

ソフトウェア基礎論 配布資料 (1)

五十嵐 淳

平成 15 年 10 月 15 日

各種事務連絡

教官について

五十嵐 淳

所属 知能情報学専攻 ソフトウェア基礎論分野

居室 工学部 10 号館 1 階 142 号室

e-mail igarashi@kuis.kyoto-u.ac.jp

講義予定

前半 (7–8 回): プログラム意味論 (操作的意味論・表示の意味論・公理の意味論)

後半 (3–4 回): 型システム

成績評価

(レポート (1 回程度) & 試験) または レポート 2 回

参考図書

Glynn Winskel. *The Formal Semantics of Programming Languages*. The MIT Press. 1993.

Benjamin C. Pierce. *Types and Programming Languages*. The MIT Press. 2002.

1 数学的準備: 集合に関する基礎知識

1.1 論理の記法

以下で A, B を, 命題(*proposition*), つまり何かを述べている文 (statement, 疑問文・命令文ではない) とする. また, 変数を含む statement を述語(*predicate*) という. 述語の真偽は, 変数に適当に数を割り当てることで決まる. 例: 2 変数述語 $P(x, y) \stackrel{\text{def}}{=} (x \leq y)$. 命題や述語に, 「かつ」「ならば」といった論理結合子(*logical connectives*) や, 「任意の ~ に対して」「ある ~ に対して」といった限量子(*quantifier*) を適用することで複雑な命題, 述語を構成することができる. この講義では, 命題・述

語を簡潔に記述するために、「かつ」などの日本語の代わりに、「&」などの記号を用いることが多い。これらの記号を表 1 にまとめておく。

記法	説明
$\neg A$	A ではない。(not)
$A \& B$	A かつ B である。(and, conjunction)
$A \text{ or } B$	A または B である。(or, disjunction)
$A \Rightarrow B$	もし A ならば B である。(if-then, implication)
$A \Longleftrightarrow B$	A ならば B であり、 A であるのは B のときのみである。 (if-and-only-if, logical equivalence)
$\exists x_1, \dots, x_n. P(x_1, \dots, x_n)$	ある $x_1, \dots, x_n$ に対して $P(x_1, \dots, x_n)$ である。(there exists)
$\forall x_1, \dots, x_n. P(x_1, \dots, x_n)$	任意の $x_1, \dots, x_n$ について $P(x_1, \dots, x_n)$ である。(for all)
$\forall x \in X. P(x)$	$\forall x. x \in X \Rightarrow P(x)$ の略記。 x の値の集合を指定する。
$\exists! x. P(x)$	$(\exists x. P(x)) \& \forall y, z. (P(y) \& P(z) \Rightarrow y = z)$ の略記。 「 $P(x)$ を満す x がただひとつ存在する」

表 1: 論理の記法

1.2 集合の記法

この講義で主に用いる、集合に関する記法を表 2 にまとめる。

基礎の公理 とは、 $\dots \in b_n \in \dots \in b_1 \in b_0$ のような無限列は存在しない、という性質。

1.3 関係と関数

n 項関係 集合 $X_1, \dots, X_n$ が与えられたとき、 $\mathcal{P}(X_1 \times \dots \times X_n)$ の要素を $X_1, \dots, X_n$ 間の n 項関係(n -ary relation) であるという。 R が二項関係(binary relation) であるとき、 $(x, y) \in R$ を xRy と表記する。

部分関数 以下の条件

$$\forall x, y, y'. ((x, y) \in f \& (x, y') \in f) \Rightarrow y = y'$$

を満す(二項)関係 $f \in \mathcal{P}(X \times Y)$ を X から Y への部分関数(*partial function*) という。 $(x, y) \in f$ であるとき、 $f(x) = y$ と表記する。またこのとき f は x において定義される(*defined*) といい、 x に対して $\forall y. f(x) \neq y$ のとき x において未定義(*undefined*) であるという。

X から Y への部分関数全体の集合を $X \rightharpoonup Y$ と表記する。

全値関数 X から Y への部分関数 f で、 $\forall x \in X. \exists y \in Y. f(x) = y$ をみたすものを全値関数(*total function*) という。

X から Y への全値関数全体の集合を $X \rightarrow Y$ と表記する。

集合 X に対して $Id_X \in X \rightarrow X \stackrel{\text{def}}{=} \{(x, x) \mid x \in X\}$ を X 上の恒等関数(*identity function*) という。

