfrac{\dfrac{}{\vdash_a \langle true\rangle \texttt{x = 2;} \langle x = 2\rangle}\ (\text{COM})}{\vdash_a \langle true\rangle\ \mathsf{N}\ \langle x = 2\rangle}\ (\text{ANG})}{\vdash_a \langle true\rangle\ \mathsf{N}\ \langle x = 1,\ x = 2\rangle}\ (\text{GATHER}) \quad 1$$

$$\dfrac{\dfrac{}{\vdash_a \langle x = 1\rangle \texttt{x++;} \langle x = 2\rangle}\ (\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 1\rangle \texttt{skip;} \langle x = 1\rangle}\ (\text{COM})}{\vdash_a \langle x = 1\rangle \texttt{x++;} + \texttt{skip;} \langle x = 1 \vee x = 2\rangle}\ (\text{DEM}) \quad 2$$

$$\dfrac{\dfrac{}{\vdash_a \langle x = 2\rangle \texttt{x++;} \langle x = 3\rangle}\ (\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 2\rangle \texttt{skip;} \langle x = 2\rangle}\ (\text{COM})}{\vdash_a \langle x = 2\rangle \texttt{x++;} + \texttt{skip;} \langle x = 2 \vee x = 3\rangle}\ (\text{DEM}) \quad 3$$

2

$\langle true\rangle$
N
$\langle x = 1,\ x = 2\rangle$
x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 1;} \langle x = 1 \rangle}\,(\text{COM})}{\vdash_a \langle true \rangle\ \mathsf{N}\ \langle x = 1 \rangle}\,(\text{ANG}) \qquad \dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 2;} \langle x = 2 \rangle}\,(\text{COM})}{\vdash_a \langle true \rangle\ \mathsf{N}\ \langle x = 2 \rangle}\,(\text{ANG})}{\vdash_a \langle true \rangle\ \mathsf{N}\ \langle x = 1, x = 2 \rangle}\,(\text{GATHER}) \quad 1$$

$$(\text{DEM})\ \dfrac{\dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{x++;} \langle x = 2 \rangle}\,(\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{skip;} \langle x = 1 \rangle}\,(\text{COM})}{\vdash_a \langle x = 1 \rangle \texttt{x++;}\ +\ \texttt{skip;} \langle x = 1 \vee x = 2 \rangle} \quad 2$$

$$(\text{DEM})\ \dfrac{\dfrac{}{\vdash_a \langle x = 2 \rangle \texttt{x++;} \langle x = 3 \rangle}\,(\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 2 \rangle \texttt{skip;} \langle x = 2 \rangle}\,(\text{COM})}{\vdash_a \langle x = 2 \rangle \texttt{x++;}\ +\ \texttt{skip;} \langle x = 2 \vee x = 3 \rangle} \quad 3$$

2 3

$\langle true \rangle$
N
$\langle x = 1, x = 2 \rangle$
x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$
\dfrac{
  \dfrac{
    \dfrac{}{\vdash_a \langle \mathit{true} \rangle \texttt{x = 1;} \langle x = 1 \rangle}\,(\text{COM})
  }{\vdash_a \langle \mathit{true} \rangle\, \mathsf{N}\, \langle x = 1 \rangle}\,(\text{ANG})
  \qquad
  \dfrac{
    \dfrac{}{\vdash_a \langle \mathit{true} \rangle \texttt{x = 2;} \langle x = 2 \rangle}\,(\text{COM})
  }{\vdash_a \langle \mathit{true} \rangle\, \mathsf{N}\, \langle x = 2 \rangle}\,(\text{ANG})
}{\vdash_a \langle \mathit{true} \rangle\, \mathsf{N}\, \langle x = 1,\ x = 2 \rangle}\,(\text{GATHER}) \quad \boxed{1}
$$

$$
(\text{DEM})\,\dfrac{
  \dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{x++;} \langle x = 2 \rangle}\,(\text{COM})
  \qquad
  \dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{skip;} \langle x = 1 \rangle}\,(\text{COM})
}{\vdash_a \langle x = 1 \rangle \texttt{x++;} \;+\; \texttt{skip;} \langle x = 1 \vee x = 2 \rangle} \quad \boxed{2}
$$

$$
(\text{DEM})\,\dfrac{
  \dfrac{}{\vdash_a \langle x = 2 \rangle \texttt{x++;} \langle x = 3 \rangle}\,(\text{COM})
  \qquad
  \dfrac{}{\vdash_a \langle x = 2 \rangle \texttt{skip;} \langle x = 2 \rangle}\,(\text{COM})
}{\vdash_a \langle x = 2 \rangle \texttt{x++;} \;+\; \texttt{skip;} \langle x = 2 \vee x = 3 \rangle} \quad \boxed{3}
$$

$\boxed{2}$ $\boxed{3}$

$\langle \mathit{true} \rangle$
N
$\langle x = 1,\ x = 2 \rangle$
x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\textbf{(GATHER)}\ \dfrac{\textbf{(ANG)}\ \dfrac{\textbf{(COM)}\ \dfrac{}{\vdash_a \langle true \rangle \texttt{x = 1;} \langle x = 1 \rangle}}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1 \rangle} \qquad \textbf{(ANG)}\ \dfrac{\textbf{(COM)}\ \dfrac{}{\vdash_a \langle true \rangle \texttt{x = 2;} \langle x = 2 \rangle}}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 2 \rangle}}{\vdash_a \langle true \rangle\, \mathsf{N}\, \langle x = 1, x = 2 \rangle}\ \boxed{1}$$

$$\textbf{(DEM)}\ \dfrac{\textbf{(COM)}\ \dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{x++;} \langle x = 2 \rangle} \qquad \textbf{(COM)}\ \dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{skip;} \langle x = 1 \rangle}}{\vdash_a \langle x = 1 \rangle \texttt{x++;} + \texttt{skip;} \langle x = 1 \vee x = 2 \rangle}\ \boxed{2}$$

$$\textbf{(DEM)}\ \dfrac{\textbf{(COM)}\ \dfrac{}{\vdash_a \langle x = 2 \rangle \texttt{x++;} \langle x = 3 \rangle} \qquad \textbf{(COM)}\ \dfrac{}{\vdash_a \langle x = 2 \rangle \texttt{skip;} \langle x = 2 \rangle}}{\vdash_a \langle x = 2 \rangle \texttt{x++;} + \texttt{skip;} \langle x = 2 \vee x = 3 \rangle}\ \boxed{3}$$

$$\textbf{(GATHER)}\ \dfrac{\boxed{2} \qquad \boxed{3}}{\vdash_a \langle x = 1, x = 2 \rangle \texttt{x++;} + \texttt{skip;} \langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle}\ \boxed{4}$$

$\langle true \rangle$
N
$\langle x = 1, x = 2 \rangle$
x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$
\text{(GATHER)}\;\dfrac{\text{(ANG)}\;\dfrac{\text{(COM)}\;\dfrac{}{\vdash_a \langle \mathit{true}\rangle \mathtt{x = 1;} \langle x = 1\rangle}}{\vdash_a \langle \mathit{true}\rangle \, N \, \langle x = 1\rangle} \qquad \dfrac{\dfrac{}{\vdash_a \langle \mathit{true}\rangle \mathtt{x = 2;} \langle x = 2\rangle}\;\text{(COM)}}{\vdash_a \langle \mathit{true}\rangle \, N \, \langle x = 2\rangle}\;\text{(ANG)}}{\vdash_a \langle \mathit{true}\rangle \, N \, \langle x = 1, x = 2\rangle}\;\boxed{1}
$$

$$
\text{(DEM)}\;\dfrac{\text{(COM)}\;\dfrac{}{\vdash_a \langle x = 1\rangle \mathtt{x{+}{+};} \langle x = 2\rangle} \qquad \dfrac{}{\vdash_a \langle x = 1\rangle \mathtt{skip;} \langle x = 1\rangle}\;\text{(COM)}}{\vdash_a \langle x = 1\rangle \mathtt{x{+}{+};} \; + \; \mathtt{skip;} \langle x = 1 \lor x = 2\rangle}\;\boxed{2}
$$

$$
\text{(DEM)}\;\dfrac{\text{(COM)}\;\dfrac{}{\vdash_a \langle x = 2\rangle \mathtt{x{+}{+};} \langle x = 3\rangle} \qquad \dfrac{}{\vdash_a \langle x = 2\rangle \mathtt{skip;} \langle x = 2\rangle}\;\text{(COM)}}{\vdash_a \langle x = 2\rangle \mathtt{x{+}{+};} \; + \; \mathtt{skip;} \langle x = 2 \lor x = 3\rangle}\;\boxed{3}
$$

$$
\text{(GATHER)}\;\dfrac{\boxed{2} \qquad \boxed{3}}{\vdash_a \langle x = 1, x = 2\rangle \mathtt{x{+}{+};} \; + \; \mathtt{skip;} \langle x = 1 \lor x = 2, x = 2 \lor x = 3\rangle}\;\boxed{4}
$$

$\langle \mathit{true} \rangle$

N

$\langle x = 1, x = 2\rangle$

x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{\dfrac{}{\vdash_a \langle true\rangle \texttt{x = 1;} \langle x = 1\rangle}\;(\text{COM})}{\vdash_a \langle true\rangle\, \mathsf{N}\, \langle x = 1\rangle}\;(\text{ANG}) \qquad \dfrac{\dfrac{}{\vdash_a \langle true\rangle \texttt{x = 2;} \langle x = 2\rangle}\;(\text{COM})}{\vdash_a \langle true\rangle\, \mathsf{N}\, \langle x = 2\rangle}\;(\text{ANG})}{\vdash_a \langle true\rangle\, \mathsf{N}\, \langle x = 1,\ x = 2\rangle}\;(\text{GATHER})\quad 1$$

$$\dfrac{\dfrac{}{\vdash_a \langle x = 1\rangle \texttt{x++;} \langle x = 2\rangle}\;(\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 1\rangle \texttt{skip;} \langle x = 1\rangle}\;(\text{COM})}{\vdash_a \langle x = 1\rangle \texttt{x++;} + \texttt{skip;} \langle x = 1 \vee x = 2\rangle}\;(\text{DEM})\quad 2$$

$$\dfrac{\dfrac{}{\vdash_a \langle x = 2\rangle \texttt{x++;} \langle x = 3\rangle}\;(\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 2\rangle \texttt{skip;} \langle x = 2\rangle}\;(\text{COM})}{\vdash_a \langle x = 2\rangle \texttt{x++;} + \texttt{skip;} \langle x = 2 \vee x = 3\rangle}\;(\text{DEM})\quad 3$$

$$\dfrac{2 \qquad 3}{\vdash_a \langle x = 1, x = 2\rangle \texttt{x++;} + \texttt{skip;} \langle x = 1 \vee x = 2,\ x = 2 \vee x = 3\rangle}\;(\text{GATHER})\quad 4$$

1

$\langle true\rangle$
N
$\langle x = 1, x = 2\rangle$
x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\dfrac{\dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 1;} \langle x = 1 \rangle}\,(\text{COM})}{\vdash_a \langle true \rangle \, \mathsf{N} \, \langle x = 1 \rangle}\,(\text{ANG}) \qquad \dfrac{\dfrac{}{\vdash_a \langle true \rangle \texttt{x = 2;} \langle x = 2 \rangle}\,(\text{COM})}{\vdash_a \langle true \rangle \, \mathsf{N} \, \langle x = 2 \rangle}\,(\text{ANG})}{\vdash_a \langle true \rangle \, \mathsf{N} \, \langle x = 1, \; x = 2 \rangle}\,(\text{GATHER}) \; \boxed{1}$$

$$\dfrac{\dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{x++;} \langle x = 2 \rangle}\,(\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 1 \rangle \texttt{skip;} \langle x = 1 \rangle}\,(\text{COM})}{\vdash_a \langle x = 1 \rangle \texttt{x++;} \; + \; \texttt{skip;} \langle x = 1 \vee x = 2 \rangle}\,(\text{DEM}) \; \boxed{2}$$

$$\dfrac{\dfrac{}{\vdash_a \langle x = 2 \rangle \texttt{x++;} \langle x = 3 \rangle}\,(\text{COM}) \qquad \dfrac{}{\vdash_a \langle x = 2 \rangle \texttt{skip;} \langle x = 2 \rangle}\,(\text{COM})}{\vdash_a \langle x = 2 \rangle \texttt{x++;} \; + \; \texttt{skip;} \langle x = 2 \vee x = 3 \rangle}\,(\text{DEM}) \; \boxed{3}$$

$$\dfrac{\boxed{2} \qquad \boxed{3}}{\vdash_a \underbrace{\langle x = 1, x = 2 \rangle}_{\boxed{1}} \texttt{x++;} \; + \; \texttt{skip;} \underbrace{\langle x = 1 \vee x = 2, \; x = 2 \vee x = 3 \rangle}_{\boxed{4}}}\,(\text{GATHER}) \; \boxed{4}$$

