# Special Topics in Logic and Security 1

Variable and Memory Space Analysis

Paul Irofti

Master Year II, Sem. I, 2021-2022

#### 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;
}</pre>
```

How do current tools behave when encountering this sequence?

How can we use static analysis to find such defects?

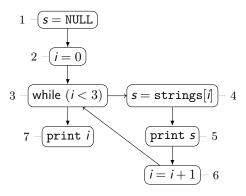
#### Example: C routine

```
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);</pre>
```

### 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 A.

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

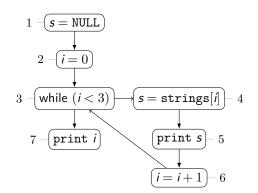
For the constraints system we will need the operator

$$\left[\ell_{1}, u_{1}\right] \overline{\Upsilon}\left[\ell_{2}, u_{2}\right] = \left[\min\left(\ell_{1}, \ell_{2}\right), \max\left(u_{1}, u_{2}\right)\right]$$

that computes the minimum range containing both given ranges.

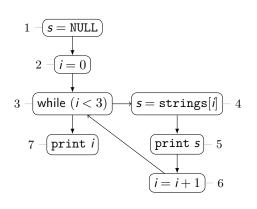
## Example: ranges

$$\begin{array}{rcl} \mathbf{v}_{1}^{i} & = & [0,0] \\ \mathbf{v}_{2}^{i} & = & [0,0] \\ \mathbf{v}_{3}^{i} & = & \mathbf{v}_{2}^{i} \overline{\Upsilon} \mathbf{v}_{6}^{i} \\ \mathbf{v}_{4}^{i} & = & \mathbf{v}_{3}^{i} \cap \left[-2^{31},2\right] \\ \mathbf{v}_{5}^{i} & = & \mathbf{v}_{4}^{i} \cap \left[-2^{31},2\right] \\ \mathbf{v}_{6}^{i} & = & \left\{\mathbf{v}+1 \mid \mathbf{v} \in \mathbf{v}_{5}^{i}\right\} \\ \mathbf{v}_{7}^{i} & = & \mathbf{v}_{3}^{i} \cap \left[3,2^{31}-1\right] \end{array}$$



### Example: addresses

$$\begin{array}{rcl} \textit{v}_{5}^{\textit{s}} & = & \emptyset \\ \\ \textit{v}_{2}^{\textit{s}} & = & \textit{v}_{1}^{\textit{s}} \\ \\ \textit{v}_{3}^{\textit{s}} & = & \textit{v}_{2}^{\textit{s}} \cup \textit{v}_{6}^{\textit{s}} \\ \\ \textit{v}_{4}^{\textit{s}} & = & \left\{ \textit{s}_{1} \mid 0 \in \textit{v}_{4}^{\textit{j}} \right\} \cup \\ & \left\{ \textit{s}_{2} \mid 1 \in \textit{v}_{4}^{\textit{j}} \right\} \cup \\ & \left\{ \textit{s}_{3} \mid 2 \in \textit{v}_{4}^{\textit{j}} \right\} \\ \\ \textit{v}_{5}^{\textit{s}} & = & \textit{v}_{4}^{\textit{s}} \\ \\ \textit{v}_{6}^{\textit{s}} & = & \textit{v}_{5}^{\textit{s}} \\ \\ \textit{v}_{7}^{\textit{s}} & = & \textit{v}_{3}^{\textit{s}} \\ \end{array}$$



### Example: resulting equations

Range	es		Addı	esses	5
$v_1^i$	=	[0, 0]	$v_1^s$	=	Ø
$v_2^j$	=	[0, 0]	$V_2^s$	=	$v_1^s$
$v_3^i$	=	$v_2^i \overline{\Upsilon} v_6^i$	$V_3^s$	=	$v_2^s \cup v_6^s$
$v_4^i$	=	$\mathbf{v}_3^i\cap\left[-2^{31},2 ight]$	$v_4^{s}$	=	$\left\{ \mathbf{s}_{1}\mid0\in\mathbf{v}_{4}^{\mathbf{j}}\right\} \cup$
$v_5^i$	=	$\textit{v}_{4}^{\textit{j}} \cap \left[-2^{31},2\right]$			$\left\{ \mathbf{s}_{2}\mid1\in\mathbf{v}_{4}^{i}\right\} \cup$
$v_6^i$	=	$\left\{ v+1\mid v\in v_{5}^{i}\right\}$			$\left\{ \mathbf{s}_{3}\mid2\in\mathbf{v}_{4}^{\mathbf{j}}\right\}$
$v_7^i$	=	$v_3^i \cap \left[3, 2^{31} - 1\right]$	$V_5^{\rm S}$	=	$V_4^s$
			$v_6^s$	=	$V_5^s$
