プログラム理論

GB20501

水谷哲也

2025年(令和7年)度の内容

担当:水谷 mizutani@cs.tsukuba.ac.jp

Preliminary: 一階述語論理

逐次的プログラムの検証　Hoare論理

ダイクストラによるガード付きコマンドを用いた非決定的プログラムの検証法

資料は筑波大学学習管理システム(manaba)

https://manaba.tsukuba.ac.jp/

におきます.

授業に関する連絡事項は原則として授業中に行います.

授業スケジュール

第1週(07/09)　授業全般の説明, 一階述語論理概説
第2週(07/16)　仕様表現と検証, プログラムの意味, Hoare論理概説
第3週(07/23)　Hoare論理によるプログラムの検証　部分的正当性と停止性の証明
第4週(07/30)　Hoare論理における配列などの扱い
第5週(08/06)　ガード付きコマンドを用いた非決定的プログラムの検証法

成績　　出席を前提とし, 授業後のレポートと期末レポートにより, 総合的に評価
　　確認テスト(期末試験)は行わない

レポートは「自分の言葉」で解答してください.
他人と相談したり勉強会を開くことは奨励しますが, 丸写しはいけません.
同様に, ネットで検索したり生成AIに頼ったりすることもあるかもしれませんが,
丸写しはダメです.
必ず自分で内容を理解し, 自分で消化してからレポートにしてください.
生成AIの利用にあたっては、筑波大学発行の
「教育における生成AI活用のガイドライン（学生向け）」を参照し
適切な利用を心がけてください.
文献を参照したときには参考文献を一覧の形て提示してください.
生成AIを参照した際にもどのように参照したかを明記してください.

講義概要

一階述語論理

論理的表現に慣れる

例

1. Use the predicates

$$\begin{aligned} A(x,y): &\quad x \text{ admires } y \\ B(x,y): &\quad x \text{ attended } y \\ P(x): &\quad x \text{ is a professor} \\ S(x): &\quad x \text{ is a student} \\ L(x): &\quad x \text{ is a lecture} \end{aligned}$$

and the nullary function symbol (constant)

$$m: \quad \text{Mary}$$

to translate the following into predicate logic:

(a) Mary admires every professor.
(The answer is not $\forall x\, A(m, P(x))$.)

(b) Some professor admires Mary.

(c) Mary admires herself.

(d) No student attended every lecture.

(e) No lecture was attended by every student.

(f) No lecture was attended by any student.

逐次的プログラムの検証　Hoare論理

Algol-like 逐次プログラムの正当性の検証のための公理系

プログラムの表明

部分的正当性と停止性

ループ不変表明

などについて理解する

例

while (x!=0){y=y*x; x=x-1}

のようなプログラムの「意味」と「仕様」を論理的に表現し，

プログラムが仕様を満たしていることを形式的に証明する.

そのための体系を学ぶ.

「仕様」には「停止性」を含む.

ダイクストラの方法による非決定的プログラムの検証

最弱前条件twp(P, B)を用いて検証を行う.

非決定的プログラム言語を用いる.

参考文献

Huth, M. and Ryan, M. :
Logic in Computer Science, Modelling and Reasoning about Systems,
2nd edition, Cambridge Univ. Press, 2005.

　このスライドの前半はこの教科書の一部に準拠

林晋: プログラム検証論, 共立出版, 1995.

　後半はこの教科書の一部を参照

Apt, K. R., de Boer, F. S. and, Olderog, E-R. :
Verification of Sequential and Concurrent Programs, 3rd edition,
Springer-Verlag, 2009.

Manna, Z. :
Mathematical Theory of Computation, Dover Pubns, 2003 (McGraw-Hill, 1974)
五十嵐滋(訳): プログラムの理論,
日本コンピュータ協会, 1974.

プログラムの理論

計算についての我々の理解を数学的に厳格にすること,
なかんずくコンピュータ・プログラムについての検証のアート
(かの名高いデバッグの技術)を1つのサイエンスにすることを目指す理論
Z. Manna (1974), Mathematical Theory of Computation, McGraw-Hill.
“I consider it to be the theory which attempts to formalize our understanding of computation, and in particular to make the art of verifying computer programs (the famous debugging technique) into a science.”