$\langle true \rangle$
N
$\langle x = 1, x = 2 \rangle$
$\texttt{x++;} \; + \; \texttt{skip;}$

N ::= x = 1 | x = 2

Realizability Logic

$$\text{(GATHER)}\ \dfrac{\text{(ANG)}\ \dfrac{\text{(COM)}\ \dfrac{}{\vdash_a \langle \mathit{true} \rangle \mathtt{x\ =\ 1;} \langle x = 1 \rangle}}{\vdash_a \langle \mathit{true} \rangle\, \mathsf{N}\, \langle x = 1 \rangle} \qquad \text{(ANG)}\ \dfrac{\text{(COM)}\ \dfrac{}{\vdash_a \langle \mathit{true} \rangle \mathtt{x\ =\ 2;} \langle x = 2 \rangle}}{\vdash_a \langle \mathit{true} \rangle\, \mathsf{N}\, \langle x = 2 \rangle}}{\vdash_a \langle \mathit{true} \rangle\, \mathsf{N}\, \langle x = 1, x = 2 \rangle}\ \boxed{1}$$

$$\text{(DEM)}\ \dfrac{\text{(COM)}\ \dfrac{}{\vdash_a \langle x = 1 \rangle \mathtt{x++;} \langle x = 2 \rangle} \qquad \text{(COM)}\ \dfrac{}{\vdash_a \langle x = 1 \rangle \mathtt{skip;} \langle x = 1 \rangle}}{\vdash_a \langle x = 1 \rangle \mathtt{x++;}\ +\ \mathtt{skip;} \langle x = 1 \lor x = 2 \rangle}\ \boxed{2}$$

$$\text{(DEM)}\ \dfrac{\text{(COM)}\ \dfrac{}{\vdash_a \langle x = 2 \rangle \mathtt{x++;} \langle x = 3 \rangle} \qquad \text{(COM)}\ \dfrac{}{\vdash_a \langle x = 2 \rangle \mathtt{skip;} \langle x = 2 \rangle}}{\vdash_a \langle x = 2 \rangle \mathtt{x++;}\ +\ \mathtt{skip;} \langle x = 2 \lor x = 3 \rangle}\ \boxed{3}$$

$$\text{(GATHER)}\ \dfrac{\boxed{2} \qquad \boxed{3}}{\vdash_a \langle x = 1, x = 2 \rangle \mathtt{x++;}\ +\ \mathtt{skip;} \langle x = 1 \lor x = 2, x = 2 \lor x = 3 \rangle}\ \boxed{4}$$

$$\text{(SEQ)}\ \dfrac{\boxed{1} \qquad \boxed{4}}{\vdash_a \langle \mathit{true} \rangle\, \mathsf{N}; (\mathtt{x++;}\ +\ \mathtt{skip;}) \langle x = 1 \lor x = 2, x = 2 \lor x = 3 \rangle}$$

$\langle \mathit{true} \rangle$

N

$\langle x = 1, x = 2 \rangle$

x++; + skip;

$\langle x = 1 \lor x = 2, x = 2 \lor x = 3 \rangle$

N ::= x = 1 | x = 2

Contribution 1:

Realizability Logic

$$\vdash_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \models_a \langle R \rangle \texttt{sketch} \langle S \rangle$$

Contribution 1:

Realizability Logic

$$\vdash_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \models_a \langle R \rangle \texttt{sketch} \langle S \rangle$$

But what makes this efficient?

Realizability Logic - Secret Sauce

$\langle x = 0 \rangle$

N;

N;

N;

N ::= x++ | x--

Realizability Logic - Secret Sauce

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -1 \rangle$

N;

N;

N ::= x++ | x--

Realizability Logic - Secret Sauce

$$\langle x = 0 \rangle$$

N;

$$\langle x = 1, x = -1 \rangle$$

N;

$$\langle x = 2, x = 0, x = -2 \rangle$$

N;

N ::= x++ | x--

Realizability Logic - Secret Sauce

$$\langle x = 0 \rangle$$

N;

$$\langle x = 1, x = -1 \rangle$$

N;

$$\langle x = 2, x = 0, x = -2 \rangle$$

N;

$$\langle x = 3, x = 1, x = -1, x = -3 \rangle$$

N ::= x++ | x--

Realizability Logic - Secret Sauce

$$\langle x = 0 \rangle$$

N;

$$\langle x = 1, x = -1 \rangle$$

N;

$$\langle x = 2, x = 0, x = -2 \rangle$$

N;

$$\langle x = 3, x = 1, x = -1, x = -3 \rangle$$

N ::= x++ | x--

8 Programs vs. 4 Predicates

Realizability Logic - Secret Sauce

$$\langle x = 0 \rangle$$
N;
$$\langle x = 1, x = -1 \rangle$$
N;
$$\langle x = 2, x = 0, x = -2 \rangle$$
N;
$$\langle x = 3, x = 1, x = -1, x = -3 \rangle$$

N ::= x++ | x--

8 Programs vs. 4 Predicates

Problem: We forgot the program!

Realizability Logic - Secret Sauce

Solution:

<u>Realization Logic</u>

Rewrite proof to derive program

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -$ …

N;

$\langle x = 2, x$ …

N;

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

N ::= x++ | x--

8 Programs vs. 4 Predicates

Problem: We forgot the program!

Realization Logic

N ::= x++ | x--

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -1 \rangle$

N;

$\langle x = 2, x = 0, x = -2 \rangle$

N;

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

Realization Logic

N ::= x++ | x--

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -1 \rangle$

N;

$\langle x = 2, x = 0, x = -2 \rangle$

N;

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

Realization Logic

N ::= x++ | x--

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -1 \rangle$

N;

$\langle x = 2, x = 0, x = -2 \rangle$

N;

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

$\models_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \texttt{prog} \in drv(\texttt{sketch}).\ \models_d \{r\}\texttt{prog}\{s\}$.

Realization Logic

N ::= x++ | x--

$$\langle x = 2, x = 0, x = -2 \rangle$$

N;

$$\langle x = 3, x = 1, x = -1, x = -3 \rangle$$

$$\langle x = 0 \rangle$$

N;

$$\langle x = 1, x = -1 \rangle$$

N;

$$\langle x = 2, x = 0, x = -2 \rangle$$

N;

$$\langle x = 3, x = 1, x = -1, x = -3 \rangle$$

$$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\}\mathtt{prog}\{s\}\ .$$

Realization Logic

N ::= x++ | x--

$$\langle x = 2, x = 0, x = -2 \rangle$$
N;
$$\langle x = 3, x = 1, x = -1, x = -3 \rangle$$
$$\mid\!\sim$$

$$\langle x = 0 \rangle$$
N;
$$\langle x = 1, x = -1 \rangle$$
N;
$$\langle x = 2, x = 0, x = -2 \rangle$$
N;
$$\langle x = 3, x = 1, x = -1, x = -3 \rangle$$

$$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\}\mathtt{prog}\{s\}\ .$$

Realization Logic

N ::= x++ | x--

$\langle x = 2, x = 0, x = -2 \rangle$

N;

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

$\mid\!\sim$

$\langle x = 2, x = 0, x = -2 \rangle$

N;

$\langle x = 1 \rangle$

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -1 \rangle$

N;

$\langle x = 2, x = 0, x = -2 \rangle$

N;

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\}\mathtt{prog}\{s\}$.

Realization Logic

N ::= x++ | x--

$$\langle x = 2\underline{,}\ x = 0\underline{,}\ x = -2 \rangle$$

N;

$$\langle x = 3\underline{,}\ x = 1\underline{,}\ x = -1\underline{,}\ x = -3 \rangle$$

$$\mathrel{|\!\!\sim}$$

$$\langle x = 2\underline{,}\ x = 0\underline{,}\ x = -2 \rangle$$

N;

$$\langle x = 1 \rangle$$

$$\langle x = 0 \rangle$$

N;

$$\langle x = 1\underline{,}\ x = -1 \rangle$$

N;

$$\langle x = 2\underline{,}\ x = 0\underline{,}\ x = -2 \rangle$$

N;

$$\langle x = 1 \rangle$$

$$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\}\mathtt{prog}\{s\}\ .$$

Realization Logic

N ::= x++ | x--

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -1 \rangle$

N;

$\langle x = 2, x = 0, x = -2 \rangle$

N;

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\} \mathtt{prog} \{s\}\ .$

Realization Logic

N ::= x++ | x--

$\langle x = 2, x = 0, x = -2 \rangle$

N;

$\langle x = 1 \rangle$

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -1 \rangle$

N;

$\langle x = 2, x = 0, x = -2 \rangle$

N;

$\langle x = 1 \rangle$

$$\models_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \texttt{prog} \in drv(\texttt{sketch}).\ \models_d \{r\}\texttt{prog}\{s\}\ .$$

Realization Logic

N ::= x++ | x--

$$\langle x = 2, x = 0, x = -2 \rangle$$

N;

$$\langle x = 1 \rangle$$

$$\mid\!\sim$$

$$\langle x = 2, x = 0, x = -2 \rangle$$

x++;

$$\langle x = 1 \rangle$$

$$\langle x = 0 \rangle$$

N;

$$\langle x = 1, x = -1 \rangle$$

N;

$$\langle x = 2, x = 0, x = -2 \rangle$$

N;

$$\langle x = 1 \rangle$$

$$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\}\mathtt{prog}\{s\}\ .$$

Realization Logic

N ::= x++ | x--

$\langle x = 2 \underline{,} \; x = 0 \underline{,} \; x = -2 \rangle$

N;

$\langle x = 1 \rangle$

$\mid\!\sim$

$\langle x = 2 \underline{,} \; x = 0 \underline{,} \; x = -2 \rangle$

x++;

$\langle x = 1 \rangle$

$\langle x = 0 \rangle$

N;

$\langle x = 1 \underline{,} \; x = -1 \rangle$

N;

$\langle x = 2 \underline{,} \; x = 0 \underline{,} \; x = -2 \rangle$

x++;

$\langle x = 1 \rangle$

$$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\}\mathtt{prog}\{s\}\ .$$

Realization Logic

N ::= x++ | x--

$\langle x = 0\rangle$

N;

$\langle x = 1, x = -1\rangle$

N;

$\langle x = 2, x = 0, x = -2\rangle$

x++;

$\langle x = 1\rangle$

$$\models_a \langle R\rangle \texttt{sketch}\langle S\rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \texttt{prog} \in drv(\texttt{sketch}).\ \models_d \{r\}\texttt{prog}\{s\}\ .$$

Realization Logic

N ::= x++ | x--

$\langle x = 2, x = 0, x = -2 \rangle$

x++;

$\langle x = 1 \rangle$

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -1 \rangle$

N;

$\langle x = 2, x = 0, x = -2 \rangle$

x++;

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \texttt{prog} \in drv(\texttt{sketch}).\ \models_d \{r\}\texttt{prog}\{s\}\ .$

Realization Logic

N ::= x++ | x--

$\langle x = 2, x = 0, x = -2 \rangle$

x++;

$\langle x = 1 \rangle$

$\mathrel{|\!\sim}$

$\langle x = 0 \rangle$

x++;

$\langle x = 1 \rangle$

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -1 \rangle$

N;

