# Special Topics in Logic and Security 1

## Variable and Memory Space Analysis

Paul Irofti

Master Year II, Sem. I, 2022-2023

# How to detect buffer overflow

Often exploited software defects can be reduced to the following snippet:

```
char buf[10];
i = 0;
while (i < 20) {
    buf[i] = i;
    i = i + 1;
}
```

How do current tools behave when encountering this sequence?

How can we use static analysis to find such defects?

# Example: C routine

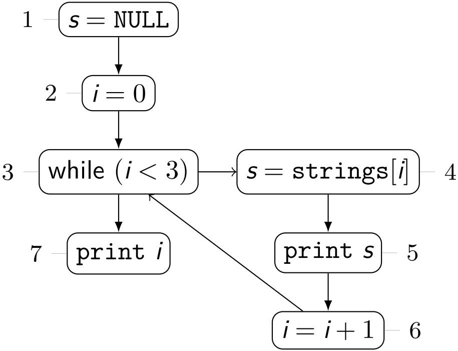
```c
char *strings[] = { "One", "Two", "Three" };

char *s = NULL;
int i;

for (i = 0; i < 3; i++) {
    s = strings[i];
    printf("%s\n", s);
}

printf("%d\n", i);
```

# Example: IMP and CFG adaptation



# Preliminaries

We denote

- $v_n^i$ – the possible values of variable $i$ in nodes $n = \overline{1,6}$
- $v_n^s$ – the memory addresses towards which $s$ points to in nodes $n = \overline{1,6}$

We describe the values of $i$ as an interval and those of $s$ as an abstract set of addersses $\mathcal{A}$.

- `strings[i]` represents the address of string $i$
- we store this address as $s_i \in \mathcal{A}$ for $i \in \{1, 2, 3\}$
- we denote void, zero, or uninitialized addresses with `NULL` or $\emptyset$

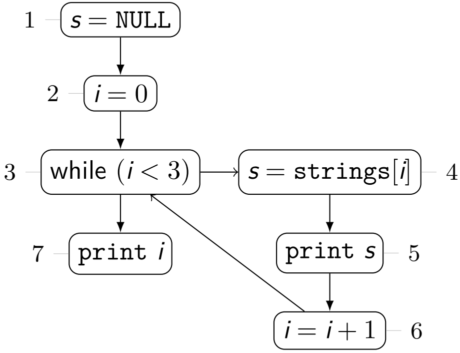
For the constraints system we will need the operator

$$[\ell_1, u_1] \, \overline{\Upsilon} \, [\ell_2, u_2] = [\min(\ell_1, \ell_2), \max(u_1, u_2)]$$

that computes the minimum range containing both given ranges.

# Example: ranges

$$
\begin{aligned}
v_1^i &= [0,0] \\
v_2^i &= [0,0] \\
v_3^i &= v_2^i \,\overline{\Upsilon}\, v_6^i \\
v_4^i &= v_3^i \cap \left[-2^{31}, 2\right] \\
v_5^i &= v_4^i \cap \left[-2^{31}, 2\right] \\
v_6^i &= \left\{ v + 1 \mid v \in v_5^i \right\} \\
v_7^i &= v_3^i \cap \left[3, 2^{31} - 1\right]
\end{aligned}
$$



1 $s = \texttt{NULL}$

2 $i = 0$

3 while $(i < 3)$

4 $s = \texttt{strings}[i]$

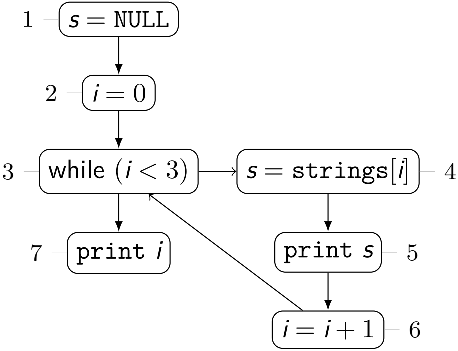
5 $\texttt{print}\ s$

6 $i = i + 1$

7 $\texttt{print}\ i$

# Example: addresses

$$
\begin{aligned}
v_1^s &= \emptyset \\
v_2^s &= v_1^s \\
v_3^s &= v_2^s \cup v_6^s \\
v_4^s &= \{s_1 \mid 0 \in v_4^i\} \cup \\
&\phantom{=} \{s_2 \mid 1 \in v_4^i\} \cup \\
&\phantom{=} \{s_3 \mid 2 \in v_4^i\} \\
v_5^s &= v_4^s \\
v_6^s &= v_5^s \\
v_7^s &= v_3^s
\end{aligned}
$$



