### Topici speciale în logică și securitate l

Analiza variabilelor și adreselor de memorie

Paul Irofti

Master anul II, Sem. I, 2019-2020

#### Cum putem detecta buffer overflow

Tipul de defecte software ce sunt exploatate adesea iau forma:

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

Cum se comportă tool-urile existente când întâlnesc o astfel de secvență?

Cum putem folosi analiza statică să găsim astfel de defecte?

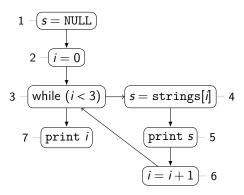
#### Exemplu: rutină C

```
char *strings[] = { "Unu", "doi", "trei" };
char *s = NULL;
int i;

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

printf("%d\n", i);</pre>
```

### Exemplu: Adaptare IMP și CFG



#### Convenții și notații

#### Notăm cu

- $v_n^i$  valorile posibile ale variabilei i în nodurile  $n = \overline{1,6}$
- $v_n^s$  adresele de memorie către care s poate indica în nodurile  $n = \overline{1,6}$

Descriem valorile lui i drept un interval și pe cele ale lui s drept un set abstract de adrese  $\mathcal{A}$ .

- strings[i] oferă adresa șirului i
- păstrăm această adresă drept  $s_i \in \mathcal{A}$  pentru  $i \in 1, 2, 3$
- ullet notăm cu NULL sau  $\emptyset$  adresa vidă, zero, neinițializată

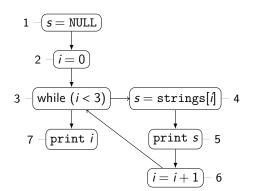
În sistemul de constrângeri vom avea nevoie de operatorul

$$[l_1, u_1] \overline{\Upsilon} [l_2, u_2] = [\min (l_1, l_2), \max (u_1, u_2)]$$

ce calculează intervalul minim ce conține cele două intervale date.

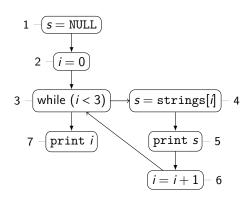
#### Exemplu: intervale

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



#### Exemplu: adrese

$$\begin{array}{rcl} v_{1}^{s} & = & \emptyset \\ v_{2}^{s} & = & v_{1}^{s} \\ v_{3}^{s} & = & v_{2}^{s} \cup v_{6}^{s} \\ v_{4}^{s} & = & \left\{ s_{1} \mid 0 \in v_{4}^{i} \right\} \cup \\ & \left\{ s_{2} \mid 1 \in v_{4}^{i} \right\} \cup \\ & \left\{ s_{3} \mid 2 \in v_{4}^{i} \right\} \\ v_{5}^{s} & = & v_{4}^{s} \\ v_{6}^{s} & = & v_{5}^{s} \\ v_{7}^{s} & = & v_{3}^{s} \end{array}$$



#### Exemplu: ecuațiile rezultate

Observați legătura dintre domeniul valorilor lui i reprezentate drept intervale și cel al pointer-ului s reprezentat ca seturi de adrese.

#### Intervale

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

#### Adrese

$$\begin{array}{rcl} v_{1}^{s} & = & \emptyset \\ v_{2}^{s} & = & v_{1}^{s} \\ v_{3}^{s} & = & v_{2}^{s} \cup v_{6}^{s} \\ v_{4}^{s} & = & \left\{ s_{1} \mid 0 \in v_{4}^{i} \right\} \cup \\ & & \left\{ s_{2} \mid 1 \in v_{4}^{i} \right\} \cup \\ & & \left\{ s_{3} \mid 2 \in v_{4}^{i} \right\} \end{array}$$

$$\begin{array}{rcl} v_{5}^{s} & = & v_{4}^{s} \\ v_{6}^{s} & = & v_{5}^{s} \\ v_{7}^{s} & = & v_{2}^{s} \end{array}$$

