数理解析研究所講究録
第458巻 1982年 247-255

多ソート部分的代数に対する等式推論規則

名古屋大学工学部　坂部俊樹
名古屋大学工学部　稲垣康善
豊橋技術科学大学　本多波雄

1. まえがき　近年活発に研究がなされている抽象データタイプの代数的仕様記述法[1~8]において等式論理は重要な役割を果たしている. しかし, 抽象データタイプのモデルである多ソート代数に対しては, 特殊な場合だけであるが, 従来の等式論理が完全ではないことが指摘されている[2]. すなわち, 等式の集合から推論規則を使って演繹した結果が等式集合のすべての等式を満たす代数において成立することが保証されない. このような不都合は, 定数項(変数を含まない項)が存在しないソートがあるような演算記号ドメインの場合のみに生じる可能性がある. 従って, この不都合は従来の抽象データタイプの議論においてそれほど重大ではない.

これに対して, 著者等が抽象データタイプのモデルとして採用している多ソート部分的代数に対しては, どのソートにも評価可能な定数項が存在するという制限を演算記号ドメイ

ンに課しても従来の等式論理が完全ではないことが知られる．このことは，演算が全域関数である多ソート代数（多ソート全域的代数）をモデルとして得られた従来の抽象データタイプに関する結果がそのままでは成立しないことを意味する．

本文では，多ソート部分的代数に対しても条件付で完全であるような等式推論規則を与える．また，この規則によって定められる項集合上の同値関係と部分的代数間の弱準同形写像の関係を示す．

2 準備　ソートの集合を S とする．S ソート演算記号ドメイン Σ は集合族 $\langle \Sigma_{w,s} \rangle_{w \in S^*, s \in S}$ である．$\sigma \in \Sigma_{w,s}$ のとき σ をアリティ w，ソート s の演算記号と言い，$arity(\sigma) = w$，$sort(\sigma) = s$ と書く．X を変数集合族 $\langle X_s \rangle_{s \in S}$ とする．$x \in X_s$ のとき，x はソート s の変数と言われ，$sort(x) = s$ と書く．集合族 $T_\Sigma(X) = \langle T_\Sigma(X)_s \rangle_{s \in S}$ を，次の条件を満たす最小の集合族とする．各 $s \in S$ に対して，

(1) $X_s \cup \Sigma_{\varepsilon,s} \subseteq T_\Sigma(X)_s$．ただし ε は空系列である．

(2) $\sigma \in \Sigma_{s_1 \cdots s_n, s}$，$\xi_i \in T_\Sigma(X)_{s_i}$ $(i = 1, 2, \cdots n)$ ならば $\sigma(\xi_1, \cdots, \xi_n) \in T_\Sigma(X)_s$．

$T_\Sigma(X)_s$ の元をソート s の $\Sigma(X)$ 項又は単に項という．$\xi \in T_\Sigma(X)_s$ のとき $sort(\xi) = s$ と書く．$\Sigma(X)$ 項 ξ の中に出現する変数の集合を $var(\xi)$ と書く．$var(\xi) \subseteq \{x_1, \cdots, x_n\}$ かつ $sort(x_i) = s_i$ $(i = 1, \cdots, n)$ のとき，ξ のアリティは $s_1 \cdots s_n$ であるといい，$arity(\xi) = s_1 \cdots s_n$ と書く．$arity(\xi) = \varepsilon$ である項を Σ 項又は定数項という．ソー

トλの変数xをソートλの項τで置き換えてξから得られる項をξ[τ/x]と書く．x∉VAR(ξ)ならばξ=ξ[τ/x]である．

定義1　部分的Sソート Σ代数（Sソート Σ代数，Σ代数，代数などということもある）Aは次の(i)，(ii)の2項目からなる．

(i) 集合族$\langle A_\lambda\rangle_{\lambda\in S}$．$A_\lambda$はソートλの台と呼ばれる

(ii) 各$\alpha\in\Sigma_{w,\lambda}$に対して次のような$\alpha_A$．

(1) $w=\varepsilon$のとき，α_AはA_λの元．

(2) $w\neq\varepsilon$のとき，α_Aは部分関数：$A_{\lambda_1}\times\cdots\times A_{\lambda_n}\to A_\lambda$　$(w=\lambda_1\cdots\lambda_n)$