# Example: resulting equations

Ranges

$$\begin{aligned}
v_1^i &= [0,0] \\
v_2^i &= [0,0] \\
v_3^i &= v_2^i \,\overline{\Upsilon}\, v_6^i \\
v_4^i &= v_3^i \cap \left[-2^{31}, 2\right] \\
v_5^i &= v_4^i \cap \left[-2^{31}, 2\right] \\
v_6^i &= \left\{ v+1 \mid v \in v_5^i \right\} \\
v_7^i &= v_3^i \cap \left[3, 2^{31}-1\right]
\end{aligned}$$

Addresses

$$\begin{aligned}
v_1^s &= \emptyset \\
v_2^s &= v_1^s \\
v_3^s &= v_2^s \cup v_6^s \\
v_4^s &= \left\{ s_1 \mid 0 \in v_4^i \right\} \cup \\
&\quad\; \left\{ s_2 \mid 1 \in v_4^i \right\} \cup \\
&\quad\; \left\{ s_3 \mid 2 \in v_4^i \right\} \\
v_5^s &= v_4^s \\
v_6^s &= v_5^s \\
v_7^s &= v_3^s
\end{aligned}$$

Remark

*Note the link between the values domain of i represented as ranges and the domain of `pointer` s represented as a set of addresses.*

# Solving with the Fixed Point Theorem

The solution to the above equations can be obtained through the fixed point theorem:

- start from the initial state $\bot = (\emptyset, \ldots, \emptyset)$
- iterates towards the top of the lattice with $F^n(\bot) = F(F^{n-1}(\bot))$
- here each unknown $x_j \in \{x_1, \ldots, x_n\}$ represents a tuple consisting of the range $x_j^i$ and the address set $x_j^s$
- denote the initial state $x_j^i = \bot$ and $x_j^s = \emptyset$ such that $x_j = \bot = \langle \bot, \emptyset \rangle$

**Exercise:** Determine the least fixed point:

| | $x_1^i$ | $x_1^s$ | $x_2^i$ | $x_2^s$ | $x_3^i$ | $x_3^s$ | $x_4^i$ | $x_4^s$ | $x_5^i$ | $x_5^s$ | $x_6^i$ | $x_6^s$ | $x_7^i$ | $x_7^s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\bot$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| $F(\bot)$ | $\bot$ | $\{\texttt{NULL}\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| $F^2(\bot)$ | $\bot$ | $\{\texttt{NULL}\}$ | $[0, 0]$ | $\{\texttt{NULL}\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |

# Solution: Determining the Least Fixed Point

| | $x_1^i$ | $x_1^s$ | $x_2^i$ | $x_2^s$ | $x_3^i$ | $x_3^s$ | $x_4^i$ | $x_4^s$ | $x_5^i$ | $x_5^s$ | $x_6^i$ | $x_6^s$ | $x_7^i$ | $x_7^s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\perp$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 1 | $\perp$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 2 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 3 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |

# Solution: Determining the Least Fixed Point

| | $x_1^i$ | $x_1^s$ | $x_2^i$ | $x_2^s$ | $x_3^i$ | $x_3^s$ | $x_4^i$ | $x_4^s$ | $x_5^i$ | $x_5^s$ | $x_6^i$ | $x_6^s$ | $x_7^i$ | $x_7^s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\perp$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 1 | $\perp$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 2 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 3 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 4 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\texttt{NULL}\}$ |