#### Rezolvarea folosind teorema de punct fix

Soluția ecuațiilor de mai sus poate fi obținută cu teorema de punct fix:

- pornim de la starea inițială  $\bot = (\emptyset, ..., \emptyset)$
- iterăm către vârful laticei cu  $F^n(\bot) = F(F^{n-1}(\bot))$
- aici fiecare necunoscută  $x_j \in \{x_1, \dots, x_n\}$  reprezintă un tuplu alcătuit din intervalul  $x_i^i$  și setul adreselor  $x_i^s$
- notăm starea inițială  $x_j^i = \bot$  și  $x_j^s = \emptyset$  astfel încât  $x_j = \bot = \langle \bot, \emptyset \rangle$

Exercițiu: Determinarea celui mai mic punct fix:

	$X_1^i$	$X_1^s$	$X_2^i$	$X_2^s$	$X_3^i$	$x_3^s$	$X_4^i$	$X_4^s$	$X_5^i$	$x_5^s$	$x_6^i$	$x_6^s$	$X_7^i$	$x_7^s$
	1	Ø	1		1	Ø	1	Ø	1	Ø	1	Ø	上	Ø
$F(\perp)$		$\{NULL\}$		Ø	上	Ø	上	Ø	1	Ø	上	Ø	上	Ø
$F^{2}(\perp)$	_	{NULL}	[0, 0]	{NULL}	1	Ø	上	Ø	1	Ø	1	Ø	上	Ø
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:

	$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	$X_3^s$	$x_4^i$	$X_4^s$	;	x <sub>5</sub>	$X_5^s$	$x_6^i$	$x_6^s$	$x_7^i$	x <sub>7</sub> <sup>s</sup>	
1	Τ	Ø	Τ	Ø	Τ	Ø	1	Ø		T	Ø	Т	Ø	Τ	Ø	
1	$\perp$	{NULL}	1	Ø	1	Ø	1	Ø		L	Ø	1	Ø		Ø	
2	$\perp$	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø		L	Ø	1	Ø		0	
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	1	Ø		L	Ø	1	Ø	1	Ø	

	$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	$x_3^s$	$x_4^i$	$x_4^s$	$x_5^i$	$X_5^s$	$x_6^i$	$x_6^s$	$x_7^i$	x <sup>s</sup> <sub>7</sub>
	Τ	Ø	1	Ø	Τ	0	1	Ø	1	Ø	1	0	Τ (	D
1	$\perp$	{NULL}	$\perp$	Ø	1	Ø	1	Ø		Ø	1	Ø	Ι (	D
2	$\perp$	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø	1	Ø	1	Ø	⊥ (	D
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø	1	Ø	⊥ (	D
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0,0]	{s <sub>1</sub> }	1	Ø	1	0	⊥ {	(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	Т	Ø	Т	Ø	1	Ø	1	Ø	1	Ø	Τ	Ø
1	$\perp$	{NULL}	$\perp$	Ø	$\perp$	Ø	1	0	1	Ø		Ø	Τ.	Ø
2	$\perp$	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø	1	Ø		Ø	1	Ø
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø		Ø	1	Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	1	Ø		Ø	1	{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	[0, 0]	$\{s_1\}$	1	Ø	Τ.	{NULL}