$\langle x = 2, x = 0, x = -2 \rangle$

x++;

$\langle x = 1 \rangle$

$$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\}\mathtt{prog}\{s\}\ .$$

Realization Logic

N ::= x++ | x--

$\langle x = 2, x = 0, x = -2 \rangle$

x++;

$\langle x = 1 \rangle$

$\mid\!\sim$

$\langle x = 0 \rangle$

x++;

$\langle x = 1 \rangle$

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -1 \rangle$

N;

$\langle x = 0 \rangle$

x++;

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \texttt{prog} \in drv(\texttt{sketch}).\ \models_d \{r\} \texttt{prog} \{s\}\ .$

Realization Logic

N ::= x++ | x--

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -1 \rangle$

N;

$\langle x = 0 \rangle$

x++;

$\langle x = 1 \rangle$

$$\models_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \texttt{prog} \in drv(\texttt{sketch}).\ \models_d \{r\}\texttt{prog}\{s\}\ .$$

Realization Logic

N ::= x++ | x--

$\langle x = 1, x = -1 \rangle$
N;
$\langle x = 0 \rangle$

$\langle x = 0 \rangle$
N;
$\langle x = 1, x = -1 \rangle$
N;
$\langle x = 0 \rangle$
x++;
$\langle x = 1 \rangle$

$$\models_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \texttt{prog} \in drv(\texttt{sketch}).\ \models_d \{r\}\texttt{prog}\{s\}\ .$$

Realization Logic

N ::= x++ | x--

$\langle x = 1\underline{,}\ x = -1 \rangle$

N;

$\langle x = 0 \rangle$

$\mid\!\sim$

$\langle x = 1\underline{,}\ x = -1 \rangle$

x++;

$\langle x = 0 \rangle$

$\langle x = 0 \rangle$

N;

$\langle x = 1\underline{,}\ x = -1 \rangle$

N;

$\langle x = 0 \rangle$

x++;

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \texttt{prog} \in drv(\texttt{sketch}).\ \models_d \{r\}\texttt{prog}\{s\}\ .$

Realization Logic

N ::= x++ | x--

$\langle x = 0 \rangle$

N;

$\langle x = 1, x = -1 \rangle$

x++;

$\langle x = 0 \rangle$

x++;

$\langle x = 1 \rangle$

$$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\}\mathtt{prog}\{s\}\ .$$

Realization Logic

N ::= x++ | x--

$\langle x = 1, x = -1 \rangle$
x++;
$\langle x = 0 \rangle$

$\langle x = 0 \rangle$
N;
$\langle x = 1, x = -1 \rangle$
x++;
$\langle x = 0 \rangle$
x++;
$\langle x = 1 \rangle$

$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\} \mathtt{prog} \{s\}\ .$

Realization Logic

N ::= x++ | x--

$\langle x = 1, x = -1 \rangle$
x++;
$\langle x = 0 \rangle$

$\mid\!\sim$

$\langle x = -1 \rangle$
x++;
$\langle x = 0 \rangle$

$\langle x = 0 \rangle$
N;
$\langle x = 1, x = -1 \rangle$
x++;
$\langle x = 0 \rangle$
x++;
$\langle x = 1 \rangle$

$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\}\mathtt{prog}\{s\}\ .$

Realization Logic

N ::= x++ | x--

$\langle x = 1, x = -1 \rangle$

x++;

$\langle x = 0 \rangle$

$\mid\!\sim$

$\langle x = -1 \rangle$

x++;

$\langle x = 0 \rangle$

$\langle x = 0 \rangle$

N;

$\langle x = -1 \rangle$

x++;

$\langle x = 0 \rangle$

x++;

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \texttt{prog} \in drv(\texttt{sketch}).\ \models_d \{r\}\texttt{prog}\{s\}\ .$

Realization Logic

N ::= x++ | x--

$\langle x = 0 \rangle$

N;

$\langle x = -1 \rangle$

x++;

$\langle x = 0 \rangle$

x++;

$\langle x = 1 \rangle$

$$\models_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \texttt{prog} \in drv(\texttt{sketch}).\ \models_d \{r\}\texttt{prog}\{s\}\ .$$

Realization Logic

N ::= x++ | x--

$\langle x = 0 \rangle$
N;
$\langle x = -1 \rangle$

$\langle x = 0 \rangle$
N;
$\langle x = -1 \rangle$
x++;
$\langle x = 0 \rangle$
x++;
$\langle x = 1 \rangle$

$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\}\mathtt{prog}\{s\}$.

Realization Logic

N ::= x++ | x--

$\langle x = 0 \rangle$

N;

$\langle x = -1 \rangle$

$\mid\!\sim$

$\langle x = 0 \rangle$

x--;

$\langle x = -1 \rangle$

$\langle x = 0 \rangle$

N;

$\langle x = -1 \rangle$

x++;

$\langle x = 0 \rangle$

x++;

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \texttt{prog} \in drv(\texttt{sketch}).\ \models_d \{r\}\texttt{prog}\{s\}$.

Realization Logic

N ::= x++ | x--

$\langle x = 0 \rangle$

N;

$\langle x = -1 \rangle$

$\mid\!\sim$

$\langle x = 0 \rangle$

x--;

$\langle x = -1 \rangle$

$\langle x = 0 \rangle$

x--;

$\langle x = -1 \rangle$

x++;

$\langle x = 0 \rangle$

x++;

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \texttt{prog} \in drv(\texttt{sketch}).\ \models_d \{r\}\texttt{prog}\{s\}$.

Contribution 2:

Realization Logic

$$\vdash_a \langle R \rangle \mathsf{po} \langle S \rangle \quad \wedge \quad \langle R \rangle \mathsf{po} \langle S \rangle \mathrel{|\!\!\sim} \langle R' \rangle \mathsf{po}' \langle S' \rangle$$
$$\Longrightarrow \quad \vdash_a \langle R' \rangle \mathsf{po}' \langle S' \rangle$$

Sound

Realization Logic

N ::= x++ | x--

Contribution 2:

Realization Logic

$$\vdash_a \langle R \rangle \mathsf{po} \langle S \rangle \quad \wedge \quad \langle R \rangle \mathsf{po} \langle S \rangle \mathrel{|\!\sim} \langle R' \rangle \mathsf{po}' \langle S' \rangle$$
$$\Longrightarrow \quad \vdash_a \langle R' \rangle \mathsf{po}' \langle S' \rangle$$

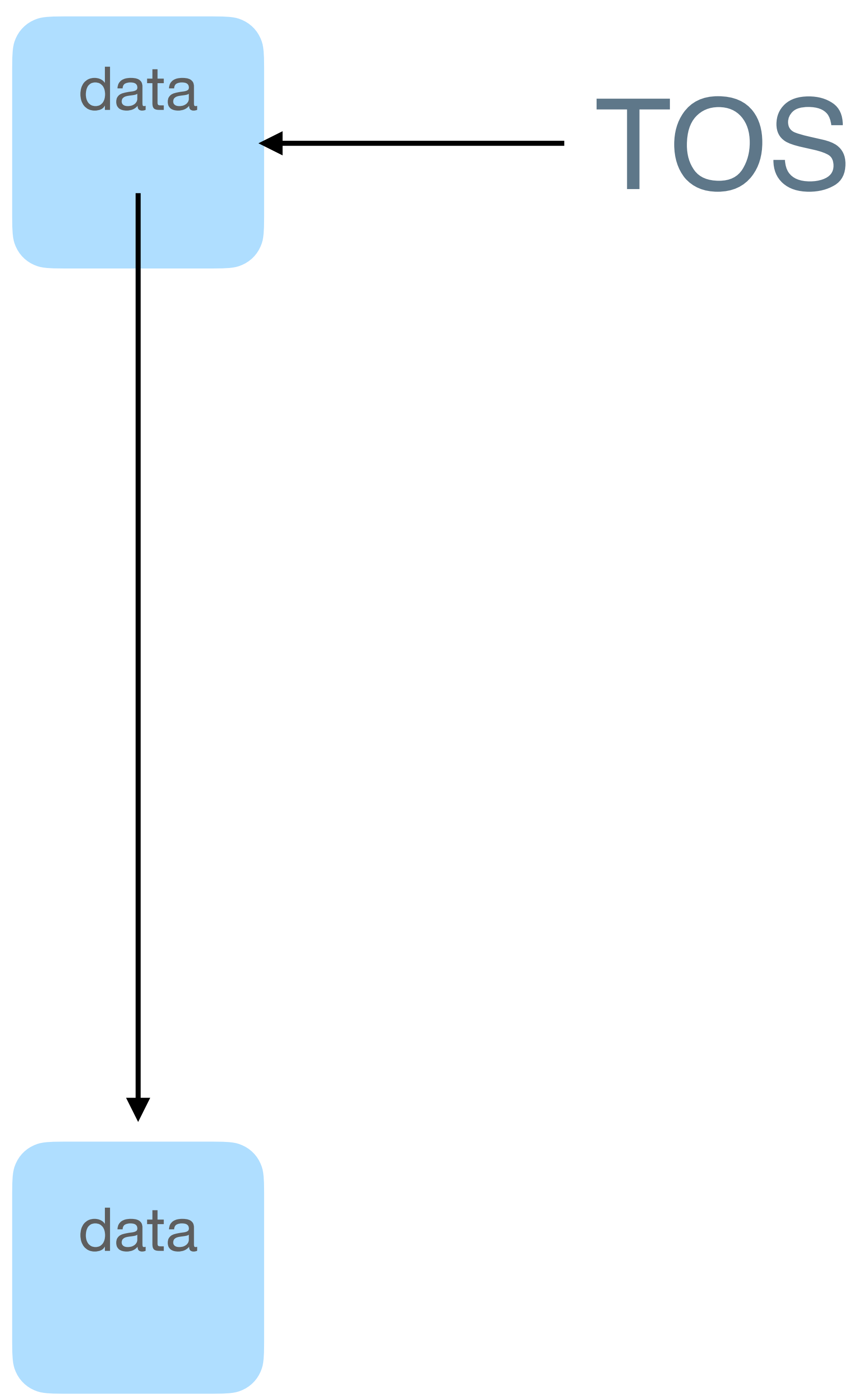
Sound and Complete

$$\vdash_a \langle R \rangle \mathsf{po} \langle S \rangle \quad \wedge \quad \vdash_a \langle R' \rangle \mathsf{po}' \langle S \rangle \quad \wedge \quad \langle R \rangle \mathsf{po} \langle S \rangle \preceq_p \langle R' \rangle \mathsf{po}' \langle S' \rangle$$
$$\Longrightarrow \quad \langle R \rangle \mathsf{po} \langle S \rangle \mathrel{|\!\sim} \langle R' \rangle \mathsf{po}' \langle S' \rangle$$

$$\models_a \langle R \rangle \mathtt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S.\ \exists r \in R.\ \exists \mathtt{prog} \in drv(\mathtt{sketch}).\ \models_d \{r\} \mathtt{prog} \{s\}\,.$$

