

Topici speciale în logică și securitate I

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;  
}
```

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

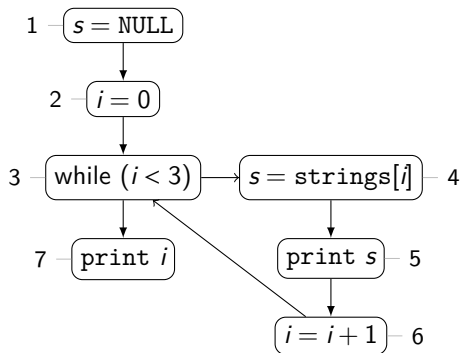
```
char *strings[] = { "Unu", "doi", "trei" };

char *s = NULL;
int i;

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

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

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 $i \in 1, 2, 3$
- notăm cu `NULL` sau \emptyset adresa vidă, zero, neinițializată

În sistemul de constrângeri vom avea nevoie de operatorul

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

ce calculează intervalul minim ce conține cele două intervale date.

Exemplu: intervale

$$v_1^i = [0, 0]$$

$$v_2^i = [0, 0]$$

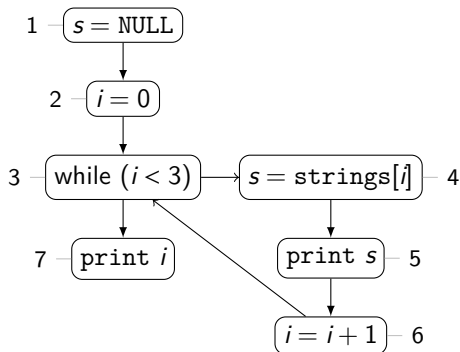
$$v_3^i = v_2^i \overline{\cap} v_6^i$$

$$v_4^i = v_3^i \cap [-2^{31}, 2]$$

$$v_5^i = v_4^i \cap [-2^{31}, 2]$$

$$v_6^i = \{v + 1 \mid v \in v_5^i\}$$

$$v_7^i = v_3^i \cap [3, 2^{31} - 1]$$



Exemplu: adrese

$$v_1^s = \emptyset$$

$$v_2^s = v_1^s$$

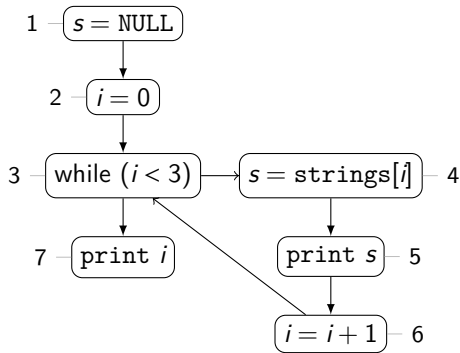
$$v_3^s = v_2^s \cup v_6^s$$

$$v_4^s = \{s_1 \mid 0 \in v_4^i\} \cup \\ \{s_2 \mid 1 \in v_4^i\} \cup \\ \{s_3 \mid 2 \in v_4^i\}$$

$$v_5^s = v_4^s$$

$$v_6^s = v_5^s$$

$$v_7^s = v_3^s$$



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

$$v_1^i = [0, 0]$$

$$v_2^i = [0, 0]$$

$$v_3^i = v_2^i \overline{\cap} v_6^i$$

$$v_4^i = v_3^i \cap [-2^{31}, 2]$$

$$v_5^i = v_4^i \cap [-2^{31}, 2]$$

$$v_6^i = \{v + 1 \mid v \in v_5^i\}$$

$$v_7^i = v_3^i \cap [3, 2^{31} - 1]$$

Adrese

$$v_1^s = \emptyset$$

$$v_2^s = v_1^s$$

$$v_3^s = v_2^s \cup v_6^s$$

$$v_4^s = \{s_1 \mid 0 \in v_4^i\} \cup$$

$$\{s_2 \mid 1 \in v_4^i\} \cup$$

$$\{s_3 \mid 2 \in v_4^i\}$$

$$v_5^s = v_4^s$$

$$v_6^s = v_5^s$$

$$v_7^s = v_3^s$$

Rezolvarea folosind teorema de punct fix

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

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

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
\perp	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
$F(\perp)$	\perp	$\{\text{NULL}\}$	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
$F^2(\perp)$	\perp	$\{\text{NULL}\}$	$[0, 0]$	$\{\text{NULL}\}$	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots

Soluție: Determinarea celui mai mic punct fix

	x_1^j	x_1^s	x_2^j	x_2^s	x_3^j	x_3^s	x_4^j	x_4^s	x_5^j	x_5^s	x_6^j	x_6^s	x_7^j	x_7^s
\perp	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
1	\perp	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
2	\perp	{NULL}	[0, 0]	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
3	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset

Soluție: 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
\perp	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
1	\perp	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
2	\perp	{NULL}	[0, 0]	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
3	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
4	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	\perp	\emptyset	\perp	\emptyset	\perp	{NULL}

Soluție: 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
\perp	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
1	\perp	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
2	\perp	{NULL}	[0, 0]	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
3	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
4	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	\perp	\emptyset	\perp	\emptyset	\perp	{NULL}
5	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	\perp	\emptyset	\perp	{NULL}

