

分離論理入門のようなもの

そくらてす

ScienSlack

2020/8/23

分離論理とは？

- 分離論理とは？
 - ヒープ領域に言及できる論理体系
 - ヒープ領域の状態を表す記法
- ヒープ領域とは？
 - C言語などのポインタで触ることのできるメモリの領域 (と思っといてくれ)

分離論理の論理式

Definition 1 (分離論理の論理式)

Variables(変数記号)

$x \in \text{Variables}$

Terms(項)

$t ::= \text{nil} \mid x$

Atomic Formulae(原子論理式)

$\alpha ::= \text{emp} \mid t = t \mid t \xrightarrow{1} \langle t \rangle \mid t \xrightarrow{2} \langle t, t \rangle \mid$
 $\text{ls}(t, t) \mid \text{tree}(t)$

Formulae(論理式)

$\varphi ::= \alpha \mid \neg \varphi \mid \varphi \wedge \varphi \mid \exists x. \varphi \mid \varphi * \varphi \mid \varphi \rightarrow^* \varphi$

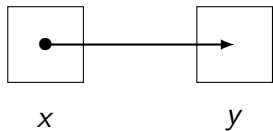
分離論理の意味のイメージ

emp

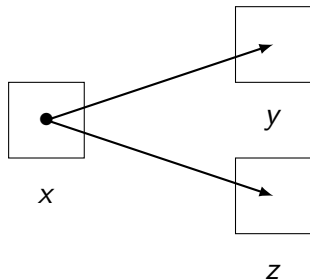
emp

分離論理の意味のイメージ

\vdash



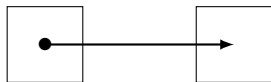
$$x \vdash^1 \langle y \rangle$$



$$x \vdash^2 \langle y, z \rangle$$

分離論理の意味のイメージ

*

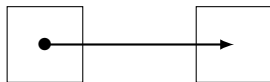


x

y

$$x \stackrel{1}{\mapsto} \langle y \rangle$$

*

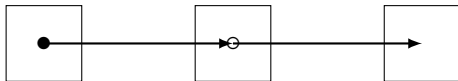


y

z

$$y \stackrel{1}{\mapsto} \langle z \rangle$$

*



x

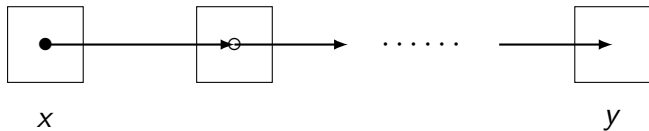
y

z

$$x \stackrel{1}{\mapsto} \langle y \rangle * y \stackrel{1}{\mapsto} \langle z \rangle$$

分離論理の意味のイメージ

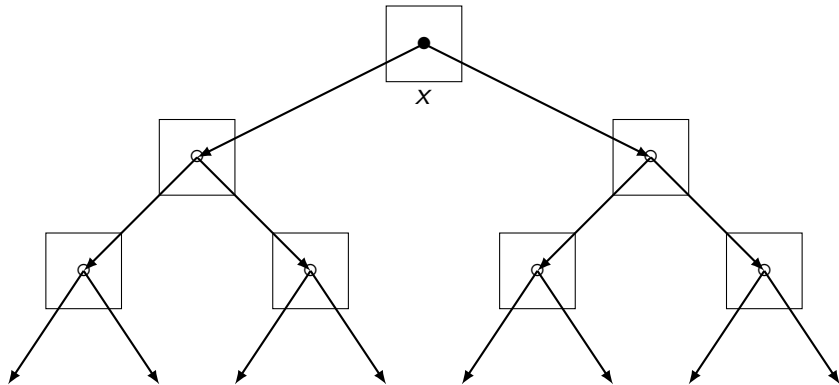
$ls(-, -)$



$ls(x, y)$

分離論理の意味のイメージ

tree(-)



tree(x)

プログラム検証とは？

- プログラム検証とは？

- プログラムが持っていてほしい性質を持っているかどうかを数学的に保証すること




- プログラムが持っていてほしい性質とは？

- 仕様を満たしているか？（部分正当性）
- プログラムはきちんと停止するか？（停止性）
- エラーを吐かないか？（安全性） etc.

プログラム検証の例のようなもの

```
{tree(x)}  
deltree(*x){  
  if (x = NULL) return 0;    {emp}  
  else{    {x  $\xrightarrow{2}$  <y, z> * tree(y) * tree(z)}  
    l := x.left;    r := x.right;    {x  $\xrightarrow{2}$  <l, r> * tree(l) * tree(r)}  
    deltree(l);    {x  $\xrightarrow{2}$  <l, r> * emp * tree(r)}  
    deltree(r);    {x  $\xrightarrow{2}$  <l, r> * emp}  
    free(x);    {emp}  
  }    {emp}  
}    {emp}
```

参考文献

-  John C. Reynolds, “Separation Logic: A Logic for Shared Mutable Data Structure”, Proceedings of the 17th Annual IEEE Symposium on Logic in Computer Science, 2002.
-  James Brotherston, “ An introduction to separation logic ”, Logic Summer School, ANU, 7 December 2015.
-  Sokratesnil, 『分離論理入門のようなもの』,
<https://sokratesnil.github.io/pdfs/SL.pdf>

分離論理の意味

—*

$$\varphi * \psi \vdash \vartheta \iff \varphi \vdash \psi \multimap \vartheta$$

Example

$$\text{ls}(x, y) * \text{ls}(y, z) \vdash \text{ls}(x, z) \iff \text{ls}(x, y) \vdash \text{ls}(y, z) \multimap \text{ls}(x, z)$$

Frame Rule

Definition 2 (Frame rule)

$$\frac{\{P\} C \{Q\}}{\{P * R\} C \{Q * R\}}$$

Remark

一般に次は成立しない.

$$\frac{\{P\} C \{Q\}}{\{P \wedge R\} C \{Q \wedge R\}}$$

Symbolic heap

Definition 3 (Symbolic heap)

Variables $x \in \text{Variables}$

Terms $t ::= \text{nil} \mid x$

Pure Formulæ $\Pi ::= t = t \mid t \neq t \mid \top \mid \perp \mid \Pi \wedge \Pi$

Spatial Formulæ $\Sigma ::= \text{emp} \mid t \xrightarrow{1} \langle t \rangle \mid t \xrightarrow{2} \langle t, t \rangle \mid \text{ls}(t, t) \mid \text{tree}(t) \mid \Sigma * \Sigma$

Formulæ $\varphi ::= \Pi \wedge \Sigma$