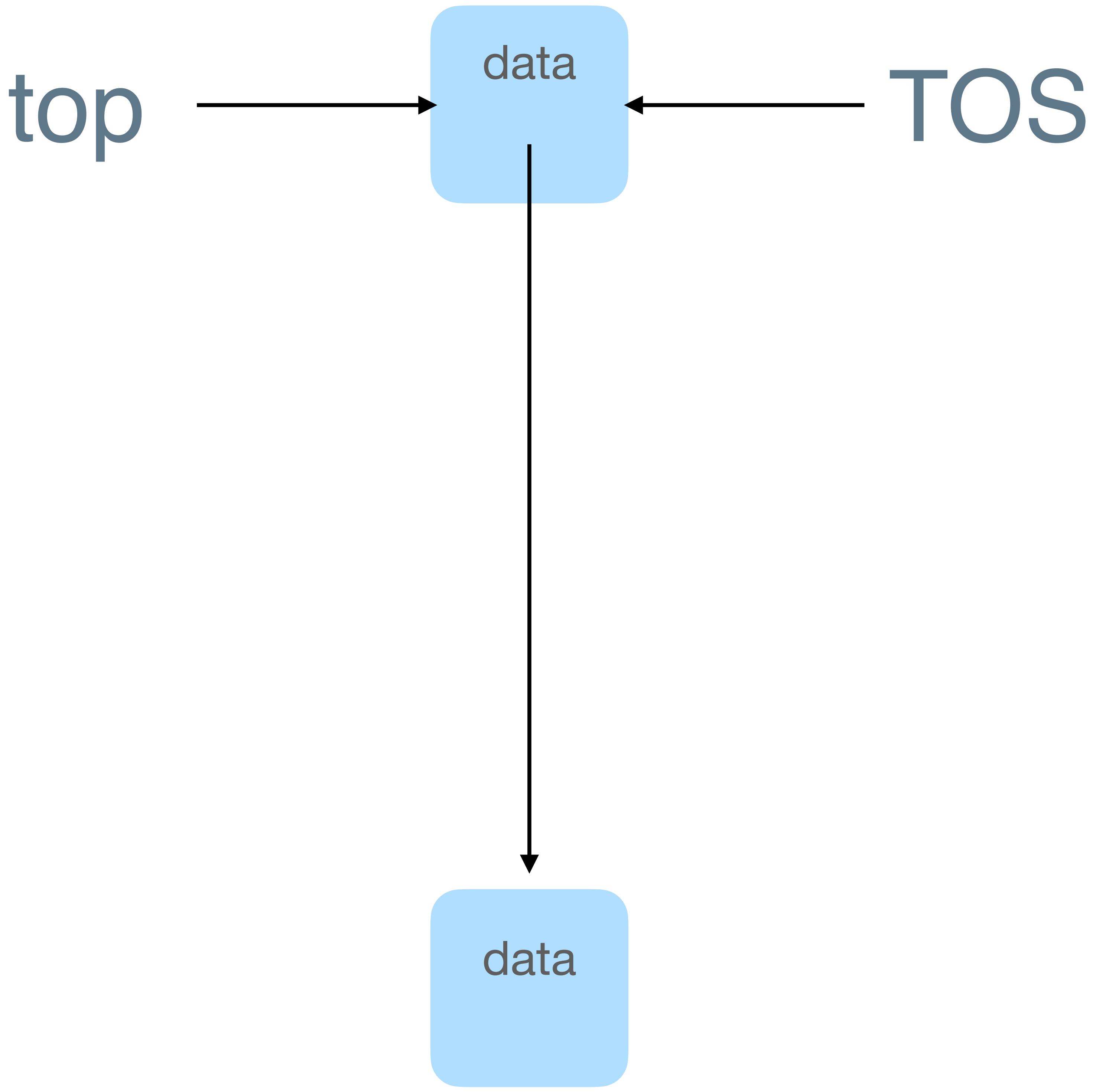
Memory Reclamation

```
top = TOS;
next = top.next;
CAS(TOS, top, next);
free(top);
```



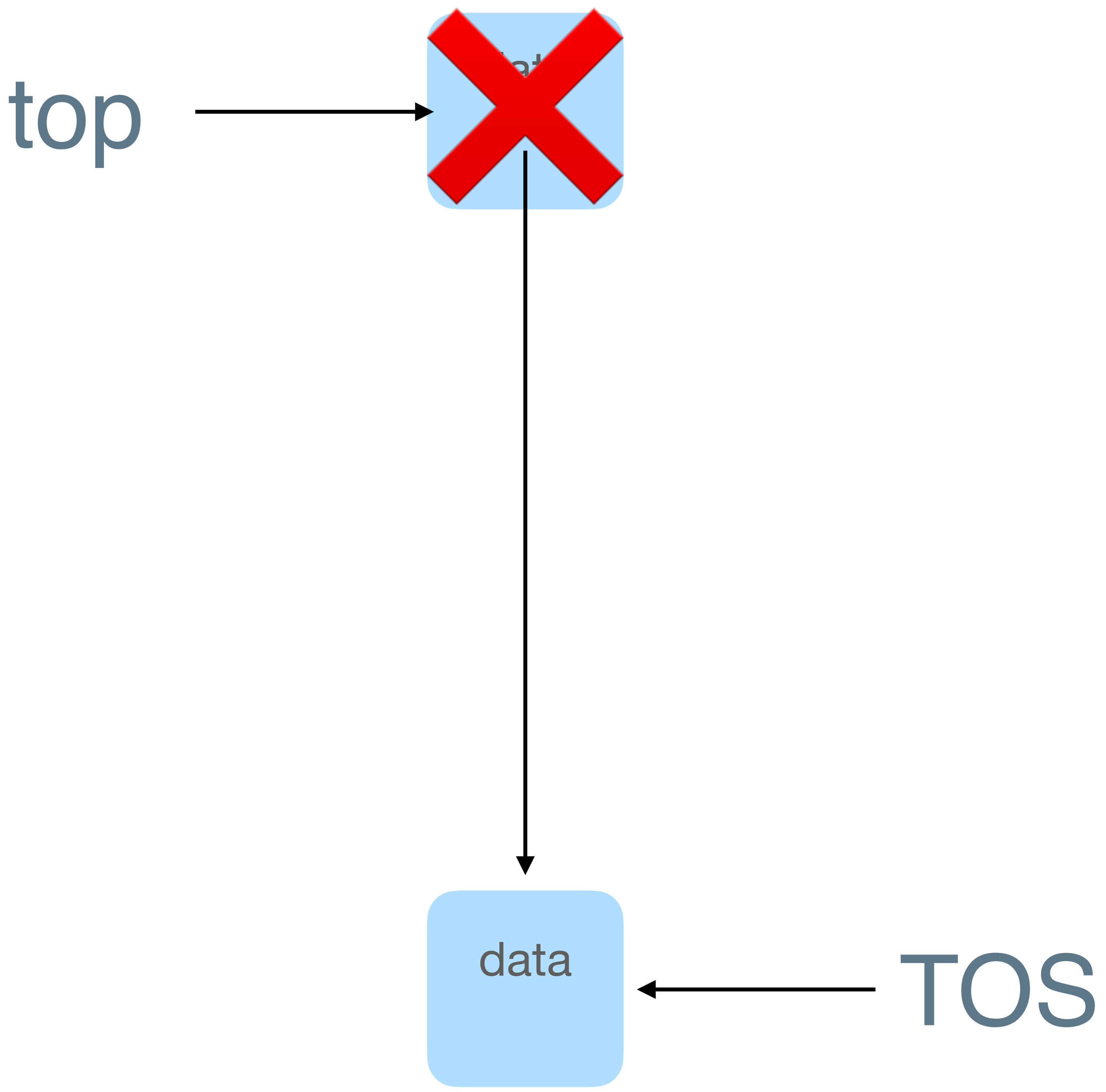
Memory Reclamation

top = TOS;
next = top.next;
CAS(TOS, top, next);
free(top);



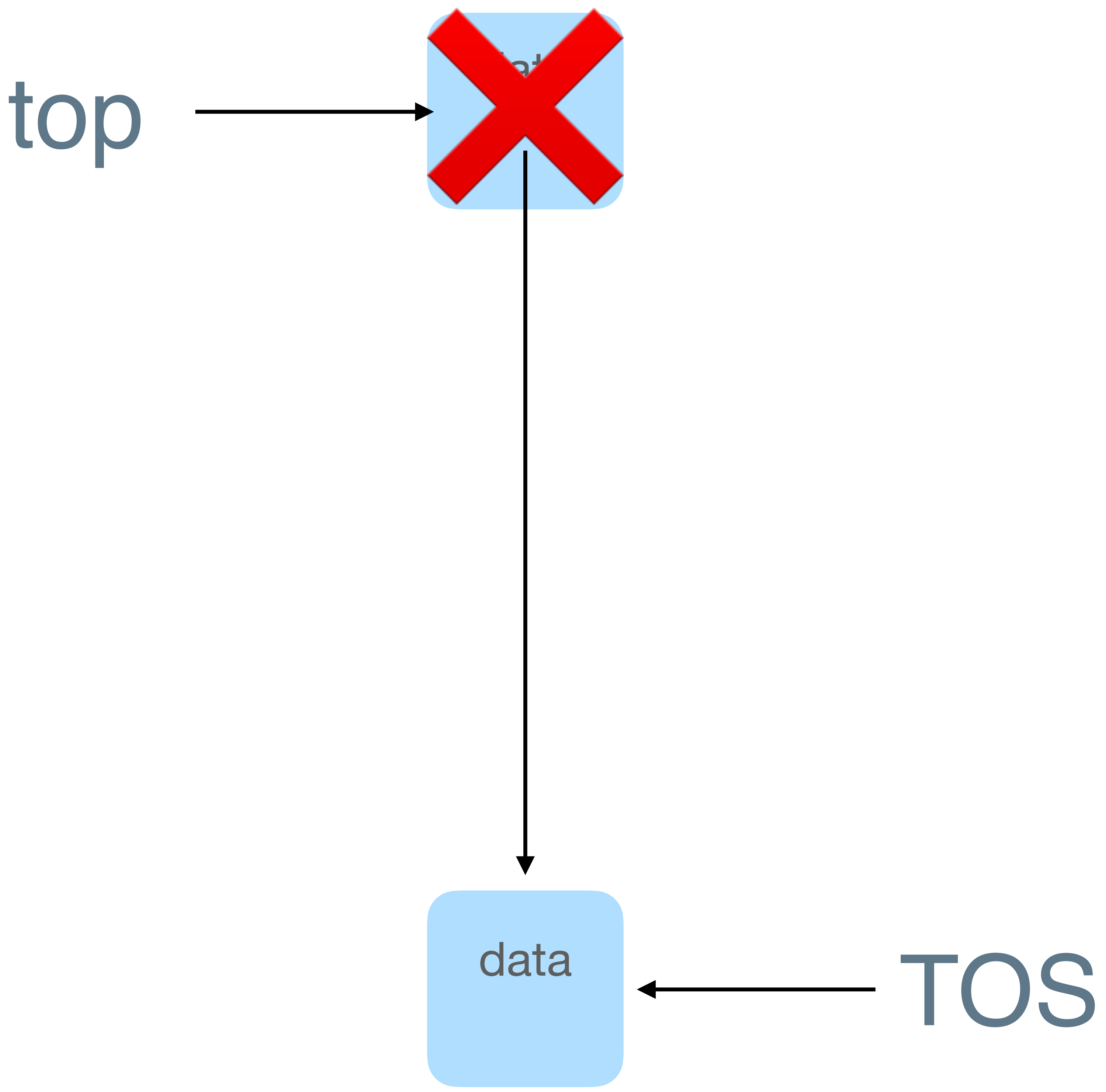
Memory Reclamation

```
top = TOS;
next = top.next;
CAS(TOS, top, next);
free(top);
```



