JAIST Repository
https://dspace.jaist.ac.jp/

Title	現実的な構成的算術の関数的解釈に関する研究
Author(s)	土佐，尚之
Citation	
Issue Date	2001-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/1456
Rights	
Description	910075x，Supervisor:石原 哉，情報科学研究科，修士

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

現実的な構成的算術の関数的解釈に関する研究

土佐 尚之

北陸先端科学技術大学院大学 情報科学研究科

2001 年 2 月 15 日

キーワード: 限定算術, 多項式時間計算可能関数, Gödel Dialectica interpretation, Kreisel realizability, Kleene realizability.

1 背景

1958 年, Kurt Gödel[5] は finite type の functional に基づく限定記号のない理論による構成的算術体系の解釈を提案した。この解釈は *Gödel's Dialectica interpretation* と呼ばれている。Gödel *Dialectica* interpretation は構成的算術体系に対する無矛盾性の証明を与えるために導入された。

この *Dialectica* interpretation は T による HA の解釈を与える。HA とは一階の構成的算術体系 "*Heyting Arithmetic*" のことであり、T とは計算可能な finite-type functional に関する限定記号のない理論である。計算可能な finite-type functional は type 0 と原始帰納法に基づいて構成される type から成る。それゆえ *primitive recursive functionals of finite type* と呼ばれる。推論規則は命題論理の規則と帰納法から成る。

Gödel は T を高階の構成的算術体系に拡張した。この高階の構成的算術体系は HA^ω と呼ばれている。HA^ω は T に各 type の限定記号と推論規則を加えたものである。

A を HA^ω の任意の formula とした時、A^D を A の *Dialectica interpretation* と呼ぶ。ただし $\mathcal{A}$ を HA^ω の限定記号を含まない formula としたとき、A^D は

$$A^D \equiv \exists \vec{Y} \forall \vec{X} \mathcal{A}(\vec{Y}, \vec{X}),$$

という形の formula である。

Gödel はこれを用いて次のことを示した。

> もし A と A^D が HA^ω で証明可能ならば, HA^ω において
> $\forall \vec{X} \mathcal{A}(f(\vec{X}), \vec{X})$ を満たす計算可能関数 f が存在する。

Copyright © 2001 by Tosa Naoyuki

これは関数的解釈と呼ばれている。

また 1973 年、Troelstra[7] は HA^ω において *modified realizability* という方法を用いて同様のことを示した。

Gödel と Troelstra は計算可能関数と構成的算術体系 HA^ω との関係を示した。そこで本研究では多項式時間計算可能関数に対する論理的算術体系について考察する。

2 多項式時間計算可能

多項式時間計算可能関数に対する算術体系はは 1975 年に Cook[3] が PV というシステムを導入した。これは多項式時間計算可能関数の等式理論であるが限定記号を用いることができなかった。

そこで 1985 年に Buss[1] は多項式時間計算可能関数に対する古典論理に基づく算術体系 S^1_2 を導入した。この中で Buss は S^1_2 において

(1) $\forall \vec{x}(\exists y \leq t)A(\vec{x}, y)$

(2) $\forall \vec{x}\forall y\forall z[A(\vec{x}, y) \wedge A(\vec{x}, z) \rightarrow y = z]$

が証明可能ならば $\forall \vec{x}A(\vec{x}, f(\vec{x}))$ となるような関数 f が多項式時間計算可能関数であることを示した。これを「関数 f は Σ^{b+}_1-define できる」という。さらに 1986 年に Buss[2] は構成的論理に基づく算術体系 IS^1_2B を導入した。この中で Buss は S^1_2 と同様の性質が IS^1_2B においても成り立つことを示した。しかし IS^1_2B の定義はとても複雑であり、さらにクラス P を表すために用いた p-types, $\Box^P_1$-functionals も複雑なので、IS^1_2B は扱いにくい。そこで 1993 年に Cook[4] は構成的論理に基づく算術体系 IS^1_2 を導入した。このシステムはとてもシンプルであり、またクラス P を表す方法として function algebra という扱いやすい方法を用いた。そして Cook は function algebra を用いて「関数 f は Σ^{b+}_1-define できる」という事を導出し、さらに IS^1_2 と IS^1_2B が同等であるという事を示した。