呼び方 (いずれも1960年代初頭より)

日本	Theory of Program (Program Theory)	Igarashi
アメリカ	Mathematical Theory of Computation	McCarthy
ソ連(ロシア)	Theoretical Programming	Ershov

(このprogrammingはsoftware engineering, software science, computer scienceといった意味.)

プログラムの検証

プログラムが正しく作動することを確認する作業

検証方法は数学的・論理的に厳密にしかつ一般性を持たせる

一階述語論理
(The first-order predicate logic)

個体(individual)に関する性質を述語(predicate)として扱う論理

例

S(x): xは学生 (x is a student), I(x): xは教師 (Instructor),

Y(x, y): xはyより若い (x is younger than y)

S, I, Y: 述語記号, x:変数

$\forall x(S(x) \supset (\exists y(I(y) \wedge Y(x, y))))$

全ての学生には自分より年上の教師がいる

「全てのxに対して, もしxが学生ならば, あるyが存在して, yは教師かつxはyより若い. 」

B(x): xは鳥である (x is a bird), F(x): xは飛べる (x can fly)

$\neg(\forall x(B(x) \supset F(x)))$　全ての鳥は飛べる訳ではない.

$\exists x(B(x) \wedge \neg F(x))$でも同じ

構文法(syntax)

語彙(vocabulary)

P: 述語記号全体の集合

F: 関数記号全体の集合

C: 定数全体の集合

V: 変数全体の集合

項(term)

変数は項

定数は項

$t_1, \ldots, t_n$が項であり, fがn引数の関数記号のとき $f(t_1, \ldots, t_n)$は項

命題(論理式: formula)

$t_1, \ldots, t_n$が項であり，pがn引数の述語記号のとき，$p(t_1, \ldots, t_n)$は命題

(原子論理式;atomic formula, primitive formula)

ϕ_1, ϕ_2が命題でxが変数のとき,

$(\neg\phi_1), (\phi_1 \wedge \phi_2), (\phi_1 \vee \phi_2), (\phi_1 \supset \phi_2), (\forall x\phi_1), (\exists x\phi_1)$は命題

$\forall, \exists$を量記号(quantifier)とよぶ.

かっこは適宜省略する

記号の結合の強さは

¬，∀x，∃yが一番強い(strongest)

その次に∧, その次に∨

⊃が一番弱い (weakest)

例

A(x)∨B(x)∧∀y(C(x, y)⊃D(y)) は (A(x)∨ (B(x)∧(∀y(C(x, y)⊃D(y)))))の略記

メタ変数（Metavariables）

「Aが式であるとき」というような表現において，“A”は「本当の」式ではなく，
式であることを表す表現，具体的には例えば（x=y ∧ y>z）（すなわち（=(x, y) ∧ >(y, z)）） というようなものでである．
このような変数をメタ変数（metavariable）またはメタ表現（meta expression）という．

部分式(subformula)
出現(occurrence)

命題 ϕを構成する過程で現れる命題をその命題の部分式という.

例:

ϕを$A(x) \vee B(x) \wedge \forall y(C(x, y) \supset D(y))$とする.

ϕの部分式は

$A(x)$, $B(x)$, $C(x, y)$, $D(y)$
$C(x, y) \supset D(y)$
$\forall y(C(x, y) \supset D(y))$
$B(x) \wedge \forall y(C(x, y) \supset D(y))$
$A(x) \vee B(x) \wedge \forall y(C(x, y) \supset D(y))$

出現 (Occurrence)

式中のそれぞれの位置での記号

例:　A(x)∨∀x(B(x)∧C(x))においてxの出現は3回

(∀xのxは通常カウントしない)

スコープ (Scope)

∀xF，∃xFの形の部分式の出現のFを，∀xまたは ∃xのスコープという

例: A(x)∨∀x(B(x)∧C(x))において ∀xのスコープは B(x)∧C(x)

自由変数(free variable)と束縛変数(bound variable)

ϕを命題とする.

ϕにおけるxの出現が量記号 $\forall x$，$\exists x$のスコープにあるとき

そのxの出現は束縛されているといい,

そうでなければ自由であるという.

代入(substitution)

A[t/x]

論理式A中の自由変数xを全て項tで置き換えた論理式

例

Aをx=2∨y=3xとし, tをy+2とする.

このとき A[t/x], すなわち A[y+2/x] は

y+2=2∨y=3(y+2)となる.