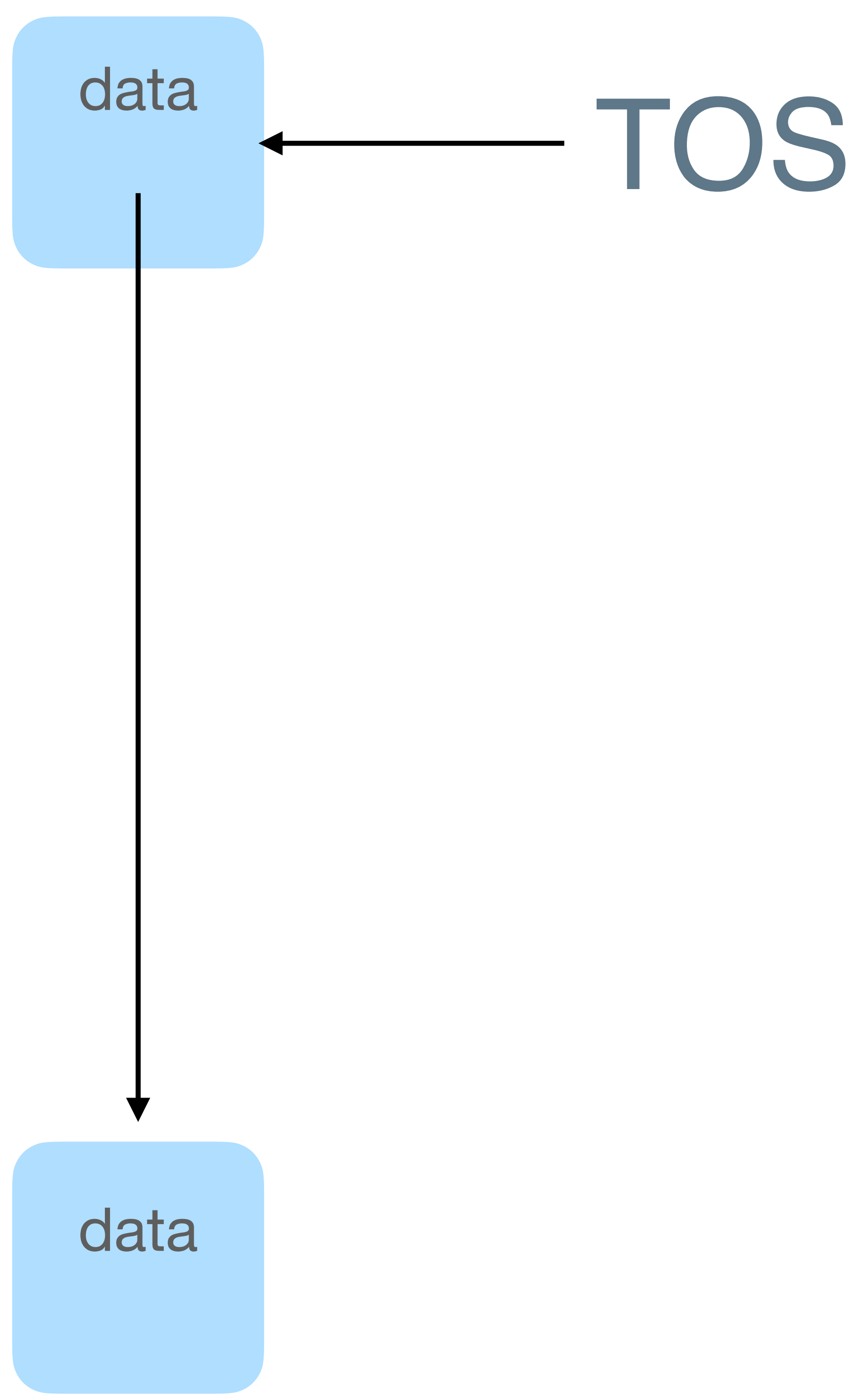
Memory Reclamation

top = TOS;
next = top.next; Unsafe Dereference
CAS(TOS, top, next);
free(top);



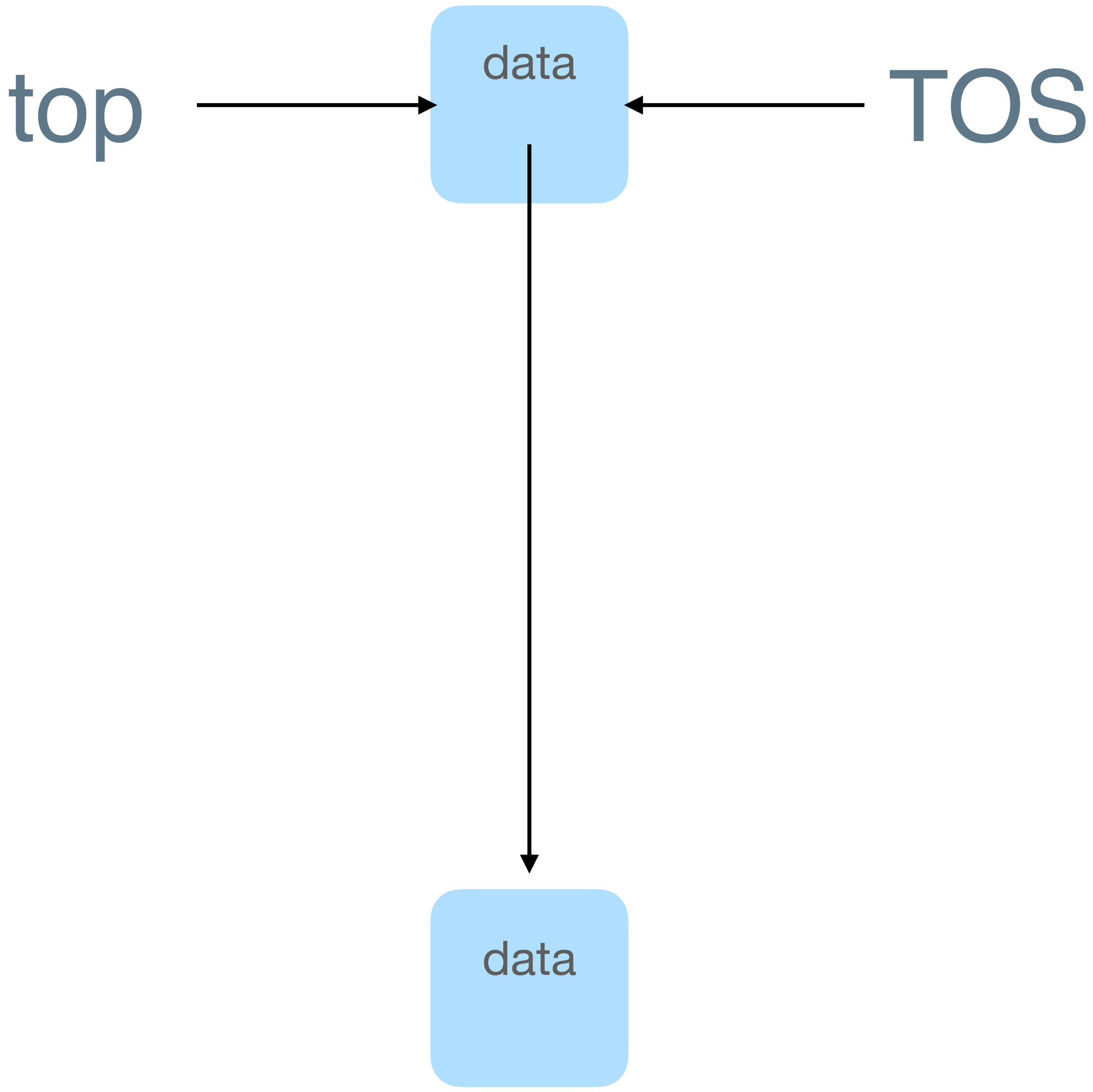
Memory Reclamation

```
top = TOS;
next = top.next;
CAS(TOS, top, next);
free(top);
```



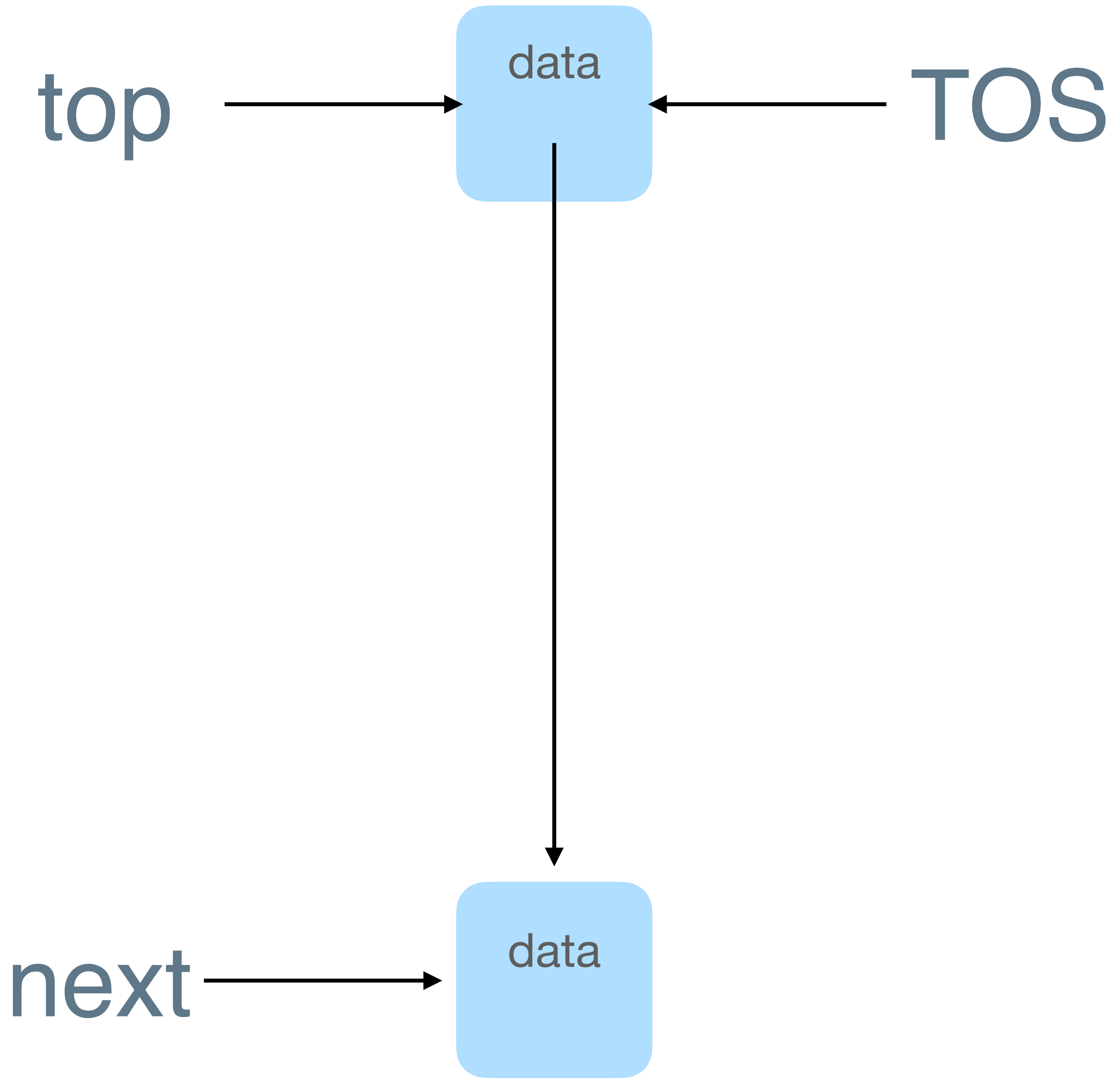
Memory Reclamation

top = TOS;
next = top.next;
CAS(TOS, top, next);
free(top);