	$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	$x_3^s$	$x_4^i$	$X_4^s$	$x_5^i$	<i>x</i> <sub>5</sub> <sup>5</sup>	$x_6^i$	$x_6^s$	$x_7^i$	x <sub>7</sub> s
	Τ	Ø	Τ	0	Т	0	Τ	Ø	Т	Ø	Τ	Ø	Τ	0
1	$\perp$	{NULL}	1	Ø	1	Ø	1	Ø	1	Ø	1	Ø	1	Ø
2	$\perp$	{NULL}	[0, 0]	{NULL}	$\perp$	0	1	0	1	0	1	0	1	0
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	1	0	1	0	1	0	1	0
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	1	Ø	1	Ø	1	{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	1	Ø	1	{NULL}
6	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	[1, 1]	{s <sub>1</sub> }	1	{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>
	I	0	Ţ	0	1	Ø	1	Ø	1	Ø	1	Ø	1	0
1	$\perp$	{NULL}	1	Ø	1	Ø	1	Ø	1	Ø	1	0	1	Ø
2	_	{NULL}	[0, 0]	{NULL}	1	0	1	Ø	1	Ø	1	Ø	1	Ø
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	1	0	1	0	1	0	$\perp$	Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	1	Ø	1	0	$\perp$	{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0,0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	1	0	$\perp$	{NULL}
6	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0,0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	[1, 1]	{s <sub>1</sub> }	$\perp$	{NULL}
7	- 1	{NULL!}	[0.0]	{NULL:	[0. 1]	{NULL, s <sub>1</sub> }	[0.0]	{s <sub>1</sub> }	[0.0]	{s <sub>1</sub> }	Î1. 1Î	{s <sub>1</sub> }	1	{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 <sub>7</sub> <sup>s</sup>
	Τ	Ø	Τ	Ø	Т	Ø	Т	0	Τ	0	Т	Ø	Τ	Ø
1	$\perp$	{NULL}	1	Ø	1	0	1	Ø	1	Ø	$\perp$	Ø	1	Ø
2	$\perp$	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	1	Ø	1	Ø	1	Ø	1	0
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø	$\perp$	Ø	1	Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	$\{s_1\}$	1	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 <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	[1, 1]	{s <sub>1</sub> }	1	{NULL}
7	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	[1, 1]	{s <sub>1</sub> }	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]	$\{s_1, s_2\}$	$\perp$	$\{NULL, s_1\}$

	$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	$X_3^s$	$X_4^i$	$x_4^s$	$x_5^i$	$x_5^s$	$x_6^i$	$x_6^s$	$x_7^i$	x <sub>7</sub> <sup>s</sup>
	Τ	Ø	Τ	0	Т	Ø	Τ	Ø	Τ	0	Τ	Ø	Τ	0
1	$\perp$	{NULL}	1	Ø	1	0	1	Ø	1	Ø	1	Ø	$\perp$	Ø
2	$\perp$	{NULL}	[0, 0]	{NULL}	$\perp$	Ø	1	Ø	1	Ø	1	0	$\perp$	Ø
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø	1	0	$\perp$	Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	1	Ø	1	0	$\perp$	{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	[0, 0]	$\{s_1\}$	1	Ø	$\perp$	{NULL}
6	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	[1, 1]	{s <sub>1</sub> }	$\perp$	{NULL}
7	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	[1, 1]	{s <sub>1</sub> }	$\perp$	{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]	$\{s_1, s_2\}$	[1, 2]	{s <sub>1</sub> , s <sub>2</sub> }	$\perp$	$\{NULL, s_1\}$

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

	$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	$X_3^s$	$X_4^i$	$x_4^s$	$x_5^i$	$x_5^s$	$x_6^i$	$x_6^s$	$x_7^i$	x <sub>7</sub> <sup>s</sup>
1	Τ	Ø	Τ	Ø	Τ	Ø	Τ	Ø	Τ	Ø	Τ	Ø	Т	0
1	1	{NULL}	1	Ø	1	Ø	1	Ø	1	Ø	1	Ø	1	0
2	$\perp$	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø	1	Ø	1	Ø	$\perp$	Ø
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø	1	Ø	$\perp$	Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	1	Ø	1	Ø	1	{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0,0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	1	Ø	1	{NULL}
6	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	[1, 1]	{s <sub>1</sub> }	1	{NULL}
7	1	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	[1, 1]	{s <sub>1</sub> }	1	{NULL}
8	1	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\{s_1, s_2\}$	[0, 1]	$\{s_1, s_2\}$	[1, 1]	$\{s_1, s_2\}$	1	$\{NULL, s_1\}$
9	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\{s_1, s_2\}$	[0, 1]	$\{s_1, s_2\}$	[1, 2]	$\{s_1, s_2\}$	1	$\overline{\{\text{NULL}, s_1\}}$
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]	$\{s_1, s_2\}$	1	$\{NULL, s_1, s_2\}$
11	Τ	{NULL}	[0, 0]	{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]	$\{s_1,s_2,s_3\}$	$\perp$	$\{\mathtt{NULL}, s_1, s_2, s_3\}$