例

Bを $\exists x(x=2 \vee y=x+1) \wedge x>0$とし, tをy+2とする.

このとき B[t/x], すなわち B[y+2/x] は $\exists x(x=2 \vee y=x+1) \wedge y+2>0$となる.

例

Cを $\exists y(x=2 \vee y=x+1) \wedge x>0$とし, uをy+2とする.

このとき C[u/x], すなわち C[y+2/x] は $\exists y(y+2=2 \vee y=(y+2)+1) \wedge y+2>0$とならない.

何故か. 束縛変数と同じ変数を代入してはいけない.

どうするか. 束縛変数名を変更する.

例:

C : ∃y(x=2∨y=x+1)∧x>0, t : y+2のとき

Cは ∃z(x=2∨z=x+1)∧x>0と同じなので

(アルファ同値 α equivalence)

C[t/x], すなわち C[y+2/x] は ∃z(y+2=2∨z=y+2+1)∧y+2>0.

意味(Semantics)

一階述語論理式の意味を定義する.

これと同様の方法でプログラムの意味も定義できる(後述)

D: 領域(universe): 空でない集合;変数や定数の値

ρ: 附値(assignment): 変数の集合Vから領域Dへの関数

xが変数のとき, ρ(x)でxの「値」を表す.

ρ(x), ρ(y), … と考えることができる.

また, ρ_1(x), ρ_1(y), …, ρ_2(x), ρ_2(y), …, ρ_3(x), ρ_3(y), …と様々な附値を考える必要がある.

Ω={true, false}:真理値集合 (Truth set)

M: モデル(Model)

以下の関数f^M, p^Mを定めることにより一つのモデルMが確定する

これらは関数記号, 述語記号の「解釈」を与える

n引数関数記号fに対してf^M: $D^n \to D$

定数は0引数関数記号と考える.

n引数述語記号pに対してp^M: $D^n \to \Omega$

項や命題の意味はモデルMおよび附値 ρ に依存する.

$M[t]_\rho$: 項tの意味

項の構造による帰納的定義

tが変数xのとき $M[t]_\rho = \rho(x)$

tが$f(t_1, \ldots, t_n)$のとき, $M[t]_\rho = f^M(M[t_1]_\rho, \ldots, M[t_n]_\rho)$

$M[\phi]_\rho$：命題 ϕの意味
命題の構造による帰納的定義

ϕが$p(t_1, \ldots, t_n)$のとき, $M[\phi]_\rho = p^M(M[t_1]_\rho, \ldots, M[t_n]_\rho)$

ϕが$\neg\phi_1$のとき, $M[\phi]_\rho$は$M[\phi_1]_\rho$がfalseのときのみtrue, その他はfalse

ϕが$\phi_1 \wedge \phi_2$のとき, $M[\phi]_\rho$は$M[\phi_1]_\rho$も$M[\phi_2]_\rho$もtrueのときのみtrue, その他はfalse

ϕが$\phi_1 \vee \phi_2$のとき, $M[\phi]_\rho$は$M[\phi_1]_\rho$または$M[\phi_2]_\rho$がtrueのときのみtrue, その他はfalse

ϕが$\phi_1 \supset \phi_2$のとき, $M[\phi]_\rho$は$M[\phi_1]_\rho$がtrueでないか$M[\phi_2]_\rho$もtrueのときのみtrue
その他はfalse

$\rho[v/x]$: 附値ρに対して,
xの割当のみv∈Dにかえたもの
すなわち,

$$\rho[v/x](y) = \begin{cases} \rho(y) & \text{if } y \text{がxでないとき} \\ v & \text{if } y \text{がxのとき} \end{cases}$$

ϕが $\forall x\phi_1$のとき, $M[\phi]_\rho$はどんなv∈Dに対しても$M[\phi_1]_{\rho[v/x]}$がtrueのときのみtrue, その他はfalse

ϕが $\exists x\phi_1$のとき, $M[\phi]_\rho$は$M[\phi_1]_{\rho[v/x]}$がtrueになるvが存在するときのみtrue, その他はfalse

例D=N(自然数全体の集合), ρ(x)=0, ρ(y)=1のとき

$M[\exists z(z=x) \wedge \exists z(z=y)]_\rho$を解釈する.