			$V_7^{s}$	=	$v_3^s$

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

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

	$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	$x_3^s$	$x_4^i$	$x_4^s$	$x_5^i$	$x_5^s$	$x_6^i$	$x_6^s$	$x_7^i$	$X_7^{s}$
	1	Ø	1	Ø	1	Ø	1	Ø	1	Ø	1	Ø	1	Ø
$F(\perp)$	1	$\{\mathtt{NULL}\}$	1	Ø	_	Ø	1	Ø	_	Ø	1	Ø	_	Ø
$F^2(\perp)$	上	$\{\mathtt{NULL}\}$	[0, 0]	$\{\mathtt{NULL}\}$	_	$\emptyset$	1	Ø	1	Ø	Τ	Ø	_	Ø
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:

	$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	$x_3^s$	3	$x_4^i$ $x$	د 4	$x_5^i$	$x_5^s$	$x_6^i$	$x_6^s$	$x_7^i$	$X_7^s$	
Τ.	Τ.	Ø		Ø	Τ	Ø		⊥ ∅	)	Τ.	Ø		Ø	Τ	Ø	
1	$\perp$	{NULL}	$\perp$	Ø	$\perp$	Ø		⊥ ∅	)	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	
2	$\perp$	{NULL}	[0, 0]	{NULL}	$\perp$	Ø		⊥ ∅	)	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	
3		{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}		⊥ Ø	)	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	

	,		,		,		;		,				,	
	$x'_1$	$x_1^s$	$x_2'$	$x_2^s$	$x_3'$	x3	$x_4'$	$x_4^s$	$x_5'$	$x_5^{s}$	$x_6'$	$x_6^s$	$x_7'$	X <sup>5</sup> 7
	 Τ	Ø	Τ.	Ø	Τ	Ø	Τ.	Ø	Τ	Ø		Ø	Τ.	Ø
1	$\perp$	{NULL}	$\perp$	Ø	1	Ø	1	Ø		Ø		Ø		Ø
2	$\perp$	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	$\perp$	Ø		Ø	$\perp$	Ø		Ø
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø		Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	$\perp$	Ø	Τ.	Ø		$\{\mathtt{NULL}\}$

	$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	$x_3^s$	$x_4^i$	$x_4^s$	$x_5^i$	$x_5^s$	$x_6^i$	$x_6^s$	$x_7^i$	<i>x</i> <sub>7</sub> <sup>s</sup>
Τ.		Ø		Ø	Τ	Ø	Τ.	Ø	1	Ø		Ø	1	Ø
1	$\perp$	$\{NULL\}$	$\perp$	Ø	$\perp$	Ø		Ø	1	Ø	$\perp$	Ø		Ø
2	$\perp$	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø	1	Ø	$\perp$	Ø		Ø
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø		Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	1	Ø	$\perp$	Ø		{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	$\perp$	Ø		{NULL}

	$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	x <sub>3</sub> <sup>s</sup>	$x_4^i$	$x_4^s$	$x_5^i$	$x_5^s$	$x_6^i$	$x_6^s$	$x_7^i$	<i>X</i> <sup>S</sup> <sub>7</sub>
Τ	Τ.	Ø	Τ.	Ø	Τ	Ø	Τ.	Ø	Τ.	Ø		Ø	Τ.	Ø
1	$\perp$	{NULL}	$\perp$	Ø	$\perp$	Ø	1	Ø	1	Ø	$\perp$	Ø	$\perp$	Ø
2	$\perp$	{NULL}	[0, 0]	$\{NULL\}$	$\perp$	Ø		Ø	$\perp$	Ø	$\perp$	Ø	1	Ø
3	$\perp$	$\{NULL\}$	[0, 0]	$\{NULL\}$	[0, 0]	{NULL}		Ø	$\perp$	Ø	$\perp$	Ø	1	Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	1	Ø	$\perp$	Ø	$\perp$	{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	$\perp$	Ø	$\perp$	{NULL}
6	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	$\perp$	{NULL}

	$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	<i>x</i> <sub>3</sub> <sup>s</sup>	$x_4^i$	$x_4^s$	$x_5^i$	$x_5^s$	$x_6^i$	$x_6^s$	$x_7^i$	<i>x</i> <sub>7</sub> <sup>s</sup>
		Ø	Τ.	Ø	1	Ø	1	Ø	1	Ø	1	Ø	1	Ø
1	$\perp$	{NULL}	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	1	Ø