Soluție: Determinarea celui mai mic punct fix

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

Soluție: 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
\perp	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
1	\perp	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
2	\perp	{NULL}	[0, 0]	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
3	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
4	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{ s_1 }	\perp	\emptyset	\perp	\emptyset	\perp	{NULL}
5	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{ s_1 }	[0, 0]	{ s_1 }	\perp	\emptyset	\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}

Soluție: 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
\perp	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
1	\perp	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
2	\perp	{NULL}	[0, 0]	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
3	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
4	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{ s_1 }	\perp	\emptyset	\perp	\emptyset	\perp	{NULL}
5	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{ s_1 }	[0, 0]	{ s_1 }	\perp	\emptyset	\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 }

Soluție: 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	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
1	\perp	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
2	\perp	{NULL}	[0, 0]	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
3	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset	\perp	\emptyset
4	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{ s_1 }	\perp	\emptyset	\perp	\emptyset	\perp	{NULL}
5	\perp	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{ s_1 }	[0, 0]	{ s_1 }	\perp	\emptyset	\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]	<u>{s_1, s_2}</u>	[0, 1]	<u>{s_1, s_2}</u>	[1, 1]	<u>{s_1, s_2}</u>	\perp	<u>{NULL, s_1}</u>
9	\perp	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s_1 }	[0, 1]	<u>{s_1, s_2}</u>	[0, 1]	<u>{s_1, s_2}</u>	<u>[1, 2]</u>	<u>{s_1, s_2}</u>	\perp	<u>{NULL, s_1}</u>

Soluție: 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	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅
1	⊥	{NULL}	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅
2	⊥	{NULL}	[0, 0]	{NULL}	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅
3	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	⊥	∅	⊥	∅	⊥	∅	⊥	∅
4	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	⊥	∅	⊥	∅	⊥	{NULL}
5	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	⊥	∅	⊥	{NULL}
6	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	[1, 1]	{s ₁ }	⊥	{NULL}
7	⊥	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s ₁ }	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	[1, 1]	{s ₁ }	⊥	{NULL}
8	⊥	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s ₁ }	[0, 1]	<u>{s₁, s₂}</u>	[0, 1]	<u>{s₁, s₂}</u>	[1, 1]	<u>{s₁, s₂}</u>	⊥	<u>{NULL, s₁}</u>
9	⊥	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s ₁ }	[0, 1]	<u>{s₁, s₂}</u>	[0, 1]	<u>{s₁, s₂}</u>	[1, 2]	<u>{s₁, s₂}</u>	⊥	<u>{NULL, s₁}</u>
10	⊥	{NULL}	[0, 0]	{NULL}	<u>[0, 2]</u>	<u>{NULL, s₁, s₂}</u>	[0, 2]	{s ₁ , s ₂ }	[0, 2]	{s ₁ , s ₂ }	[1, 2]	{s ₁ , s ₂ }	⊥	{NULL, s ₁ , s ₂ }

Soluție: 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	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅
1	⊥	{NULL}	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅
2	⊥	{NULL}	[0, 0]	{NULL}	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅
3	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	⊥	∅	⊥	∅	⊥	∅	⊥	∅
4	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	⊥	∅	⊥	∅	⊥	{NULL}
5	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	⊥	∅	⊥	{NULL}
6	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	[1, 1]	{s ₁ }	⊥	{NULL}
7	⊥	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s ₁ }	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	[1, 1]	{s ₁ }	⊥	{NULL}
8	⊥	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s ₁ }	[0, 1]	<u>{s₁, s₂}</u>	[0, 1]	<u>{s₁, s₂}</u>	[1, 1]	<u>{s₁, s₂}</u>	⊥	<u>{NULL, s₁}</u>
9	⊥	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s ₁ }	[0, 1]	<u>{s₁, s₂}</u>	[0, 1]	<u>{s₁, s₂}</u>	[1, 2]	<u>{s₁, s₂}</u>	⊥	<u>{NULL, s₁}</u>
10	⊥	{NULL}	[0, 0]	{NULL}	[0, 2]	<u>{NULL, s₁, s₂}</u>	[0, 2]	{s ₁ , s ₂ }	[0, 2]	{s ₁ , s ₂ }	[1, 2]	{s ₁ , s ₂ }	⊥	{NULL, s ₁ , s ₂ }
11	⊥	{NULL}	[0, 0]	{NULL}	[0, 2]	{NULL, s ₁ , s ₂ , s ₃ }	[0, 2]	<u>{s₁, s₂, s₃}</u>	[0, 2]	{s ₁ , s ₂ , s ₃ }	[1, 2]	{s ₁ , s ₂ , s ₃ }	⊥	{NULL, s ₁ , s ₂ , s ₃ }