	$x_1^i$	$x_1^s$	$x_2^i$	$X_2^s$	$x_3^i$	$x_3^s$	$X_4^i$	$X_4^s$	$x_5^i$	$X_5^s$	$x_6^i$	$x_6^s$	$x_7^i$	x <sub>7</sub> s
	Τ	Ø	Τ	Ø	Τ	Ø	Τ	Ø	Τ	Ø	Τ	Ø	Т	Ø
1	$\perp$	{NULL}	1	Ø	1	Ø	1	Ø	1	Ø	1	Ø	$\perp$	Ø
2	$\perp$	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø	1	Ø	1	Ø	$\perp$	Ø
3	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø	1	Ø	$\perp$	Ø
4	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	1	Ø	1	Ø	$\perp$	{NULL}
5	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	1	Ø	$\perp$	{NULL}
6	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	[1, 1]	{s <sub>1</sub> }	$\perp$	{NULL}
7	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	[1, 1]	{s <sub>1</sub> }	$\perp$	{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]	$\{s_1, s_2\}$		$\{NULL, s_1\}$
9	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\{s_1, s_2\}$	[0, 1]	$\{s_1, s_2\}$	[1, 2]	$\{s_1, s_2\}$	$\perp$	$\overline{\{\text{NULL}, s_1\}}$
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]	$\{s_1, s_2\}$	$\perp$	$\{NULL, s_1, s_2\}$
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]	$\{s_1, s_2, s_3\}$	$\perp$	$\{\mathtt{NULL}, s_1, s_2, s_3\}$
12	$\perp$	{NULL}	[0, 0]	{NULL}	[0, 2]	$\{\mathtt{NULL}, s_1, s_2, s_3\}$	[0, 2]	$\overline{\{s_1, s_2, s_3\}}$	[0, 2]	$\{s_1,s_2,s_3\}$	[1, 3]	$\{s_1,s_2,s_3\}$	$\perp$	$\{\mathtt{NULL}, s_1, s_2, s_3\}$

	$x_1^i$	$x_1^s$	$x_2^i$	$x_2^s$	$x_3^i$	$x_3^s$	$x_4^i$	$\chi_4^s$	$x_5^i$	<i>x</i> <sub>5</sub> <sup>s</sup>	$x_6^i$	$x_6^s$	$x_7^i$	x <sub>7</sub> <sup>s</sup>
	1	Ø	1	Ø	1	0	Τ	Ø	Τ	Ø	1	Ø	1	0
1	1	{NULL}	1	Ø	1	0	Τ.	Ø	1	Ø	1	Ø	1	0
2	1	{NULL}	[0, 0]	{NULL}	1	0	1	Ø	1	Ø	1	Ø	1	Ø
3	1	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	1	Ø	1	Ø	1	Ø	1	Ø
4	1	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	1	Ø	1	Ø	1	{NULL}
5	1	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	1	Ø	1	{NULL}
6	1	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	[1, 1]	{s <sub>1</sub> }	1	{NULL}
7	1	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 0]	{s <sub>1</sub> }	[0, 0]	{s <sub>1</sub> }	[1, 1]	{s <sub>1</sub> }	1	{NULL}
8	1	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\{s_1, s_2\}$	[0, 1]	$\{s_1, s_2\}$	[1, 1]	$\{s_1, s_2\}$	1	$\{NULL, s_1\}$
9	1	{NULL}	[0, 0]	{NULL}	[0, 1]	$\{NULL, s_1\}$	[0, 1]	$\{s_1, s_2\}$	[0, 1]	$\{s_1, s_2\}$	[1, 2]	$\{s_1, s_2\}$	1	$\overline{\{\text{NULL}, s_1\}}$
10	1	{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]	$\{s_1, s_2\}$	1	$\{NULL, s_1, s_2\}$
11	1	{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, 2]	$\{s_1, s_2, s_3\}$	1	$\{\mathtt{NULL}, s_1, s_2, s_3\}$
12	1	{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]	$\{s_1,s_2,s_3\}$	1	$\{\mathtt{NULL}, s_1, s_2, s_3\}$
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]	$\{\mathtt{NULL}, s_1, s_2, s_3\}$