# Solution: Determining the Least Fixed Point

|  | $x_1^i$ | $x_1^s$ | $x_2^i$ | $x_2^s$ | $x_3^i$ | $x_3^s$ | $x_4^i$ | $x_4^s$ | $x_5^i$ | $x_5^s$ | $x_6^i$ | $x_6^s$ | $x_7^i$ | $x_7^s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\perp$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 1 | $\perp$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 2 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 3 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 4 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 5 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\texttt{NULL}\}$ |

# Solution: Determining the Least Fixed Point

|  | $x_1^i$ | $x_1^s$ | $x_2^i$ | $x_2^s$ | $x_3^i$ | $x_3^s$ | $x_4^i$ | $x_4^s$ | $x_5^i$ | $x_5^s$ | $x_6^i$ | $x_6^s$ | $x_7^i$ | $x_7^s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\perp$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 1 | $\perp$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 2 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 3 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 4 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 5 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 6 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\perp$ | $\{\texttt{NULL}\}$ |

# Solution: Determining the Least Fixed Point

| | $x_1^i$ | $x_1^s$ | $x_2^i$ | $x_2^s$ | $x_3^i$ | $x_3^s$ | $x_4^i$ | $x_4^s$ | $x_5^i$ | $x_5^s$ | $x_6^i$ | $x_6^s$ | $x_7^i$ | $x_7^s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\perp$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 1 | $\perp$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 2 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 3 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 4 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 5 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 6 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 7 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,1]$ | $\{\texttt{NULL}, s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\perp$ | $\{\texttt{NULL}\}$ |

# Solution: Determining the Least Fixed Point

| | $x_1^i$ | $x_1^s$ | $x_2^i$ | $x_2^s$ | $x_3^i$ | $x_3^s$ | $x_4^i$ | $x_4^s$ | $x_5^i$ | $x_5^s$ | $x_6^i$ | $x_6^s$ | $x_7^i$ | $x_7^s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\bot$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| 1 | $\bot$ | {NULL} | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| 2 | $\bot$ | {NULL} | $[0,0]$ | {NULL} | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| 3 | $\bot$ | {NULL} | $[0,0]$ | {NULL} | $[0,0]$ | {NULL} | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| 4 | $\bot$ | {NULL} | $[0,0]$ | {NULL} | $[0,0]$ | {NULL} | $[0,0]$ | $\{s_1\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | {NULL} |
| 5 | $\bot$ | {NULL} | $[0,0]$ | {NULL} | $[0,0]$ | {NULL} | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $\bot$ | $\emptyset$ | $\bot$ | {NULL} |
| 6 | $\bot$ | {NULL} | $[0,0]$ | {NULL} | $[0,0]$ | {NULL} | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\bot$ | {NULL} |
| 7 | $\bot$ | {NULL} | $[0,0]$ | {NULL} | $[0,1]$ | {NULL, $s_1$} | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\bot$ | {NULL} |
| 8 | $\bot$ | {NULL} | $[0,0]$ | {NULL} | $[0,1]$ | {NULL, $s_1$} | $[0,1]$ | $\underline{\{s_1, s_2\}}$ | $[0,1]$ | $\underline{\{s_1, s_2\}}$ | $[1,1]$ | $\underline{\{s_1, s_2\}}$ | $\bot$ | $\underline{\{\texttt{NULL}, s_1}$ |

# Solution: Determining the Least Fixed Point

| | $x_1^i$ | $x_1^s$ | $x_2^i$ | $x_2^s$ | $x_3^i$ | $x_3^s$ | $x_4^i$ | $x_4^s$ | $x_5^i$ | $x_5^s$ | $x_6^i$ | $x_6^s$ | $x_7^i$ | $x_7^s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\bot$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| 1 | $\bot$ | $\{\mathtt{NULL}\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| 2 | $\bot$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| 3 | $\bot$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| 4 | $\bot$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\{\mathtt{NULL}\}$ |
| 5 | $\bot$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\{\mathtt{NULL}\}$ |
| 6 | $\bot$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\bot$ | $\{\mathtt{NULL}\}$ |
| 7 | $\bot$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,1]$ | $\{\mathtt{NULL}, s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\bot$ | $\{\mathtt{NULL}\}$ |
| 8 | $\bot$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,1]$ | $\{\mathtt{NULL}, s_1\}$ | $[0,1]$ | $\underline{\{s_1, s_2\}}$ | $[0,1]$ | $\underline{\{s_1, s_2\}}$ | $[1,1]$ | $\underline{\{s_1, s_2\}}$ | $\bot$ | $\underline{\{\mathtt{NULL}, s_1}$ |
| 9 | $\bot$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,1]$ | $\{\mathtt{NULL}, s_1\}$ | $[0,1]$ | $\{s_1, s_2\}$ | $[0,1]$ | $\{s_1, s_2\}$ | $\underline{[1,2]}$ | $\{s_1, s_2\}$ | $\bot$ | $\{\mathtt{NULL}, s_1$ |