Σ代数Aの上で項ξを，いわゆる内側優先の評価手続で評価して得られるA上の部分関数をξ_Aと書き，ξの導出演算と呼ぶ．$arity(\xi)=\lambda_1\cdots\lambda_n$，$sort(\xi)=\lambda$ならば，$\xi_A: A_{\lambda_1}\times\cdots\times A_{\lambda_n}\to A_\lambda$である．$arity(\xi)=\varepsilon$ならば，$\xi_A\in A_\lambda$，そうでなければ，$\xi_A$は未定義（$\xi_A=\phi$）である．

定義2　A，BをSソート Σ代数とする．射準同形写像$h: A\to B$は次の(i)，(ii)を満たす関数族$\langle h_\lambda: A_\lambda\to B_\lambda\rangle_{\lambda\in S}$である．

(i) $\alpha\in\Sigma_{\varepsilon,\lambda}$ならば$h_\lambda(\alpha_A)=\alpha_B$．

(ii) $\alpha\in\Sigma_{\lambda_1\cdots\lambda_n,\lambda}$ $(n\geq 1)$ならば$h_\lambda\circ\alpha_A\subseteq\alpha_B\circ(h_{\lambda_1}\times\cdots\times h_{\lambda_n})$．ただし，∘は$f\circ g(x)=f(g(x))$で定義される関数合成であり，$h_{\lambda_1}\times\cdots\times h_{\lambda_n}: A_{\lambda_1}\times\cdots\times A_{\lambda_n}\to B_{\lambda_1}\times\cdots\times B_{\lambda_n}$は$h_{\lambda_1}\times\cdots\times h_{\lambda_n}(a_1,\cdots,a_n)=(h_{\lambda_1}(a_1),\cdots,h_{\lambda_n}(a_n))$で定義される関数である．

3. 部分的代数に対する等式推論規則　この節では，まず従来の等式論理における推論規則が部分的代数に対しては不完全であることを示し，次に，部分的代数に対しても条件付

で完全である推論規則を与える．そして最後に，この新しい推論規則と弱準同形写像の関係を明らかにする．

S をソートの集合，Σ を S ソート演算記号ドメイン，$X = \langle X_A \rangle_{A \in S}$ を変数集合族とする．$\Sigma(X)$ 項 ξ, η に対して，$\xi \approx \eta$ を Σ 等式 または単に 等式 という．Σ 代数 A が $\xi \approx \eta$ を 満足する とは，$\xi_A = \eta_A$ であることである．等式集合 Γ を A が満足するとは，A が Γ 中のすべての等式を満足することである．Γ を満足するすべての Σ 代数のクラスを $\mathbb{V}_\Gamma$ と書く．

従来の（単一ソートの）等式論理における推論規則は，

(1) 反射性：$\vdash \xi \approx \xi$

(2) 対称性：$\{\xi \approx \eta\} \vdash \eta \approx \xi$

(3) 推移性：$\{\xi \approx \zeta, \eta \approx \zeta\} \vdash \xi \approx \zeta$

(4) 代入性：$\{\xi \approx \xi', \eta \approx \eta'\} \vdash \xi[\eta/x] \approx \xi'[\eta'/x]$

からなる．これを $\mathfrak{R}_0$ と書くことにする．$\mathfrak{R}_0$ が sound ではない（従って完全ではない）ことを示す例を次にあげる．

$S = \{a, b\}$，$\Sigma_{\varepsilon,b} = \{T, F\}$，$\Sigma_{b,b} = \{\alpha, \beta\}$，$\Sigma_{\varepsilon,a} = \{\bar{0}, \bar{1}\}$，$\Sigma_{a,a} = \{\delta\}$，$\Sigma_{a,b} = \{\gamma\}$ とする．等式集合 Γ を

$\Gamma = \{\alpha(x) \approx T,\ \beta(x) \approx F,\ \alpha(\gamma(\delta(y))) \approx \beta(\gamma(\delta(y)))\}$

とする．$\mathfrak{R}_0$ を用いれば Γ から $T \approx F$ が導出できる．すなわち，$\Gamma \overset{\mathfrak{R}_0}{\vdash} T \approx F$ である．ところが，Γ を満たすが $T \approx F$ を満足しない次のような Σ 代数 A が存在する．