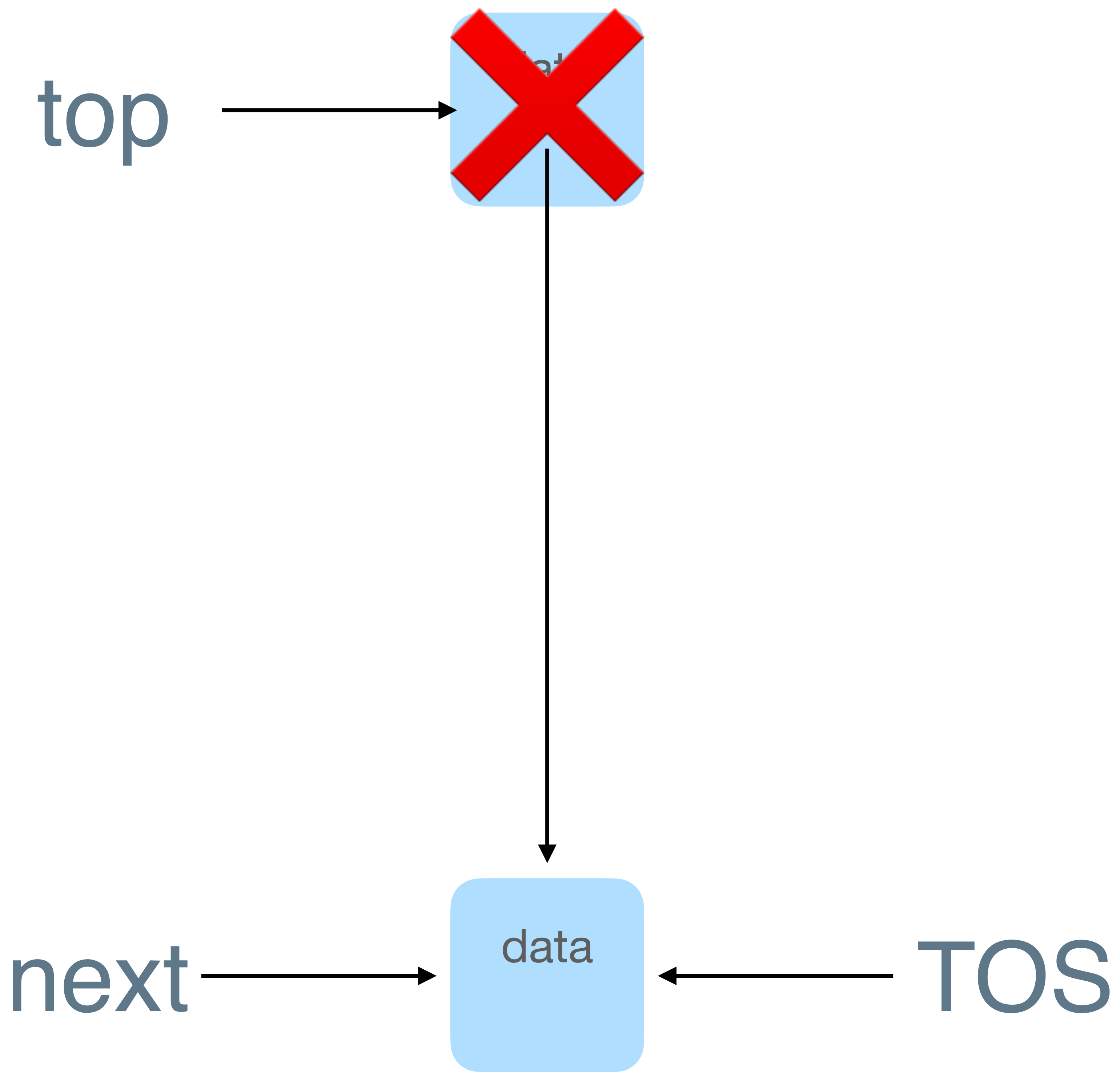
Memory Reclamation

top = TOS;
next = top.next;
CAS(TOS, top, next);
free(top);



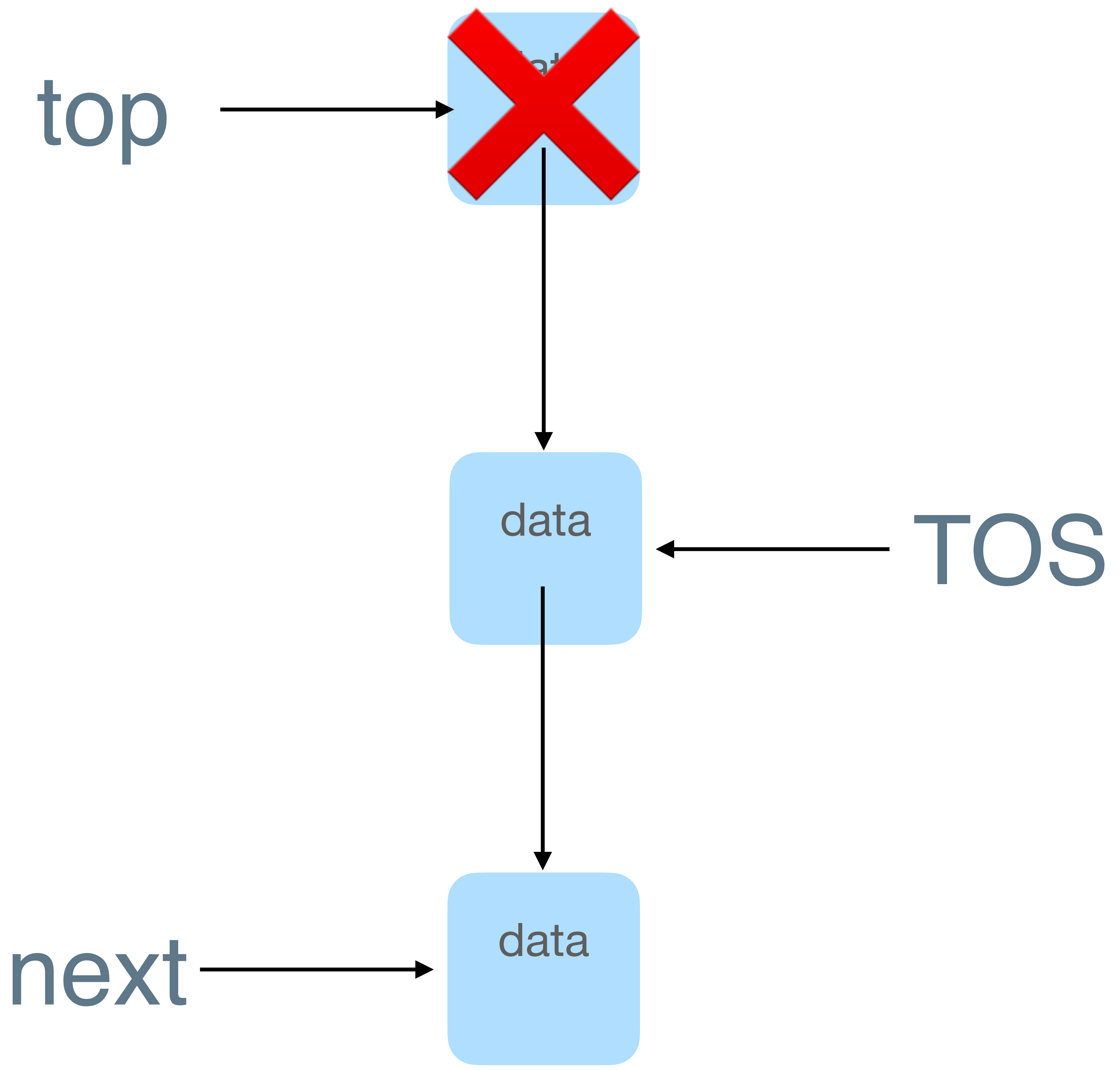
Memory Reclamation

top = TOS;
next = top.next;
CAS(TOS, top, next);
free(top);



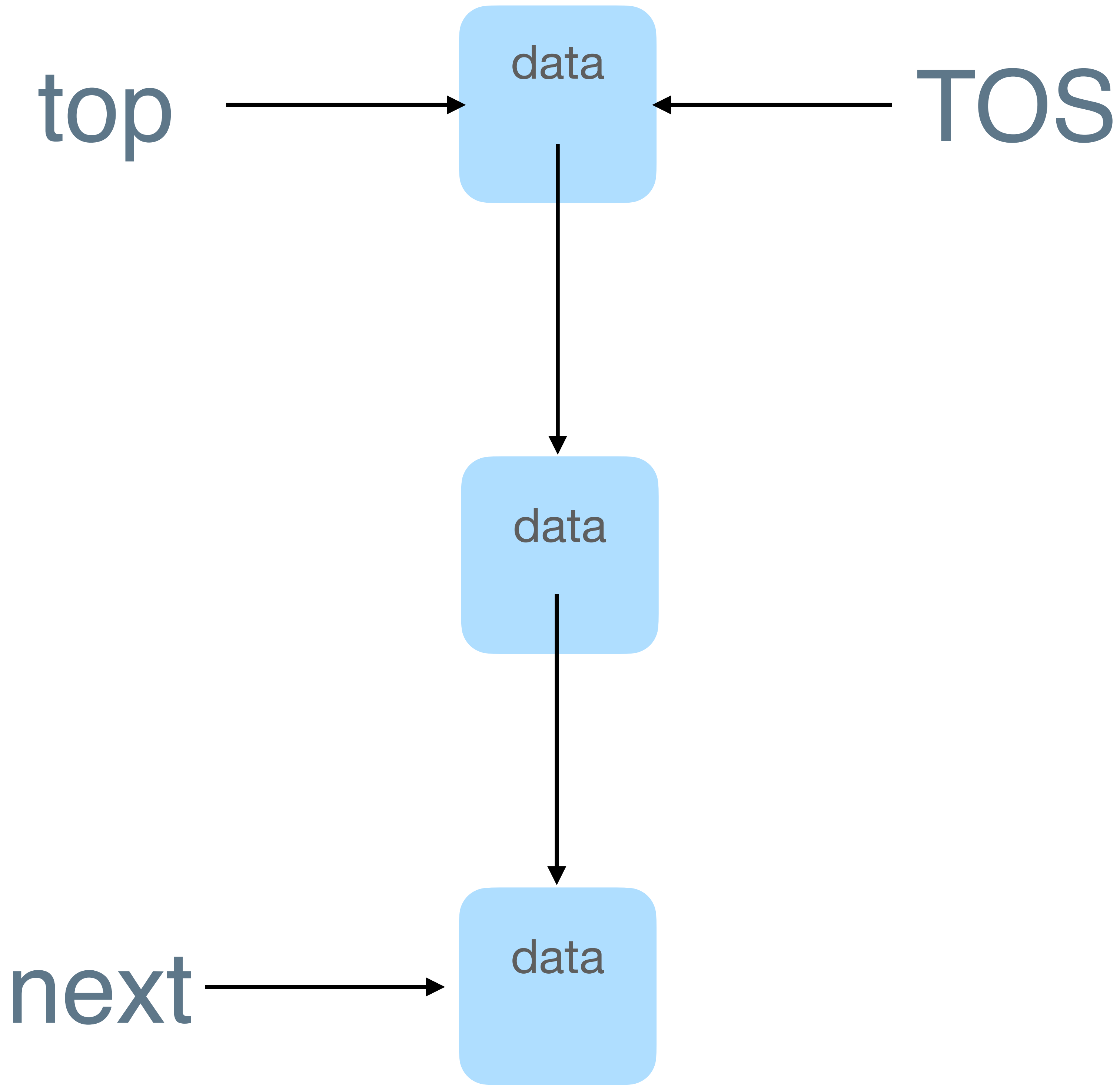
Memory Reclamation

```
top = TOS;
next = top.next;
CAS(TOS, top, next);
free(top);
```