# Solution: Determining the Least Fixed Point

| | $x_1^i$ | $x_1^s$ | $x_2^i$ | $x_2^s$ | $x_3^i$ | $x_3^s$ | $x_4^i$ | $x_4^s$ | $x_5^i$ | $x_5^s$ | $x_6^i$ | $x_6^s$ | $x_7^i$ | $x_7^s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\bot$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| 1 | $\bot$ | $\{\texttt{NULL}\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| 2 | $\bot$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| 3 | $\bot$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ |
| 4 | $\bot$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\emptyset$ | $\bot$ | $\{\texttt{NULL}\}$ |
| 5 | $\bot$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $\bot$ | $\emptyset$ | $\bot$ | $\{\texttt{NULL}\}$ |
| 6 | $\bot$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\bot$ | $\{\texttt{NULL}\}$ |
| 7 | $\bot$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,1]$ | $\{\texttt{NULL}, s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\bot$ | $\{\texttt{NULL}\}$ |
| 8 | $\bot$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,1]$ | $\{\texttt{NULL}, s_1\}$ | $[0,1]$ | $\underline{\{s_1, s_2\}}$ | $[0,1]$ | $\underline{\{s_1, s_2\}}$ | $[1,1]$ | $\underline{\{s_1, s_2\}}$ | $\bot$ | $\underline{\{\texttt{NULL}, s_1}$ |
| 9 | $\bot$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,1]$ | $\{\texttt{NULL}, s_1\}$ | $[0,1]$ | $\{s_1, s_2\}$ | $[0,1]$ | $\{s_1, s_2\}$ | $\underline{[1,2]}$ | $\{s_1, s_2\}$ | $\bot$ | $\{\texttt{NULL}, s_1$ |
| 10 | $\bot$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\underline{[0,2]}$ | $\underline{\{\texttt{NULL}, s_1, s_2\}}$ | $[0,2]$ | $\{s_1, s_2\}$ | $[0,2]$ | $\{s_1, s_2\}$ | $[1,2]$ | $\{s_1, s_2\}$ | $\bot$ | $\{\texttt{NULL}, s_1,$ |

# Solution: Determining the Least Fixed Point

| | $x_1^i$ | $x_1^s$ | $x_2^i$ | $x_2^s$ | $x_3^i$ | $x_3^s$ | $x_4^i$ | $x_4^s$ | $x_5^i$ | $x_5^s$ | $x_6^i$ | $x_6^s$ | $x_7^i$ | $x_7^s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\perp$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 1 | $\perp$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 2 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 3 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 4 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 5 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 6 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 7 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,1]$ | $\{\texttt{NULL}, s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 8 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,1]$ | $\{\texttt{NULL}, s_1\}$ | $[0,1]$ | $\underline{\{s_1, s_2\}}$ | $[0,1]$ | $\underline{\{s_1, s_2\}}$ | $[1,1]$ | $\underline{\{s_1, s_2\}}$ | $\perp$ | $\underline{\{\texttt{NULL}, s_1}$ |
| 9 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,1]$ | $\{\texttt{NULL}, s_1\}$ | $[0,1]$ | $\{s_1, s_2\}$ | $[0,1]$ | $\{s_1, s_2\}$ | $\underline{[1,2]}$ | $\{s_1, s_2\}$ | $\perp$ | $\{\texttt{NULL}, s_1$ |
| 10 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\underline{[0,2]}$ | $\underline{\{\texttt{NULL}, s_1, s_2\}}$ | $[0,2]$ | $\{s_1, s_2\}$ | $[0,2]$ | $\{s_1, s_2\}$ | $[1,2]$ | $\{s_1, s_2\}$ | $\perp$ | $\{\texttt{NULL}, s_1,$ |
| 11 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,2]$ | $\{\texttt{NULL}, s_1, s_2, s_3\}$ | $[0,2]$ | $\underline{\{s_1, s_2, s_3\}}$ | $[0,2]$ | $\{s_1, s_2, s_3\}$ | $[1,2]$ | $\{s_1, s_2, s_3\}$ | $\perp$ | $\{\texttt{NULL}, s_1,$ |