Soluție: 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	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅
1	⊥	{NULL}	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅
2	⊥	{NULL}	[0, 0]	{NULL}	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅
3	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	⊥	∅	⊥	∅	⊥	∅	⊥	∅
4	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	⊥	∅	⊥	∅	⊥	{NULL}
5	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	⊥	∅	⊥	{NULL}
6	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	[1, 1]	{s ₁ }	⊥	{NULL}
7	⊥	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s ₁ }	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	[1, 1]	{s ₁ }	⊥	{NULL}
8	⊥	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s ₁ }	[0, 1]	<u>{s₁, s₂}</u>	[0, 1]	<u>{s₁, s₂}</u>	[1, 1]	<u>{s₁, s₂}</u>	⊥	<u>{NULL, s₁}</u>
9	⊥	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s ₁ }	[0, 1]	<u>{s₁, s₂}</u>	[0, 1]	<u>{s₁, s₂}</u>	[1, 2]	<u>{s₁, s₂}</u>	⊥	<u>{NULL, s₁}</u>
10	⊥	{NULL}	[0, 0]	{NULL}	[0, 2]	<u>{NULL, s₁, s₂}</u>	[0, 2]	{s ₁ , s ₂ }	[0, 2]	{s ₁ , s ₂ }	[1, 2]	{s ₁ , s ₂ }	⊥	{NULL, s ₁ , s ₂ }
11	⊥	{NULL}	[0, 0]	{NULL}	[0, 2]	{NULL, s ₁ , s ₂ , s ₃ }	[0, 2]	<u>{s₁, s₂, s₃}</u>	[0, 2]	{s ₁ , s ₂ , s ₃ }	[1, 2]	{s ₁ , s ₂ , s ₃ }	⊥	{NULL, s ₁ , s ₂ , s ₃ }
12	⊥	{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 }	<u>[1, 3]</u>	{s ₁ , s ₂ , s ₃ }	⊥	{NULL, s ₁ , s ₂ , s ₃ }

Soluție: 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	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅
1	⊥	{NULL}	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅
2	⊥	{NULL}	[0, 0]	{NULL}	⊥	∅	⊥	∅	⊥	∅	⊥	∅	⊥	∅
3	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	⊥	∅	⊥	∅	⊥	∅	⊥	∅
4	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	⊥	∅	⊥	∅	⊥	{NULL}
5	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	⊥	∅	⊥	{NULL}
6	⊥	{NULL}	[0, 0]	{NULL}	[0, 0]	{NULL}	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	[1, 1]	{s ₁ }	⊥	{NULL}
7	⊥	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s ₁ }	[0, 0]	{s ₁ }	[0, 0]	{s ₁ }	[1, 1]	{s ₁ }	⊥	{NULL}
8	⊥	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s ₁ }	[0, 1]	<u>{s₁, s₂}</u>	[0, 1]	<u>{s₁, s₂}</u>	[1, 1]	<u>{s₁, s₂}</u>	⊥	<u>{NULL, s₁}</u>
9	⊥	{NULL}	[0, 0]	{NULL}	[0, 1]	{NULL, s ₁ }	[0, 1]	<u>{s₁, s₂}</u>	[0, 1]	<u>{s₁, s₂}</u>	[1, 2]	<u>{s₁, s₂}</u>	⊥	<u>{NULL, s₁}</u>
10	⊥	{NULL}	[0, 0]	{NULL}	[0, 2]	<u>{NULL, s₁, s₂}</u>	[0, 2]	{s ₁ , s ₂ }	[0, 2]	{s ₁ , s ₂ }	[1, 2]	{s ₁ , s ₂ }	⊥	{NULL, s ₁ , s ₂ }
11	⊥	{NULL}	[0, 0]	{NULL}	[0, 2]	{NULL, s ₁ , s ₂ , s ₃ }	[0, 2]	<u>{s₁, s₂, s₃}</u>	[0, 2]	{s ₁ , s ₂ , s ₃ }	[1, 2]	{s ₁ , s ₂ , s ₃ }	⊥	{NULL, s ₁ , s ₂ , s ₃ }
12	⊥	{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 }	⊥	{NULL, s ₁ , s ₂ , s ₃ }
13	⊥	{NULL}	[0, 0]	{NULL}	[0, 3]	{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 }	<u>[3, 3]</u>	{NULL, s ₁ , s ₂ , s ₃ }

Observații

- execuția programului poate fi observată în semantica ecuațiilor
- 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 \perp 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' care este \perp de la 4–12 $\implies x_7^S = \perp$ pentru 4–12
- operațiile de *join* depind de domeniu: reuniune simplă de seturi pentru adrese sau operația complexă $\overline{\cap}$ 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*).

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.

- \leq_N este operatorul de incluziune \subset
- $\vee_N = \overline{\cap}$ este operația de *join* pentru intervale
- \wedge_N 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 \wedge_A ?

Domeniul abstract Pts

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

Atunci $Pts = \mathcal{X} \rightarrow \mathcal{P}(\mathcal{A})$ reprezintă funcția ce leagă fiecare variabilă $x \in \mathcal{X}$ 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. $A'(x) = A_1(x) \cup A_2(x), \forall x \in \mathcal{X}$.

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 $A = \bigvee_A B \implies$ putem aplica iterații *Kleene*.

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

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