概念	記法	定義・補足
外延的 (要素の列挙による) 定義	$\{a, b, c, \dots\}$	
要素である	$a \in X$	
部分集合	$X \subseteq Y$	$\forall z \in X. z \in Y$
集合が等しい	$X = Y$	$X \subseteq Y \ \& \ Y \subseteq X$
空集合	$\emptyset$	$(\forall x. x \notin \emptyset)$
自然数の集合	$\mathbb{N}$	$\{1, 2, 3, \dots\}$
内包的定義	$\{x \in X \mid P(x)\}$	X の要素で, P を満すものの全ての集合
巾 (べき) 集合	$\mathcal{P}(X)$	$\{Y \mid Y \subseteq X\}$ X の全ての部分集合の集合
index づけされた集合 (indexed set)		
和集合	$X \cup Y$	$\{a \mid a \in X \text{ or } a \in Y\}$
集合族の和	$\bigcup X$	$\{a \mid \exists x \in X. a \in x\}$ 但し X は集合の集合
共通部分	$\bigcup_{i \in I} x_i$ $X \cap Y$	$\{a \mid a \in X \ \& \ a \in Y\}$
集合族の共通部分	$\bigcap X$	$\{a \mid \forall x \in X. a \in x\}$ 但し X は集合の集合
デカルト積	$\bigcap_{i \in I} x_i$ $X \times Y$	$\{(a, b) \mid a \in X \ \& \ b \in Y\}$
直和	$X \oplus Y$	$\{(0, a) \mid a \in X\} \cup \{(1, b) \mid b \in Y\}$
差	$X \setminus Y$	$\{x \mid x \in X \ \& \ x \notin Y\}$

表 2: 集合の記法

関数 $f \in X \rightarrow Y$ に対して, $\exists g \in Y \rightarrow X. (\forall x \in X. g(f(x)) = x \ \& \ \forall y \in Y. f(g(y)) = y)$ が成立するとき, X と Y は 1 対 1 対応 (1-1 correspondence) しているという. また, この関数 g を f の逆関数 (inverse) という. また, $\mathbb{N}$ の部分集合と 1 対 1 対応している集合を可算 (countable) であるという.

1.3.1 ラムダ記法

e を変数 x を含む式, X を集合として, $\lambda x \in X. e$ を $\{(x, e) \mid x \in X\}$ で定義される関数とする.

1.3.2 関数・関係の合成

R を X と Y の間の関係, S を Y と Z の間の関係とする. R と S の合成 (composition) を

$$S \circ R \stackrel{\text{def}}{=} \{(x, z) \mid \exists y \in Y. (x, y) \in R \ \& \ (y, z) \in S\}$$

と定義する. $S \circ R$ は X と Z の間の関係である. 関数の合成は関係の合成の定義から自然に導かれる.

Cantor の対角線論法 X と $\mathcal{P}(X)$ は 1 対 1 対応になりえない. (なると仮定, 対応関係を θ として,

$$Y = \{x \in X \mid x \notin \theta(x)\}$$

を考える.)

1.3.3 像と逆像

関係 $R \in \mathcal{P}(X \times Y)$ と $A \subseteq X$ に対し,

$$RA = \{y \in Y \mid \exists a \in A. (a, y) \in R\}$$

を A の R の下での像 (direct image) という. このとき, R は A を RA へ対応させる関数 ($\in \mathcal{P}(X) \rightarrow \mathcal{P}(Y)$) と見なすこともできる.

また, 関係 $R \in \mathcal{P}(X \times Y)$ と $B \subseteq Y$ に対し,

$$R^{-1}B = \{x \in X \mid \exists b \in B. (x, b) \in R\}$$

を B の R の下での逆像 (inverse image) という.

1.3.4 同値関係

X 上の関係 $R \in \mathcal{P}(X \times X)$ が以下の条件を満たすとき同値関係 (equivalence relation) であるという.

- 反射律 (reflexivity): $\forall x \in X. xRx$
- 対称律 (symmetry): $\forall x, y \in X. xRy \Rightarrow yRx$
- 推移律 (transitivity): $\forall x, y, z \in X. (xRy \ \& \ yRz) \Rightarrow xRz$

R が X 上の同値関係であるとき, $x \in X$ の同値類 (equivalence class) $\{x\}_R$ を $\{y \in X \mid yRx\}$ と定義する.