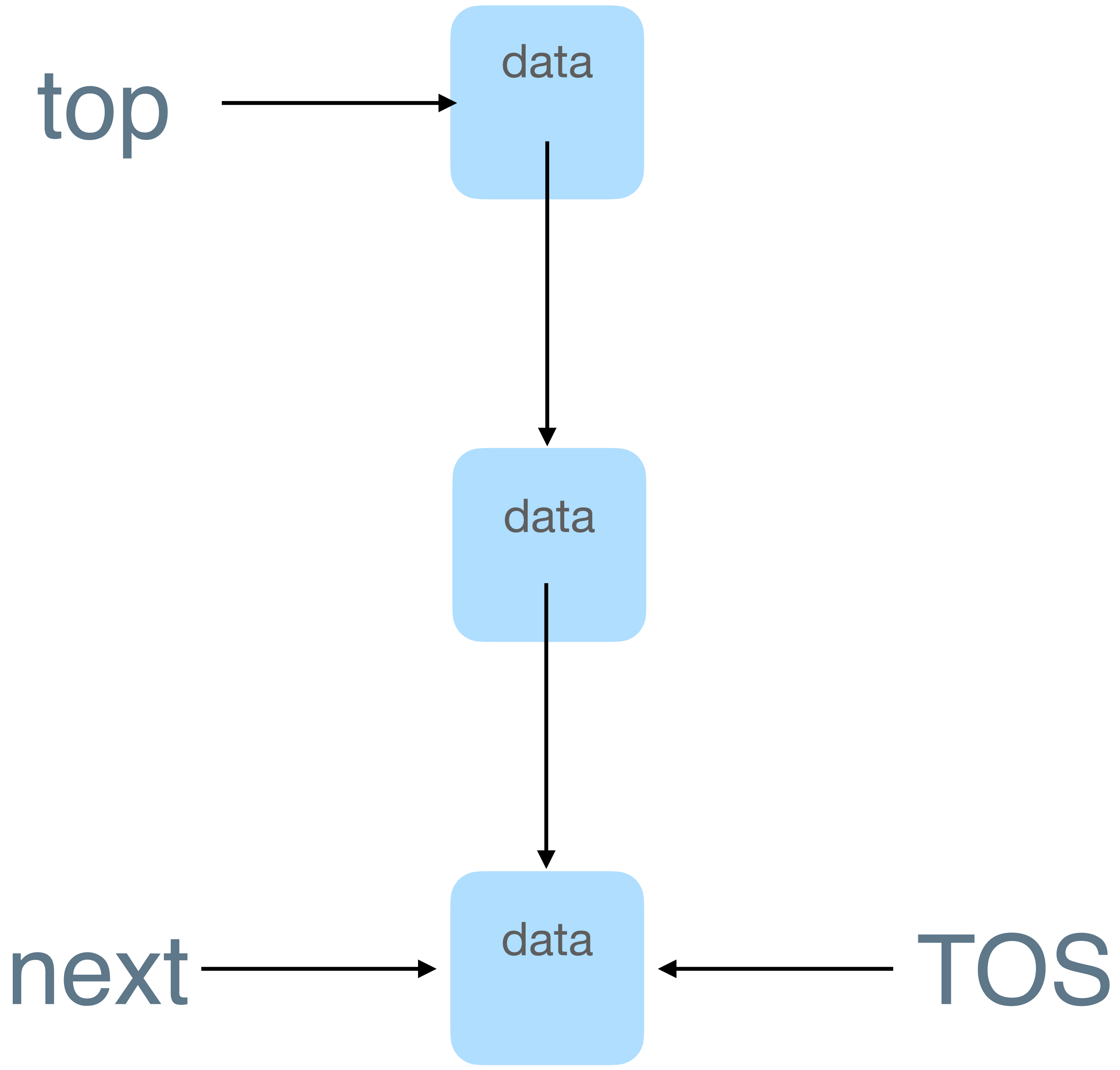
Memory Reclamation

```
top = TOS;
next = top.next;
CAS(TOS, top, next);
free(top);
```



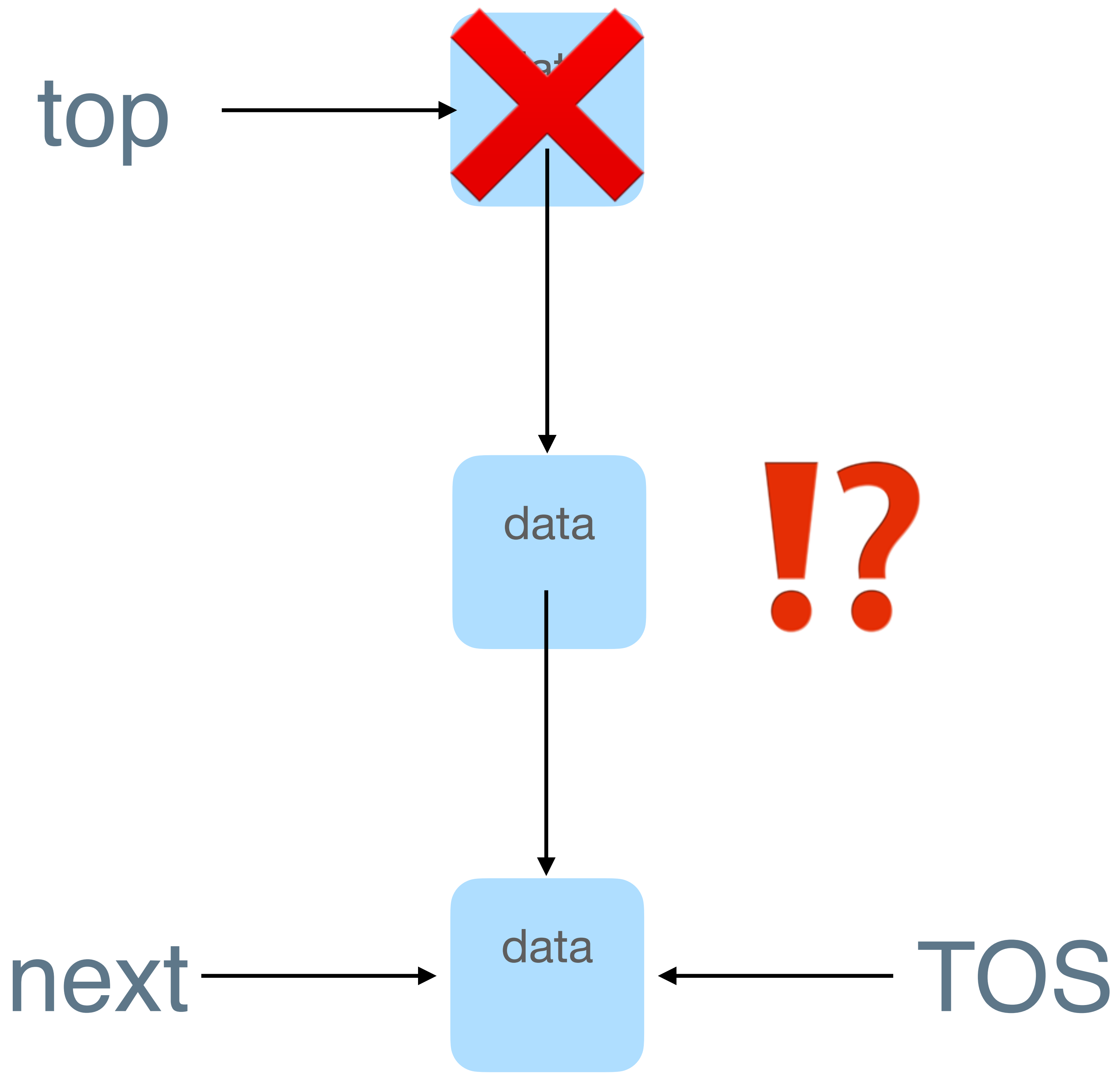
Memory Reclamation

top = TOS;
next = top.next;
CAS(TOS, top, next);
free(top);



Memory Reclamation

top = TOS;
next = top.next;
CAS(TOS, top, next);   ABA
free(top);



Safe Memory Reclamation (SMR)

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

free(-)

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

~~free(-)~~

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

~~free(-)~~ → retire(-) protect(-) unprotect(-)

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

~~free(-)~~ ⟶ retire(-)   protect(-)   unprotect(-)

- Type system to verify memory safety with SMR [Meyer, Wolff POPL'19 '20]

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

~~free(-)~~ $\longrightarrow$ retire(-)   protect(-)   unprotect(-)

- Type system to verify memory safety with SMR [Meyer, Wolff POPL'19 '20]

@inv active(-)

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

~~free(-)~~ ⟶ retire(-) protect(-) unprotect(-)

- Type system to verify memory safety with SMR [Meyer, Wolff POPL'19 '20]

@inv active(-)

$$Predicates \quad = \quad Vars \rightarrow \mathbb{T}$$

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

~~free(-)~~ $\longrightarrow$ retire(-) protect(-) unprotect(-)

- Type system to verify memory safety with SMR [Meyer, Wolff POPL'19 '20]

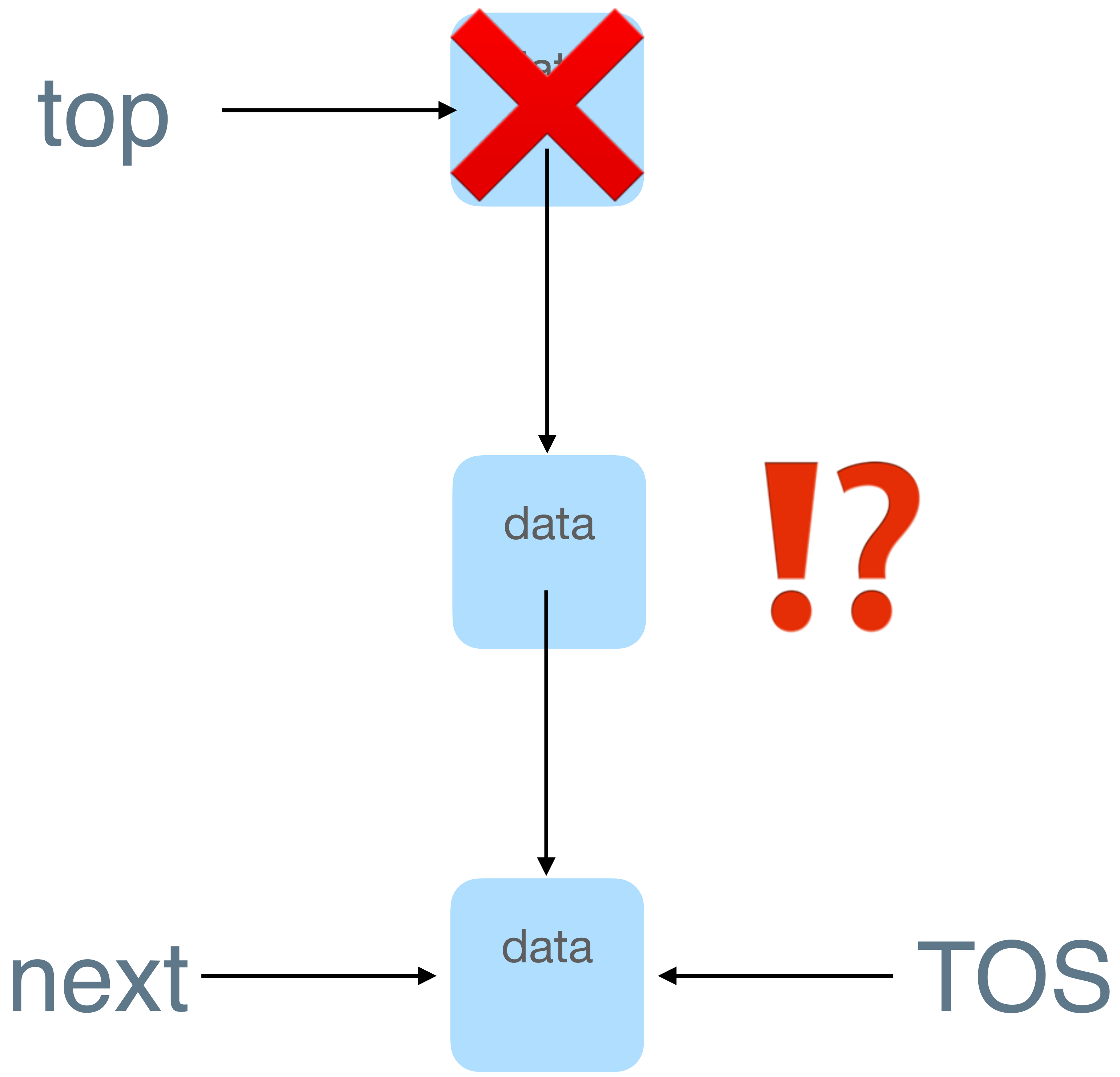
@inv active(-)

