Separation Logic
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
乓
 Pork
איחוד ערימות

ערימות יקראות זרות אם

$$dom(h_0) \cap dom(h_1) = \emptyset$$

$$h_0 \perp h_1$$

סימון:

בנוסף שני ערימות זרות ל$$h_0,h_1$$ נגדר את איחודן

$$h_0 \cdot h_1$$

$$dom(h_0 \cdot h_1) = dom(h_0) \cup dom(h_1)$$

$$(h_0 \cdot h_1)(x) = \begin{cases} h_0(x) & x \in dom(h_0) \\ h_1(x) & x \in dom(h_1) \end{cases}$$
הלוגיקה

• heap ריק - emp

\[ s, h \models emp \iff \text{dom}(h) = \emptyset \]

• heap המכיל את唯一的 השכבה השוכנת במיקום ערך - e \mapsto e'

\[ s, h \models e \mapsto e' \iff \text{dom}(h) = \{s(e)\} \land h(s(e)) = s(e') \]

• separating conjunction - \( p_0 \ast p_1 \)

הלוגיקה של שני הפרקים דרימ חכש \( p_0 \) מתת-униימ בחלקה \( p_1 \) מתת-униימ בחלקה השכנה.

\[ s, h \models p_0 \ast p_1 \]

\[ \iff \exists h_0, h_1 \left[ (h_0 \perp h_1) \land (h_0 \cdot h_1 = h) \land \right. \]

\[ (s, h_0 \models p_0) \land (s, h_1 \models p_1) \]
הלוגיקה - קיצורים

1. \( e \mapsto - \triangleq (\exists x. e \mapsto x) \)

2. \( e \mapsto e' \triangleq (e \mapsto e' \ast \text{true}) \)

3. \( e \mapsto e_1, ..., e_n \triangleq (e \mapsto e_1 \ast e + 1 \mapsto e_2 \ast \cdots \ast e) \)
דוגמה

נניח \( s(x) \neq s(y) \)

\[
h_1 = \{ s(x) \mapsto 1 \} , h_2 = \{ s(y) \mapsto 2 \}
\]

אז מה ההגנה הכלליתبيותר על התנאי \( h \) על הממקם \( p \) על \( s,h \models p \)

הביאים:

1. \( x \mapsto 1 \)
2. \( y \mapsto 2 \)
3. \( x \mapsto 1 \ast y \mapsto 2 \)
4. \( x \mapsto 1 \ast x \mapsto 1 \)
5. \( x \mapsto 1 \lor y \mapsto 2 \)
דוגמאות

6. \((x \mapsto 1 \lor y \mapsto 2) * (x \mapsto 1 \lor y \mapsto 2)\)

7. \(x \mapsto 1 * y \mapsto 2 * (x \mapsto 1 \lor y \mapsto 2)\)

8. \(x \mapsto 1 * \text{true}\)

9. \(x \mapsto 1 * \neg(x \mapsto 1)\)
1. $A * emp \equiv A$

2. $A * B \equiv B * A$

3. $A * (B * C) \equiv (A * B) * C$

4. $A * false \equiv false$
תוכנה – שפת התוכنيות

while

 funciones אטומיות
  1. \( x := e \)
  2. \( \text{skip} \)
  3. \( S_1;S_2 \)
  4. \( \text{if } B \text{ then } S_1 \text{ else } S_2 \text{ fi} \)
  5. \( \text{while } B \text{ do } S \text{ od} \)

.functions מורכבות
  1. \( e \) הואビジי, לעל משתני התכנית
  2. \( B \) הוא פ돈י (פרדיקט) לעל משתני התכנית
  3. \( S_1;S_2 \) הוא פעולות מורכבות
  4. \( S_1;S_2 \) הוא פעולות אטומיות

פעולות אטומיות

פעולות מורכבות
特斯פורת לשפה

\( x := \text{cons}(e_1, \ldots, e_n) \)

התקנה:
1. \( x \) הוא ביטוי מול משטחי החכונות \( e_i \)
2. \( e_1, \ldots, e_n \) הם ביטויים ל当地人 בלוך ביצוע מצותモン \( l \)
3. \( x \) מציבת לתחלית הרשימה.
4. \( dispose e \)

\( x := [e] \)
\( [e_1] = e_2 \)

סמנטיקה – קצפו. אם ינשונים לכניסה שלה קיימת (עד", abort שחרור, חיפוש או עדכון) עבירים ליציב שלא
מספק דבר
\[ x := \text{cons}(1,2) \quad s: \{ x \mapsto 3, y \mapsto 2 \} \quad h: \emptyset \]

\[ y := [x] \]

\[ [x + 1] := 3 \]

\[ \text{dispose}(x + 1) \quad s: \{ x \mapsto 37, y \mapsto 1 \} \quad h: \{ 37 \mapsto 1, 38 \mapsto 2 \} \]

\[ [x + 2] := 3 \]

\[ \text{abort} \]
\{q_1\} \ P \ \{q_2\}, \ \text{vars}(r) \land \text{vars}(P) = \emptyset
\hline
\{q_1 \land r\} \ P \{q_2 \land r\}
הזכורה