2	$\perp$	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	$\perp$	Ø	$\perp$	Ø	$\perp$	{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	$\perp$	Ø	$\perp$	{NULL}
6	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	$\perp$	{NULL}
7	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	$\perp$	{NULL}

		$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	$x_3^s$	$x_4^i$	$x_4^s$	$x_5^i$	$x_5^s$	$x_6^i$	$x_6^s$	$x_7^i$	$X_7^s$
_	1	Τ	Ø		Ø	Τ	Ø	Τ	Ø	Τ	Ø	1	Ø	Τ	Ø
	1	$\perp$	{NULL}	$\perp$	Ø	$\perp$	Ø	1	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø
	2	$\perp$	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø
	3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø
	4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	$\perp$	Ø	$\perp$	Ø	$\perp$	{NULL}
	5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	$\perp$	Ø	$\perp$	{NULL}
	6	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	$\perp$	{NULL}
	7	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	$\perp$	{NULL}
	8	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\{s_1, s_2\}$	[0, 1]	$\{s_1, s_2\}$	[1, 1]	$\{s_1, s_2\}$	$\perp$	$\{NULL, s_1\}$

	$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	<i>x</i> <sub>3</sub> <sup>s</sup>	$x_4^i$	$x_4^s$	$x_5^i$	<i>X</i> <sup><i>S</i></sup> <sub>5</sub>	$x_6^i$	$x_6^s$	$x_7^i$	X <sup>S</sup> <sub>7</sub>
1		Ø	1	Ø	I	Ø	1	Ø	1	Ø	I	Ø		Ø
1	$\perp$	{NULL}	$\perp$	Ø	$\perp$	Ø	1	Ø	$\perp$	Ø	$\perp$	Ø	1	Ø
2	$\perp$	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	1	Ø	$\perp$	Ø	$\perp$	Ø	1	Ø
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	1	Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	$\perp$	Ø	$\perp$	Ø	1	{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	$\perp$	Ø	1	{NULL}
6	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	1	{NULL}
7	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$		{NULL}
8	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\{s_1, s_2\}$	[0, 1]	$\{s_1, s_2\}$	[1, 1]	$\{s_1, s_2\}$	$\perp$	$\{NULL, s_1\}$
9	$\perp$	$\{\mathtt{NULL}\}$	[0, 0]	$\{\mathtt{NULL}\}$	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\overline{\{s_1, s_2\}}$	[0, 1]	$\overline{\{s_1,s_2\}}$	[1, 2]	$\overline{\{s_1, s_2\}}$	$\perp$	$\{NULL, s_1\}$

	. i	. 5	i	5	.i	.5	.i	5	.i	5	. i	5	. i	XS
	$x_1'$	$x_1^s$	$x_2'$	$x_2^s$	$x_3'$	<i>x</i> <sub>3</sub> <sup>s</sup>	$x_4'$	$x_4^s$	$x_5'$	$x_5^s$	$x_6'$	$x_6^s$	$x_7'$	X7
Τ	Τ	Ø	Τ.	Ø	1	Ø	Τ	Ø	Τ	Ø	1	Ø	Τ.	Ø
1	$\perp$	{NULL}	$\perp$	Ø	1	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø
2	$\perp$	{NULL}	[0, 0]	{NULL}	1	Ø	$\perp$	Ø	$\perp$	Ø	1	Ø	$\perp$	Ø
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	$\perp$	Ø	1	Ø	$\perp$	{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	1	Ø	$\perp$	{NULL}
6	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	$\perp$	{NULL}
7	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	$\perp$	{NULL}