# Solution: Determining the Least Fixed Point

| | $x_1^i$ | $x_1^s$ | $x_2^i$ | $x_2^s$ | $x_3^i$ | $x_3^s$ | $x_4^i$ | $x_4^s$ | $x_5^i$ | $x_5^s$ | $x_6^i$ | $x_6^s$ | $x_7^i$ | $x_7^s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\perp$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 1 | $\perp$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 2 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 3 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 4 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 5 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 6 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 7 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,1]$ | $\{\texttt{NULL}, s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\perp$ | $\{\texttt{NULL}\}$ |
| 8 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,1]$ | $\{\texttt{NULL}, s_1\}$ | $[0,1]$ | $\underline{\{s_1, s_2\}}$ | $[0,1]$ | $\underline{\{s_1, s_2\}}$ | $[1,1]$ | $\underline{\{s_1, s_2\}}$ | $\perp$ | $\underline{\{\texttt{NULL}, s_1}$ |
| 9 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,1]$ | $\{\texttt{NULL}, s_1\}$ | $[0,1]$ | $\{s_1, s_2\}$ | $[0,1]$ | $\{s_1, s_2\}$ | $\underline{[1,2]}$ | $\{s_1, s_2\}$ | $\perp$ | $\{\texttt{NULL}, s_1$ |
| 10 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $\underline{[0,2]}$ | $\underline{\{\texttt{NULL}, s_1, s_2\}}$ | $[0,2]$ | $\{s_1, s_2\}$ | $[0,2]$ | $\{s_1, s_2\}$ | $[1,2]$ | $\{s_1, s_2\}$ | $\perp$ | $\{\texttt{NULL}, s_1,$ |
| 11 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,2]$ | $\{\texttt{NULL}, s_1, s_2, s_3\}$ | $[0,2]$ | $\underline{\{s_1, s_2, s_3\}}$ | $[0,2]$ | $\{s_1, s_2, s_3\}$ | $[1,2]$ | $\{s_1, s_2, s_3\}$ | $\perp$ | $\{\texttt{NULL}, s_1,$ |
| 12 | $\perp$ | $\{\texttt{NULL}\}$ | $[0,0]$ | $\{\texttt{NULL}\}$ | $[0,2]$ | $\{\texttt{NULL}, s_1, s_2, s_3\}$ | $[0,2]$ | $\{s_1, s_2, s_3\}$ | $[0,2]$ | $\{s_1, s_2, s_3\}$ | $\underline{[1,3]}$ | $\{s_1, s_2, s_3\}$ | $\perp$ | $\{\texttt{NULL}, s_1,$ |