3 構成的論理

計算可能関数における HA、多項式時間計算可能関数における IS^1_2 及び IS^1_2B は構成的論理に基づいている。構成的論理とは古典論理から排中律 $(A \vee \neg A)$ を除いた論理である。特徴としては $\exists xA(x)$ を証明するためには古典論理では (1) $A(x)$ が true となるような x を明示する。(2) $\forall x\neg A(x)$ を仮定したら矛盾することを証明する、という 2 つの方法があるが構成的論理では (1) の方法しか認められていない。つまり「存在する」ということを証明するためには「存在しないと仮定したら矛盾するから存在する」という方法は認められておらず「具体的に存在すること」を証明しなければならない。故に IS^1_2、IS^1_2B は始

めに導入した古典述語論理に基づいた体系 S_2^1 を構成的論理で作り直す必要があったのである。

4 現実的な構成的証明

Σ_1^{b+}-define は関数 f が多項式時間計算可能関数「である」ことを示したが計算可能関数のように多項式時間計算可能関数が「存在する」ことを示したい。そこで計算可能関数のために用いられた HA における $Dialectica$ interpretation 及び realizability の手法をシステム IS_2^1 に合うように形をかえて適用し、HA と同様の性質が証明された。つまり

> 「$\forall \vec{x} \exists y A(\vec{x}, y)$ という formula が IS_2^1 で証明可能ならば,
> $\forall \vec{x} A(\vec{x}, f(\vec{x}))$ となるような多項式時間計算可能関数 f が存在する。」

ということが証明された。

5 今後の課題

計算の複雑さの理論の研究の中に各クラスの包含関係を調べる研究がある。この研究の中の有名な問題として「$P = NP$ 問題」がある。これはクラス P と NP の関係が $P = NP$ なのか $P \subsetneqq NP$ なのかわかっていない、と言う問題である。これ以外にもいくつかクラスがあるが特に function algebra で表せるクラス K, T, $\mathcal{E}$ 等に着目する。例えば $T = K$ なのか $T \subsetneqq K$ なのか分かってない。そこで P における IS_2^1 のように各クラスにおける論理的算術体系を構築し、これを用いて包含関係を明らかにしたい。そこで最初、IS_2^1 における Π_i^b、Σ_i^b のような各クラスに適した hierarchy を見つける。次にこの hierarchy を基にして論理的算術体系を構築する。そして論理的算術体系上で「関数 f が Σ'-definable であることと関数 f が各クラスの関数であることは同値である。」ということを function algebra をを用いて証明する。そして realizability と $Dialectica$ interpretation を用いて各クラスの関数が存在する、と言うことを示す。最後にこれらの論理的算術体系を用いて各クラスの包含関係を明らかにできないか調べる。又、調べる手段として realizability と $Dialectica$ interpretation のように純粋な論理学の中で用いられた方法を応用できないか検討する。

参考文献

[1] Samuel R.Buss, *Bounded Arithmetic*, Ph.D. dissertation, Princeton University 1985; reprinted Biblopolis, Napoli, 1986.

[2] Samuel R.Buss, *The polynomial hierarchy and intuitionistic bounded arithmetic*, Springer-Verlag, Berlin, 1986.

[3] S.A.Cook, *Feasibly constructive proofs and the propositional calculus.*, Proc.7th A.C.M. Symposium on the Theory of Computation,(1975), pp.83-97.

[4] S.A.Cook, *Functional interpretation of feasibly constructive arithmetic*, Annals of Pure and Applied Logic, 63 (1993), pp.103-200.

[5] Kurt Gödel, Über *eine bifher noch nicht* benützte *erweiterung des finiten standpunktes*, J. of Philosophical Logic, 9 , pp.133-142.

[6] S.C.Kleene, *On the interpretation of intuitionistic number theory*, J. Symbolic Logic, 10 , pp.109-124.

[7] A.S.Troestra, *Metamathematical investigation of intuitionistic arithmetic and anlysis*, Springer-Verlag Lecture Notes in Mathematics, No.344, 1973.