8	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\{s_1, s_2\}$	[0, 1]	$\{s_1, s_2\}$	[1, 1]	$\{s_1, s_2\}$	$\perp$	$\{NULL, s_1$
9	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\{s_1, s_2\}$	[0, 1]	$\overline{\{s_1, s_2\}}$	[1, 2]	$\overline{\{s_1, s_2\}}$	$\perp$	$\{NULL, s_1\}$
10	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 2]	$\{NULL, s_1, s_2\}$	[0, 2]	$\{s_1, s_2\}$	[0, 2]	$\{s_1, s_2\}$	[1, 2]	$\{s_1, s_2\}$	$\perp$	$\{NULL, s_1$

Τ	Τ	Ø	Τ.	Ø	Τ	Ø	Τ.	Ø	Τ	Ø		Ø	Τ	Ø
1	$\perp$	{NULL}	$\perp$	Ø	1	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	1	Ø
2	$\perp$	{NULL}	[0, 0]	{NULL}	1	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	1	Ø
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	$\perp$	Ø	$\perp$	Ø	$\perp$	{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	$\perp$	Ø	1	{NULL}
6	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	1	{NULL}
7	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	1	{NULL}
8	$\perp$	${NULL}$	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\{s_1, s_2\}$	[0, 1]	$\{s_1, s_2\}$	[1, 1]	$\{s_1, s_2\}$	$\perp$	$\{NULL, s_1\}$
9	$\perp$	{NULL}	[0, 0]	$\{NULL\}$	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\overline{\{s_1, s_2\}}$	[0, 1]	$\overline{\{s_1, s_2\}}$	[1, 2]	$\overline{\{s_1, s_2\}}$	$\perp$	$\{NULL, s_1\}$
10	$\perp$	{NULL}	[0, 0]	$\{NULL\}$	[0, 2]	$\{NULL, s_1, s_2\}$	[0, 2]	$\{s_1, s_2\}$	[0, 2]	$\{s_1, s_2\}$	[1, 2]	$\{s_1, s_2\}$	$\perp$	$\{NULL, s_1\}$
11	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 2]	$\{NULL, s_1, s_2, s_3\}$	[0, 2]	$\{s_1, s_2, s_3\}$	[0, 2]	$\{s_1, s_2, s_3\}$	[1, 2]	$\{s_1, s_2, s_3\}$	$\perp$	$\{NULL, s_1\}$

	$x_1$	$x_1$	$x_2$	$x_2$	$x_3$	<i>x</i> <sub>3</sub>	$x_4$	$x_4^{\omega}$	$x_5$	$x_5^2$	$x_6$	$x_6$	$x_7$	X7
Τ	$\perp$	Ø	Τ.	Ø	T	Ø	Τ.	Ø	Τ	Ø	Τ.	Ø	Τ	Ø
1	$\perp$	{NULL}	$\perp$	Ø	1	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø
2	$\perp$	{NULL}	[0, 0]	{NULL}	1	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø
3	$\perp$	$\{NULL\}$	[0, 0]	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø	$\perp$	Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	$\perp$	Ø	$\perp$	Ø	$\perp$	{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	$\perp$	Ø	$\perp$	{NULL}
6	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	$\perp$	{NULL}
7	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	$\perp$	{NULL}
8	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\{s_1, s_2\}$	[0, 1]	$\{s_1, s_2\}$	[1, 1]	$\{s_1, s_2\}$	$\perp$	$\{NULL, s_1$
9	$\perp$	$\{NULL\}$	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\overline{\{s_1, s_2\}}$	[0, 1]	$\overline{\{s_1, s_2\}}$	[1, 2]	$\overline{\{s_1, s_2\}}$	$\perp$	$\{NULL, s_1\}$
10	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 2]	$\{\mathtt{NULL}, s_1, s_2\}$	[0, 2]	$\{s_1, s_2\}$	[0, 2]	$\{s_1, s_2\}$	[1, 2]	$\{s_1, s_2\}$	$\perp$	$\{NULL, s_1$