$A_a = \{0, 1\}$, $A_b = \{true, false\}$, $\bar{0}_A = 0$, $\bar{1}_A = 1$, $T_A = true$, $F_A = false$,

$\alpha_A(true) = \alpha_A(false) = true$, $\beta_A(true) = \beta_A(false) = false$,

$\gamma_A(0) = true$, $\gamma_A(1)$：未定義, $\delta_A(0) = \delta_A(1) = 1$

AがΓを満足し，かつ，$\mathsf{T} \approx \mathsf{F}$を満足しないことは明らかである．従って，$\mathcal{R}_0$は sound でないことが知られる．

この例からすぐわかるように，$\mathcal{R}_0$が完全性を失なうのは，導出演算τ_Aがどの引数に対しても未定義である（$\tau_A = \phi$）ような項τを代入することが許されているからである．このことに着目して，新しく推論規則$\mathcal{R}$を定める．このために，新しい論理記号NVと<u>非空式</u>と呼ばれる式$NV(\tau)$を導入する．ただし，τは項である．Σ代数Aが$NV(\tau)$を<u>満足する</u>とは$\tau_A \neq \phi$，すなわち，τ_Aが少なくとも1つの引数に対して定義される関数であることである．従って，ここでは，純粋な等式論理に新しい論理記号と式が加えられた論理が取り扱われる．以下では，式と言えば等式又は非空式である．我々の推論規則$\mathcal{R}$は次の8個の規則からなる．

(1) 反射性：$\vdash \mathsf{t} \approx \mathsf{t}$

(2) 対称性：$\{\mathsf{t} \approx \mathsf{u}\} \vdash \mathsf{u} \approx \mathsf{t}$

(3) 推移性：$\{\mathsf{t} \approx \mathsf{u}, \mathsf{u} \approx \mathsf{s}\} \vdash \mathsf{t} \approx \mathsf{s}$

(4) 代入-I：$\{\mathsf{t} \approx \mathsf{u}\} \vdash \mathsf{s}[\mathsf{t}/x] \approx \mathsf{s}[\mathsf{u}/x]$

(5) 代入-II：$\{\mathsf{t} \approx \mathsf{u}, NV(\mathsf{s})\} \vdash \mathsf{t}[\mathsf{s}/x] \approx \mathsf{u}[\mathsf{s}/x]$

(6) 非空性-I：$\vdash NV(a)$．ただし，$a \in \Sigma_{\varepsilon,s}$．

(7) 非空性-II : $\{NV(\xi[\eta/x])\} \vdash NV(\xi)$

(8) 非空性-III : $\{NV(\xi), \xi \approx \eta[\xi/x]\} \vdash NV(\xi)$

最初の4つの規則は $\mathcal{R}_0$ と共通である. ただし, 代入の規則が2つに分けられていることに注意する. 残りの4つは非空式に関連するものである. 代入-IIの規則は導出演算 ξ_A が空になる可能性のある項 ξ の代入を禁止している. このことは非空式の解釈から明らかである. 又, 非空性I~IIIの規則が自然であることも非空式の意味から知られる.

式の集合 Γ から $\mathcal{R}$ を用いて式 φ が導出できるとき, $\Gamma \vdash^{\mathcal{R}} \varphi$ 又は単に $\Gamma \vdash \varphi$ と書く. Γ を満たすすべての代数が φ を満足するとき, $\Gamma \models \varphi$ と書く. $\Gamma \vdash^{\mathcal{R}} \varphi$ と $\Gamma \models \varphi$ が同値であるとき $\mathcal{R}$ は<u>完全</u>であるという. $\Gamma \vdash^{\mathcal{R}} \varphi$ ならば $\Gamma \models \varphi$ が成立するとき $\mathcal{R}$ は<u>sound</u>であるという. このとき次の定理が得られる.

<u>定理1 (soundness)</u> 任意の式の集合 $\Gamma \cup \{\varphi\}$ に対して, $\Gamma \vdash \varphi$ ならば $\Gamma \models \varphi$ である.

<u>定理2 (条件付完全性)</u> 任意の式の集合 Γ, 任意の非空式 φ, および任意の項 ξ, η に対して,

(i) $\Gamma \models \varphi$ ならば $\Gamma \vdash \varphi$ である.