# Solution: Determining the Least Fixed Point

| | $x_1^i$ | $x_1^s$ | $x_2^i$ | $x_2^s$ | $x_3^i$ | $x_3^s$ | $x_4^i$ | $x_4^s$ | $x_5^i$ | $x_5^s$ | $x_6^i$ | $x_6^s$ | $x_7^i$ | $x_7^s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\perp$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 1 | $\perp$ | $\{\mathtt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 2 | $\perp$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 3 | $\perp$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ |
| 4 | $\perp$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\mathtt{NULL}\}$ |
| 5 | $\perp$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $\perp$ | $\emptyset$ | $\perp$ | $\{\mathtt{NULL}\}$ |
| 6 | $\perp$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\perp$ | $\{\mathtt{NULL}\}$ |
| 7 | $\perp$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,1]$ | $\{\mathtt{NULL}, s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[0,0]$ | $\{s_1\}$ | $[1,1]$ | $\{s_1\}$ | $\perp$ | $\{\mathtt{NULL}\}$ |
| 8 | $\perp$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,1]$ | $\{\mathtt{NULL}, s_1\}$ | $[0,1]$ | $\underline{\{s_1, s_2\}}$ | $[0,1]$ | $\underline{\{s_1, s_2\}}$ | $[1,1]$ | $\underline{\{s_1, s_2\}}$ | $\perp$ | $\underline{\{\mathtt{NULL}, s_1}$ |
| 9 | $\perp$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,1]$ | $\{\mathtt{NULL}, s_1\}$ | $[0,1]$ | $\{s_1, s_2\}$ | $[0,1]$ | $\{s_1, s_2\}$ | $\underline{[1,2]}$ | $\{s_1, s_2\}$ | $\perp$ | $\{\mathtt{NULL}, s_1$ |
| 10 | $\perp$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $\underline{[0,2]}$ | $\underline{\{\mathtt{NULL}, s_1, s_2\}}$ | $[0,2]$ | $\{s_1, s_2\}$ | $[0,2]$ | $\{s_1, s_2\}$ | $[1,2]$ | $\{s_1, s_2\}$ | $\perp$ | $\{\mathtt{NULL}, s_1,$ |
| 11 | $\perp$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,2]$ | $\{\mathtt{NULL}, s_1, s_2, s_3\}$ | $[0,2]$ | $\underline{\{s_1, s_2, s_3\}}$ | $[0,2]$ | $\{s_1, s_2, s_3\}$ | $[1,2]$ | $\{s_1, s_2, s_3\}$ | $\perp$ | $\{\mathtt{NULL}, s_1,$ |
| 12 | $\perp$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $[0,2]$ | $\{\mathtt{NULL}, s_1, s_2, s_3\}$ | $[0,2]$ | $\{s_1, s_2, s_3\}$ | $[0,2]$ | $\{s_1, s_2, s_3\}$ | $\underline{[1,3]}$ | $\{s_1, s_2, s_3\}$ | $\perp$ | $\{\mathtt{NULL}, s_1,$ |
| 13 | $\perp$ | $\{\mathtt{NULL}\}$ | $[0,0]$ | $\{\mathtt{NULL}\}$ | $\underline{[0,3]}$ | $\{\mathtt{NULL}, s_1, s_2, s_3\}$ | $[0,2]$ | $\{s_1, s_2, s_3\}$ | $[0,2]$ | $\{s_1, s_2, s_3\}$ | $[1,3]$ | $\{s_1, s_2, s_3\}$ | $\underline{[3,3]}$ | $\{\mathtt{NULL}, s_1,$ |

# Remarks

- program execution can be traced in the equations semantic
- a join operation of two paths is depicted in the equations as a union operation
- a fork of two paths (or meet) can be identified in the equations as a an intersection operation
- the $\perp$ symbol denotes states that can not be reached (yet); this point in the program state is also called unreachable
- the $x_7^s$ points of iterations 4–12 do not make sense because the corresponding code is unreachable due to $x_7^i$ that is $\perp$ for 4–12 $\implies x_7^s = \perp$ for 4–12
- the join operations are domain specific: simple sets union for addresses or the complex $\overline{\Upsilon}$ operation for ranges
- in the former example the meet operations exist only for intervals

**Conclusion:** simultaneously using two domains at a time leads to new observations and new types of analysis that are based on the interaction between the two (domain interaction).

# *Num* Lattice

In general the domains and associated operations form a lattice.

### Definition

*Num* is the numerical domain bounding the possible values a variable can have.