11	$\perp$	$\{NULL\}$	[0, 0]	{NULL}	[0, 2]	$\overline{\{\text{NULL}, s_1, s_2, s_3\}}$	[0, 2]	$\{s_1, s_2, s_3\}$	[0, 2]	$\{s_1, s_2, s_3\}$	[1, 2]	$\{s_1, s_2, s_3\}$	$\perp$	$\{NULL, s_1$
12	$\perp$	$\{NULL\}$	[0, 0]	$\{NULL\}$	[0, 2]	$\{\mathtt{NULL}, s_1, s_2, s_3\}$	[0, 2]	$\{s_1, s_2, s_3\}$	[0, 2]	$\{s_1, s_2, s_3\}$	[1, 3]	$\{s_1, s_2, s_3\}$	$\perp$	$\{NULL, s_1$

	$ x_1^i $	<i>X</i> <sub>1</sub> <sup>S</sup>	$x_2^i$	$x_2^s$	l vi	vs	$x_4^i$	$X_4^s$	$x_5^i$	vs	$x_6^i$	$x_6^s$	$X_7^i$	X <sup>S</sup> <sub>7</sub>
_	^1		^2		x' <sub>3</sub>	x <sub>3</sub> s	^4		^5	x <sub>5</sub>	^6		^7	
$\perp$	1 1	Ø	1	Ø	1	Ø	1	Ø	⊥	Ø	1	Ø	1	Ø
1	1	$\{NULL\}$	$\perp$	Ø	1	Ø	1	Ø	1	Ø	$\perp$	Ø	1	Ø
2	1	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø	1	Ø		Ø	1	Ø
3	1	{NULL}	[0, 0]	$\{NULL\}$	[0, 0]	{NULL}	1	Ø	1	Ø	$\perp$	Ø	1	Ø
4	1	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	1	Ø		Ø	1	{NULL}
5	1	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$		Ø	1	{NULL}
6	1	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	1	{NULL}
7	1	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	[1, 1]	$\{s_1\}$	1	{NULL}
8	1	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{\mathtt{NULL}, s_1\}$	[0, 1]	$\{s_1, s_2\}$	[0, 1]	$\{s_1, s_2\}$	[1, 1]	$\{s_1, s_2\}$	1	$\{NULL, s_1\}$
9	1	{NULL}	[0, 0]	$\{NULL\}$	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\overline{\{s_1, s_2\}}$	[0, 1]	$\overline{\{s_1, s_2\}}$	[1, 2]	$\overline{\{s_1, s_2\}}$	1	$\{NULL, s_1\}$
10	)	{NULL}	[0, 0]	$\{NULL\}$	[0, 2]	$\{\mathtt{NULL}, s_1, s_2\}$	[0, 2]	$\{s_1, s_2\}$	[0, 2]	$\{s_1, s_2\}$	$\overline{[1,2]}$	$\{s_1, s_2\}$	1	$\{NULL, s_1\}$
11	.   _	{NULL}	[0, 0]	{NULL}	[0, 2]	$\overline{\{NULL, s_1, s_2, s_3\}}$	[0, 2]	$\{s_1, s_2, s_3\}$	[0, 2]	$\{s_1, s_2, s_3\}$	[1, 2]	$\{s_1, s_2, s_3\}$	1	$\{NULL, s_1\}$
12	1	{NULL}	[0, 0]	{NULL}	[0, 2]	$\{NULL, s_1, s_2, s_3\}$	[0, 2]	$\{s_1, s_2, s_3\}$	[0, 2]	$\{s_1, s_2, s_3\}$	[1, 3]	$\{s_1, s_2, s_3\}$	1	$\{NULL, s_1\}$
13		{NULL}	[0, 0]	{NULL}	[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]	$\{s_1,s_2,s_3\}$	[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 <u>meet</u>) can be identified in the equations as a an intersection operation
- the  $\bot$  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 <u>unreachable</u> due to  $x_7^i$  that is  $\perp$  for 4–12  $\implies x_7^s = \perp$  for 4–12
- the <u>join</u> 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

#### 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  $Pts = \mathcal{X} \to \mathcal{P}(\mathcal{A})$  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  $A' = \{A \cup [x \rightarrow a] \mid a \in A\}$  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:**  $A' = A_1 \vee_A A_2$  a.î.  $A'(x) = A_1(x) \cup A_2(x)$ ,  $\forall x \in \mathcal{X}$ .

**Meet:** The  $\underline{\text{meet}}$  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;
```