# Observații

- execuția programului poate fi observată în semantica ecuaților
- o operație de join a două căi este regăsită drept o operație de reuniune în ecuații
- o operație de bifurcare (sau meet) a două căi este regăsită drept o operație de intersecție în ecuații
- simbolul ⊥ indică stări ce nu pot fi atinse (încă); acest punct în program se mai numește unreachable
- punctele  $x_7^s$  de la iterațiile 4–12 nu au sens deoarece codul aferent este unreachable datorită  $x_7^i$  care este  $\bot$  de la 4–12  $\Longrightarrow x_7^s = \bot$  pentru 4–12
- operațiile de *join* depind de domeniu: reuniune simplă de seturi pentru adrese sau operația complexă  $\overline{\Upsilon}$  pentru intervale
- în exemplul anterior operațiile de *meet* sunt regăsite doar la intervale

**Concluzie:** utilizarea a două domenii simultan duce la noi observații și tipuri de analiză ce se bazează pe interacțiunea dintre cele două (*domain interaction*).

#### Latice

În general domeniile și operațiile aferente formează o latice.

**Definiție:** *Num* este domeniul numeric ce mărginește valorile posibile luate de o variabilă.

**Definiție:** *Pts* este domeniul indicatorilor către adrese (*points-to*) ce reprezintă zonele de memorie către care un *pointer* poate indica.

**Teoremă:**  $(Num, \leq_N, \vee_N, \wedge_N)$  formează o latice.

- ≤<sub>N</sub> este operatorul de incluziune ⊂
- $\vee_N = \overline{\Upsilon}$  este operația de *join* pentru intervale
- ∧<sub>N</sub> este operația de meet pentru intervale

**Teoremă:**  $(Pts, \leq_A, \vee_A, \wedge_A)$  formează o latice.

- cine este  $\leq_A$ ?
- $\vee_A = \cup$  este operația de *join* pentru adrese
- cine este ∧<sub>A</sub>?

#### Domeniul abstract Pts

Definim X setul finit al variabilelor existente într-un program P și  $\mathcal{A}$  setul finit al adreselor către care pot indica aceste variabile.

Atunci  $Pts = X \to \mathcal{P}(\mathcal{A})$  reprezintă funcția ce leagă fiecare variabilă  $x \in X$  de un subset de adrese  $A(x) \in \mathcal{A}$ .

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

**Actualizare:**  $A \in Pts$  devine  $A' = \{A \cup [x \rightarrow a] \mid a \in \mathcal{A}\}$  astfel încât A'(x) = a și  $A'(y) = A(y), \forall y \neq x$ .

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

**Join:**  $A' = A_1 \vee_A A_2$  a.î.  $A'(x) = A_1(x) \cup A_2(x)$ ,  $\forall x \in X$ .

**Meet:** Operația de *meet* poate fi privită ca o operație de actualizare cu ajutorul căreia filtrăm elementele din *A*.

**Concluzie:**  $(Pts, \leq_A)$  reprezintă un CPO: pentru orice configurație de subseturi  $B \in \mathcal{P}(Pts)$  există  $A \in Pts$  astfel încât  $A = \bigvee_A B \Longrightarrow$  putem aplica iterații *Kleene*.

#### Exerciții

Ce putem spune despre p? Ce ne spune analiza statică?

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