### Theorem

$(Num, \leq_N, \vee_N, \wedge_N)$ *forms a lattice.*

- $\leq_N$ *is the inclusion operator* $\subset$
- $\vee_N = \overline{\Upsilon}$ *is the join operator for ranges*
- $\wedge_N$ *is the meet operation for ranges*

$$\vee_N : Num \rightarrow Num \times Num, \qquad \forall x, y \in Num \qquad x \vee_N y := \sup\{x, y\}$$
$$\wedge_N : Num \rightarrow Num \times Num, \qquad \forall x, y \in Num \qquad x \wedge_N y := \inf\{x, y\}$$

# Proof *Num* Lattice

Theorem

$(Num, \subset, \overline{\Upsilon}, \wedge_N)$ *forms a lattice.*

$(Num, \subset)$ POSET: Let $a \leq b \leq c \leq d \in \mathbb{N}$

- reflexive: $x \in Num \implies x \subset x$ ;
  $[a, b] \subset [a, b]$ ex. $[1, 3] \subset [1, 3]$
- anti-symmetric: $x, y \in Num$ and $x \subset y, y \subset x \implies x = y$ ;
  $[a, b] \subset [a, c]$ , $[a, c] \not\subset [a, b]$, but $[a, c] \subset [a, c] \implies [a, c] = [a, c]$
  ex. $[1, 3] \subset [1, 5]$ , $[1, 5] \not\subset [1, 3]$, but $[1, 5] \subset [1, 5] \implies [1, 5] = [1, 5]$
- transitivity: $x, y, z \in Num$ and $x \subset y, y \subset z \implies x \subset z$ ;
  $[a, b] \subset [a, c]$ , $[a, c] \subset [a, d] \implies [a, b] \subset [a, d]$
  ex. $[1, 3] \subset [1, 4]$ , $[1, 4] \subset [1, 5] \implies [1, 3] \subset [1, 5]$

Lattice: Let $\overline{\Upsilon}, \wedge_N$ with $x, y, z \in Num$

- associative: $(x \vee_N y) \vee_N z = x \vee_N (y \vee_N z)$ ; $(x \wedge_N y) \wedge_N z = x \wedge_N (y \wedge_N z)$
- commute: $x \vee_N y = y \vee_N x$ ; $x \wedge_N y = y \wedge_N x$
- absorb: $x \vee_N (y \wedge_N z) = x$ ; $x \wedge_N (y \vee_N z) = x$

# *Pts* Lattice

Definition

*Pts* is the address pointer domain (points-to) used to represent the address spaces towards which a pointer can point.

Theorem

$(Pts, \leq_A, \vee_A, \wedge_A)$ *forms a lattice.*

- *what is* $\leq_A$*?*
- $\vee_A = \cup$ *is the join operation for addresses*
- *what is* $\wedge_A$*?*

# The Pts Abstract Domain

### Definition

Define $\mathcal{X}$ the finite set of variables of a program $P$ and $\mathcal{A}$ the finite set of addresses towards which these variables can point.

Then $Pts = \mathcal{X} \rightarrow \mathcal{P}(\mathcal{A})$ represents the function that ties each variable $x \in \mathcal{X}$ to a subset of addresses $A(x) \in \mathcal{A}$.

Let $A_1, A_2, A' \in Pts$.

**Update:** $A \in Pts$ becomes $A' = \{A \cup [x \rightarrow a] \mid a \in \mathcal{A}\}$ such that $A'(x) = a$ and $A'(y) = A(y), \forall y \neq x$.

**Order:** $A_1 \leq_A A_2 \iff A_1(x) \subseteq A_2(x)$, $\forall x \in \mathcal{X}$

**Join:** $A' = A_1 \vee_A A_2$ s.t. $A'(x) = A_1(x) \cup A_2(x)$, $\forall x \in \mathcal{X}$.

**Meet:** The meet operation can be seen as an update operation that helps us filter the elements of $A$.

**Conclusion:** $(Pts, \leq_A)$ forms a CPO: for any subset configuration $B \in \mathcal{P}(Pts)$ there exists $A \in Pts$ such that $A = \bigvee_A B \implies$ we can apply Kleene iterations.

# Exercise

What can we say about p? What does static analysis tell us?

```
int a, b, *p;
p = NULL;
if (rand())
    p = & a;
if (p)
    *p = 42;
```