0は自然数に含まれるものとする

$M[\exists z(z=x) \wedge \exists z(z=y)]_\rho$ = true

⇔ $M[\exists z(z=x)]_\rho$ = true かつ $M[\exists z(z=y)]_\rho$ = true

⇔ $M[z=x]_{\rho[v/z]}$=trueなるvが存在する, かつ$M[z=y]_{\rho[v/z]}$=trueなるvが存在する

⇔ $=^M(M[z]_{\rho[v/z]}, M[x]_{\rho[v/z]})$=trueなるvが存在する, かつ

$=^M(M[z]_{\rho[v/z]}, M[y]_{\rho[v/z]})$=trueなるvが存在する

⇔ $=^M(\rho[v/z](z), \rho[v/z](x))$=trueなるvが存在する, かつ

$=M(\rho[v/z](z), \rho[v/z](y))$=trueなるvが存在する

⇔ $=^M(v, 0)$=trueなるvが存在する, かつ $=^M(v, 1)$=trueなるvが存在する

⇔ $=^M(0, 0)$=true かつ $=^M(1, 1)$=true

⇔ true

$M, \rho \vDash \phi$

命題 ϕがモデルMと附値ρで充足可能(satisfiable)

定義

$M, \rho \vDash \phi \quad \Leftrightarrow \quad M[\phi]_\rho = \text{true}$

$\vDash \phi$

命題 ϕが恒真(valid)

定義

$\vDash \phi \quad \Leftrightarrow$ どんな M, ρについても $M, \rho \vDash \phi$

形式的体系（formal system）

公理 axioms

　妥当(valid)な命題

推論規則 inference rules

　一つ以上の妥当な命題から他の妥当な命題への写像

命題が

証明可能(provable), 演繹可能(deducible), 定理(theorem)

　公理, 推論規則の適用の繰り返し(証明(proof))から得られる命題

推論規則
NK(自然演繹法)

公理 排中律 $\neg A \vee A$

$$(\wedge I)\ \frac{A \quad B}{A \wedge B} \qquad (\wedge E)\ \frac{A \wedge B}{A} \qquad \frac{A \wedge B}{B} \qquad (\vee I)\ \frac{A}{A \vee B} \qquad \frac{B}{A \vee B} \qquad (\vee E)\ \frac{A \vee B \quad C \quad C}{C}$$

$$(\supset I)\ \frac{\begin{matrix}[A]\\ B\end{matrix}}{A \supset B} \qquad (\supset E)\ \frac{A \supset B \quad A}{B} \qquad (\neg I)\ \frac{\begin{matrix}[A]\\ \bot\end{matrix}}{\neg A} \qquad (\neg E)\ \frac{\neg A \quad A}{\bot} \qquad (\bot E)\ \frac{\bot}{A}$$

$$(\forall I)\ \frac{A[a]}{\forall x A[x]} \qquad (\forall E)\ \frac{\forall x A[x]}{A[t]} \qquad (\exists I)\ \frac{A[t]}{\exists x A[x]} \qquad (\exists E)\ \frac{\exists x A[x] \quad \begin{matrix}[A[a]]\\ C\end{matrix}}{C}$$

a: eigenvariable
A[x]にもA[a]が依存する仮定にも現れない

t: term

a: eigenvariable
A[x]にもCにも,
A[a]が依存する仮定にも現れない

レポート問題

D=N(自然数全体の集合), ρ(x)=2, ρ(y)=3のとき

M[$\forall z \exists w(z=2w+x \vee z=2w+y)$]$_\rho$ を解釈せよ.

締切　　7月16日(水)15:15

提出先　　manaba

レポートの形式について

解答はpdfで提出してください.

Word等で作成した場合, 手書きのノートを写真で撮影した場合も, pdfに変換してください.

解答用紙の形式は特に指定しませんが, 必ず学籍番号と氏名を書いてください.

学籍番号と氏名が書かれていないものは. 解答として認めません。.

解答用紙を撮った写真を提出する場合, 写真は解答内容を読めるように撮影してください.

（斜めから撮ったりしない）

学籍番号と氏名がしっかりと写るように注意してください.

レポート作成について

文献を参照した場合は参考文献を明記してください.

生成AIを利用した場合はどのように用いたかを明記してください.

文献参照や生成AIの利用は(グループでの勉強会と同様に)奨励しますが,「丸写し」は禁止します.

必ず自分で咀嚼して自分自身の言葉てレポートを作成してください.