$$Predicates \quad = \quad Vars \rightarrow \mathbb{T}$$

Hazard Pointer: 5 base types

Memory Reclamation

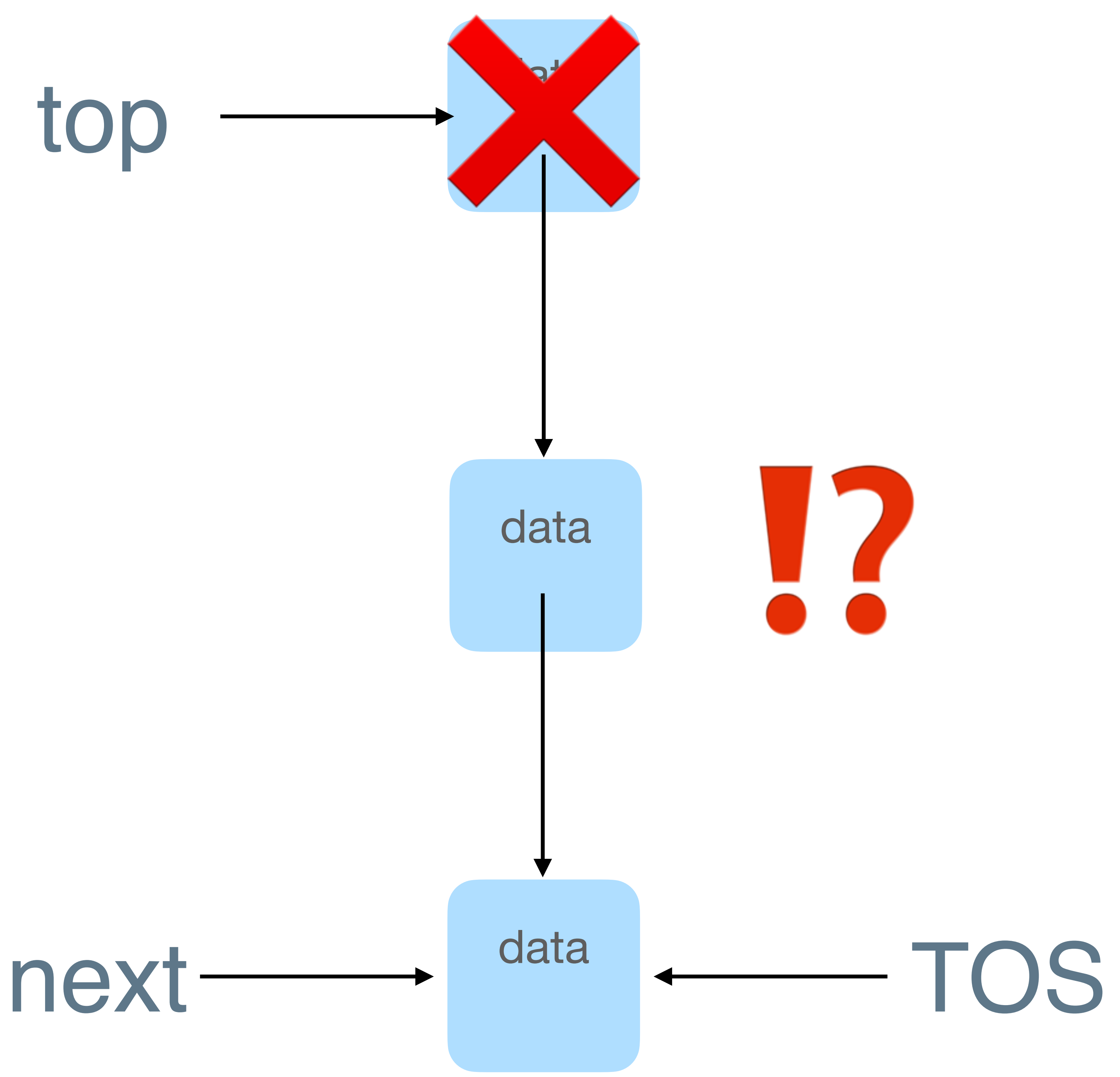
top = TOS;
next = top.next;
CAS(TOS, top, next);   ABA
free(top);



Memory Reclamation

N;
top = TOS;
N;
next = top.next;
N;
CAS(TOS, top, next);
N;
retire(top);
N;

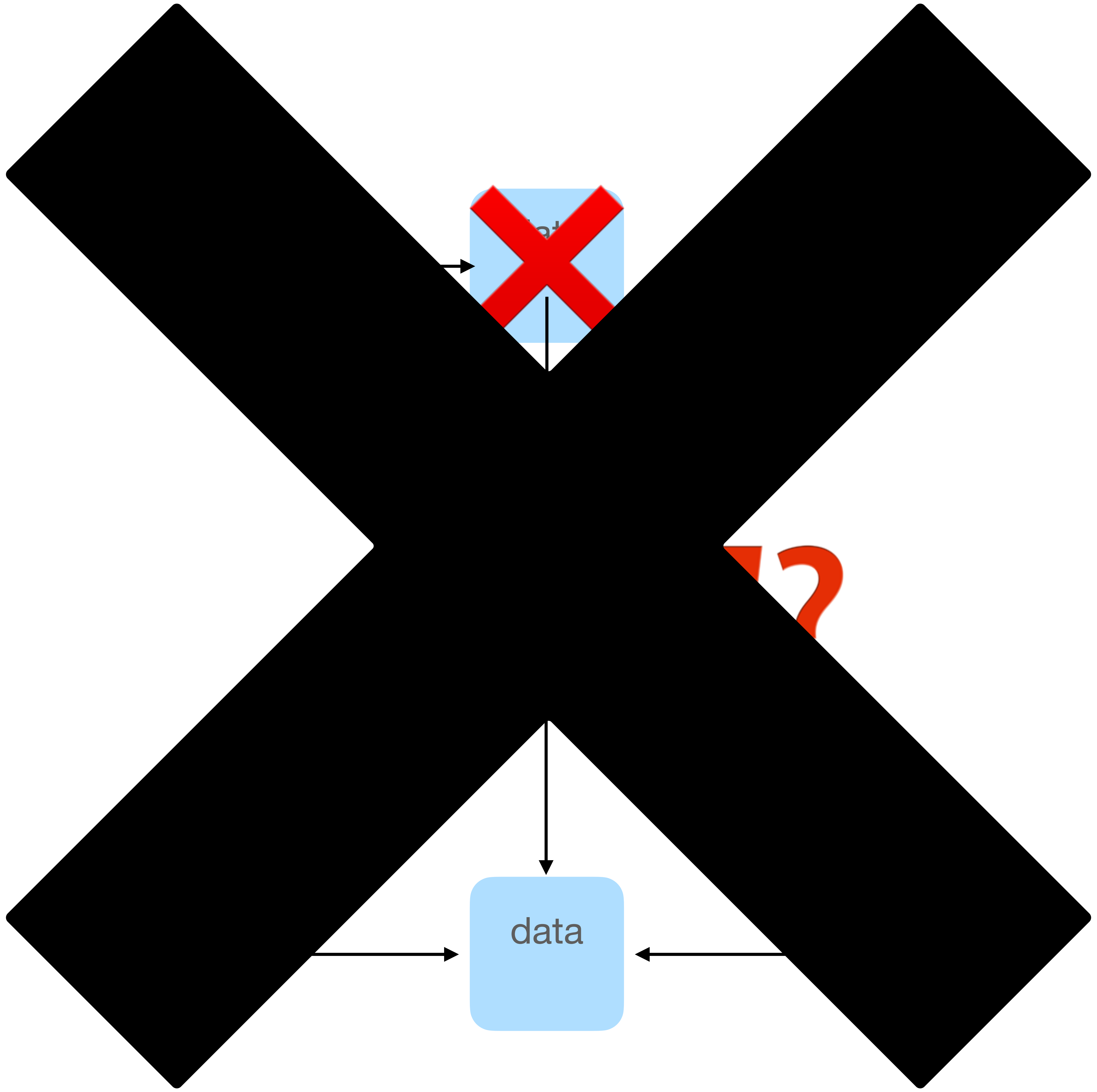
ABA



N ::= protect(top) | @inv active (TOS) | skip

Memory Reclamation

N;
top = TOS;
N;
next = top.next;
N;
CAS(TOS, top, next);
N;
retire(top);
N;



N ::= protect(top) | @inv active (TOS) | skip

Contribution 3:

Instantiation on SMR Setting

Data Structure	Treiber's Stack Pop	Treiber's Stack Push	Michael and Scott's Queue Enqueue	Michael and Scott's Queue Dequeue	ORVYY Set Add	ORVYY Set Remove
SMR Algorithm	HP1 (5 Base Types)	HP1 (5 Base Types)	HP1 (5 Base Types)	HP2 (8 Base Types)	HP2 (8 Base Types)	HP2 (8 Base Types)
Time (PO + Synth)	< 0.1s	< 0.1s	< 0.1s	< 7.5s	< 0.9s	< 0.4s
Max / Avg |R|	6 / 1.4	6 / 1.7	5 / 1.4	90 / 1.4	28 / 1.7	30 / 1.3

Conclusion

Conclusion

Summary

- 1: Realizability Logic
- 2: Realization Logic
- 3: Made Programs Memory Safe

$$\vdash_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \models_a \langle R \rangle \texttt{sketch} \langle S \rangle$$

$$\vdash_a \langle R \rangle \mathsf{po} \langle S \rangle \wedge \langle R \rangle \mathsf{po} \langle S \rangle \mathrel{\vdash\!\sim} \langle R' \rangle \mathsf{po}' \langle S' \rangle$$
$$\Longrightarrow \quad \vdash_a \langle R' \rangle \mathsf{po}' \langle S' \rangle$$

Conclusion

Summary

- 1: Realizability Logic
- 2: Realization Logic
- 3: Made Programs Memory Safe

$$\vdash_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \models_a \langle R \rangle \texttt{sketch} \langle S \rangle$$

$$\vdash_a \langle R \rangle \texttt{po} \langle S \rangle \wedge \langle R \rangle \texttt{po} \langle S \rangle \mathrel{|\!\sim} \langle R' \rangle \texttt{po}' \langle S' \rangle$$
$$\Longrightarrow \quad \vdash_a \langle R' \rangle \texttt{po}' \langle S' \rangle$$

Future Work

- SyGuS benchmarks
- Assertion Language

Conclusion

Summary

- 1: Realizability Logic
- 2: Realization Logic
- 3: Made Programs Memory Safe

$$\vdash_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \models_a \langle R \rangle \texttt{sketch} \langle S \rangle$$

$$\vdash_a \langle R \rangle \texttt{po} \langle S \rangle \wedge \langle R \rangle \texttt{po} \langle S \rangle \mathrel{|\!\sim} \langle R' \rangle \texttt{po}' \langle S' \rangle$$
$$\Longrightarrow \quad \vdash_a \langle R' \rangle \texttt{po}' \langle S' \rangle$$

Future Work

- SyGuS benchmarks
- Assertion Language

$$\langle x = 0 \wedge y = 0, x = 0 \wedge y = 1 \rangle$$

Conclusion

Summary

- 1: Realizability Logic
- 2: Realization Logic
- 3: Made Programs Memory Safe

$$\vdash_a \langle R \rangle \texttt{sketch} \langle S \rangle \quad \Leftrightarrow \quad \models_a \langle R \rangle \texttt{sketch} \langle S \rangle$$

$$\vdash_a \langle R \rangle \texttt{po} \langle S \rangle \wedge \langle R \rangle \texttt{po} \langle S \rangle \mathrel{|\!\sim} \langle R' \rangle \texttt{po}' \langle S' \rangle$$
$$\implies \quad \vdash_a \langle R' \rangle \texttt{po}' \langle S' \rangle$$

Future Work

- SyGuS benchmarks
- Assertion Language

$$\langle x = 0 \wedge y = 0, x = 0 \wedge y = 1 \rangle$$

$$\langle x = 0 \wedge \{y = 0, y = 1\} \rangle$$

Conclusion

Thanks for your attention!

Summary

- 1: Realizability Logic
- 2: Realization Logic
- 3: Made Programs Memory Safe

$$\vdash_a \langle R\rangle \mathtt{sketch} \langle S\rangle \quad \Leftrightarrow \quad \models_a \langle R\rangle \mathtt{sketch} \langle S\rangle$$

$$\vdash_a \langle R\rangle \mathtt{po} \langle S\rangle \wedge \langle R\rangle \mathtt{po} \langle S\rangle \mathrel{|\!\sim} \langle R'\rangle \mathtt{po}' \langle S'\rangle$$
$$\Longrightarrow \quad \vdash_a \langle R'\rangle \mathtt{po}' \langle S'\rangle$$

Future Work

- SyGuS benchmarks
- Assertion Language

$$\langle x = 0 \wedge y = 0, x = 0 \wedge y = 1\rangle$$

$$\langle x = 0 \wedge \{y = 0, y = 1\}\rangle$$