(ii) $\Gamma \vdash NV(\xi)$ のとき, $\Gamma \models \xi \approx \eta$ ならば $\Gamma \vdash \xi \approx \eta$ である.

定理1, 2によって, 非空式に関しては $\mathcal{R}$ は完全であり, 等式 $\xi \approx \eta$ に対しては $\Gamma \vdash NV(\xi)$ (等価的に, $\Gamma \vdash NV(\eta)$, $\Gamma \vdash NV(\xi)$,

$\Gamma \vdash NT(\eta)$）であるときに RR は完全であることが解る．RR_0 の不完全性を示す前出の例について RR を適用すると，Γ から $\Gamma \approx \Gamma$ が決して導出できないことが知られる．それは，$NT(\alpha(\beta(\delta(\gamma))))$ が Γ から導かれないので，項 $\alpha(\beta(\delta(\gamma)))$ を例中の Γ の #1 および #2 の等式の中の変数 x に代入できないからである．

最後に，RR と弱準同形写像との関係を示そう．

定理3　任意の式の集合を Γ とする．非空項の集合を，$\xi \sim \eta \Leftrightarrow \Gamma \vdash \xi \approx \eta$ で定められる同値関係 $\sim$ で同値分割して得られる代数 $\mathfrak{T}$ は，$\mathfrak{V}_\Gamma$ が弱準同形写像のもとでなすカテゴリの始代数に同形である．

この定理にみられる RR と弱準同形写像の関係は，全域的代数の枠組の中での RR_0 と Σ 準同形写像[1]との関係と同じである．

4. あとがき　本文では，部分的代数に対しては従来の等式論理の推論規則 RR_0 が不完全であることを示し，条件付で完全である規則 RR を与えた．それとともに，RR と弱準同形写像の間の関係が，丁度，全域的代数の枠組における RR_0 と Σ 準同形写像との関係と一致することを示した．

筆者等は，この規則 RR と弱準同形写像に基づいて，部分的に定義される演算を持つ抽象データタイプの仕様記述法や，さらには，抽象データタイプ構成子（パラメタ付抽象データ

タイプ）の仕様記述法を開発している．抽象データタイプの実現の正当性は，実現する抽象データタイプが満たす式の集合から実現される抽象データタイプの仕様の中の式を導くことに帰着するので，アトミが決定可能であるための下に対する十分条件を発見することや，それに基づいた検証システムを開発することは重要な課題である．

謝辞　御指導賜る名古屋大学福村晃夫教授，並びに，日頃熱心に討論して頂く本多，福村，稲垣研の方々に深謝する．

文献

(1) J.A. Goguen and J.W. Thatcher and E.G. Wagner, "An initial algebra approach to the specification, correctness and implementation of abstract data types", IBM Research Report, RC-6487 (1976)

(2) J.A. Goguen and J. Meseguer, "Completeness of many sorted equational logic", SIGPLAN NOTICES vol. 16, no. 7, July 1981

(3) J.A. Guttag, E.G. Horowitz and D.R. Musser, "Abstract data types and software validation", CACM, 21, 12 (1978)

(4) T. Kasami, K. Taniguchi, Y. Sugiyama, K. Hagihara, I. Suzuki and J. Okui, "On algebraic techniques for program specifications", Technical Report of Group on Automata and Languages, IECE of Japan, AL78-5, (1978) (In Japanese)

(5) B.H. Liskov and S.N. Zilles, "Specification techniques for data abstraction", IEEE Transaction on SE, SE-1, 1 (1975)

(6) T. Sakabe, Y. Inagaki and T. Fukumura, "Weak homomorphism between data graphs", Technical Report of Group on Automata and Languages, IECE of Japan, AL75-72 (1976) (In Japanese)

(7) Y. Sugiyama, K. Taniguchi and T. Kasami, "A specification defined as an extension of a Base algebra", The Transaction of IECE of Japan, J64-D, 4 (April 1981)

(8) J.W. Thatcher, E.G. Wagner and J.B. Wright, "Data type specification: parameterization and power of specification technique", IBM Research Report RC-7757 (1979)

(9) J.D. Monk, "Mathematical logic", Springer-Verlag (1976)