לא נאوء אם \( x,y \) מתביעים לאותי مكان

\[
\{x \rightarrow -\} \ [x] := 4 \ \{x \rightarrow 4\}
\]

\[
\{x \rightarrow -\land y \rightarrow 3\} \ [x] := 4 \ \{x \rightarrow 4 \land y \rightarrow 3\}
\]
frame rule – התייחסות

\[ \{q_1\} P \{q_2\}, \quad \text{vars}(r) \land \text{vars}(P) = \emptyset \]

\[ \{q_1 * r\} P \{q_2 * r\} \]
התקנון

\[ \{x \mapsto -\} [x] := 4 \{x \mapsto 4\} \]

\[ \{x \mapsto -* y \mapsto 3\} [x] := 4 \{x \mapsto 4 * y \mapsto 3\} \]
אקסיומות

deallocation (local):
\[ \{ e \mapsto \_ \} \text{dispose } e \{ \text{emp} \} \]

deallocation (global):
\[ \{(e \mapsto \_ ) * r \} \text{dispose } e \{ r \} \]
mutation (local):
\[ \{ e \mapsto - \} [e] := e' \{ e \mapsto e' \} \]

mutation (global):
\[ \{(e \mapsto -) * r\} [e] := e' \{(e \mapsto e') * r\} \]
אקסיומות

בעזרת $v$ שלא пояפה בחיפוש ב-$e$ או ב-$r$

_allocation (local):
\[
\{emp\} v := cons(\bar{e}) \{v \mapsto \bar{e}\}
\]

_allocation (global):
\[
\{r\} v := cons(\bar{e}) \{v \mapsto \bar{e} * r\}
\]
akkumulátion

allocation (local):
\[
\{ v' = v \} \ v := cons(e) \ { v \mapsto e[v \leftarrow v'] } \]

כ缕ך v,v' מע斯塔נים שונים
אקסיומות

עבורי $v$ שאינו выражен בתוך $e$ - $\bar{e}$

allocation (local):
$$\{emp\} v := cons(\bar{e}) \{v \mapsto \bar{e}\}$$

allocation (global):
$$\{r\} v := cons(\bar{e}) \{(v \mapsto \bar{e}) * r\}$$
_allocation (local):
\{v = v' \land emp\} \; v := \textit{cons}(\bar{e}) \; \{v \mapsto \bar{e}[v \leftarrow v']\}\}

כאשר \(v, v'\) משתנים שונים
אקסיומות

lookup (local):

\[ \{ v = v' \land (e \mapsto v'') \} \]

\[ v := [e] \]

\[ \{ v = v'' \land e[v \leftarrow v'] \mapsto v'' \} \]

כאשר "\(v',v''\) משתנים שונים \(v,v',v''\) mutually different
դուհեր

\[ x := \text{cons}(a, a) \]
\[ y := \text{cons}(b, b) \]
\[ [x + 1] := y - x \]
\[ [y + 1] := x - y \]


\{emp\} 

\(x := \text{cons}(a, a)\)

\(\{x \mapsto a, a\}\)

\(y := \text{cons}(b, b)\)

\(\{x \mapsto a, a * y \mapsto b, b\}\)  

\(\{x \mapsto a, -y \mapsto b, -\}\)  

\([x + 1] := y - x\)

\(\{x \mapsto a, (y - x) * y \mapsto b, -\}\)  

\([y + 1] := x - y\)

\(\{x \mapsto a, (y - x) * y \mapsto b, (x - y)\}\)  

\(\exists c. x \mapsto a, c * y \mapsto b, -c\)
רשימות מקושרות

• $\varepsilon$ - הסדרה הריקה

• $[a]$ -رشימה המכיל את האיבר בודד $a$ (נshima $[]$)

• שרשרת רשימות $\alpha \cdot \beta$
רשימות מכורותת

\[\text{list } \in i \triangleq \text{emp} \land i = \text{nil}\]

\[\text{list } (a \cdot \alpha) i \triangleq \exists j. i \mapsto a, j \ast \text{list } \alpha j\]
רשימות מקושרות

\[ lseg \epsilon (i, j) \triangleq emp \land i = j \]

\[ lseg a \cdot \alpha(i, k) \triangleq \exists j. i \mapsto a, j \ast lseg \alpha(j, k) \]
רשימות מקושרות – חכונת

1. \( lseg \alpha (i, j) \iff i \mapsto a, j \)
2. \( lseg \alpha \cdot \beta (i, k) \iff \exists j. lseg \alpha (i, j) * lseg \beta (j, k) \)
3. \( lseg \alpha \cdot b (i, k) \iff \exists j. lseg \alpha (i, j) * j \mapsto b, k \)
4. \( list \alpha i \iff lseg \alpha (i, nil) \)
로그מה - ההגנה עלブヘלקה הרשימה

\{lseg \alpha (i,j)\}
\textit{k := cons}(a, i)
\{k \mapsto a, i \ast lseg \alpha (i,j)\}
\{\exists i. k \mapsto a, i \ast lseg \alpha (i,j)\}
\{lseg a \cdot \alpha (k,j)\}
i := k
\{lseg a \cdot \alpha (i,j)\}
דוגמא - מחיקת האיבר בראש הרשימה

\{lseg a \cdot \alpha (i, k)\}
\{\exists j. i \mapsto a, j \cdot lseg \alpha (j, k)\}
\{\exists j. i + 1 \mapsto j \cdot (i \mapsto a \cdot lseg \alpha (j, k))\}
j := [i + 1]
\{i + 1 \mapsto j \cdot (i \mapsto a \cdot lseg \alpha (j, k))\}
\{i \mapsto a \cdot (i + 1 \mapsto j \cdot lseg \alpha (j, k))\}
dispose i
\{i + 1 \mapsto j \cdot lseg \alpha (j, k)\}
dispose i + 1
\{lseg \alpha (j, k)\}
i := j
\{lseg \alpha (i, k)\}