Functional Interpretation of Feasibly Constructive Arithmetic

Naoyuki Tosa

School of Information Science,
Japan Advanced Institute of Science and Technology

February 15, 2001

Keywords: bounded arithmetic, polynomial time computable function, Gödel Dialectica interpretation, Kreisel realizability, Kleene realizability.

1 Background

In 1958, Kurt Gödel[5] suggested an interpretation of intuitionistic arithmetic in a quantifier-free theory of functionals of finite type, an interpretation which has since come to be known as *Gödel's Dialectica interpretation*.

First Gödel *Dialectica* interpretation was introduced to provide a consistency proof for intuitionistic arithmetic by elementary logic by an interpretation of an arithmetical statement by a quantifier-free formula in a theory of objects of finite type.

The *Dialectica* interpretation reduces HA to a theory T, where HA is intuitionistic first-order arithmetic "*Heyting Arithmetic*" and T is a quantifier-free theory of computable finite-type functionals, which is defined by schemata for explicit definition and a natural extension of primitive recursion to finite types, and are therefore called *primitive recursive functionals of finite type*. Inference rules of T are propositional logic and its induction rule.

Gödel tried to extend T to the system of intuitionistic higher type arithmetic. This higher type arithmetic is called HA^ω. We can get HA^ω from T by adding each type quantifiers and rules.

Let A be any formula of HA^ω. We associate its *Dialectica interpretation* A^D, which is a formula of the form

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

where $\mathcal{A}$ is a quantifier-free formula of HA^ω.

Then Gödel's main result is as follows:

if A and A^D are provable in HA^ω, then there exists
a primitive recursive functional f such that $\forall \vec{X} \mathcal{A}(f(\vec{X}), \vec{X})$ is provable in HA^ω.

This is called *functional interpretation*.

On the other hand, Troelstra[7] used an other method of realizability for same purpose in 1973.

Realizability used by Troelstra for computable functionals is *modified realizability*. This was first introduced and used by Kreisel in 1959. Modified realizability in its abstract form provides interpretations the various HA^ω-versions into themselves. Modified realizability transform each formula A to $\vec{x}\underline{\mathbf{mr}}A$ ($\vec{x}$ modified realizes A). Then a notion $\vec{x}\underline{\mathbf{mr}}A$ means "a list of terms $\vec{x}$ makes A true in HA^ω" . In other words, "there is a list of terms $\vec{x}$ such that A is true in HA^ω".

Troelstra used the systems HA^ω same as Gödel . He proved two theorems. One is that if $\forall \vec{x} \exists y A(\vec{x}, y)$ is a theorem of HA^ω, then there exists a primitive recursive functional f and a term $\vec{t}$ such that $\forall \vec{x}(\vec{t}(\vec{x})\underline{\mathbf{mr}}A(\vec{x}, f(\vec{x})))$ is a theorem of HA^ω. Another is that if $\forall \vec{x}[\vec{t}(\vec{x})\underline{\mathbf{mr}}A(\vec{x}, f(\vec{x}))]$ is a theorem of HA^ω, then $\forall \vec{x} A(\vec{x}, f(\vec{x}))$ is a theorem of HA^ω.

Gödel and Troelstra proved the relations computable functionals and logical arithmetics HA, HA^ω. So we consider logical arithmetic which is related to polynomial time computable functionals.

2 Polynomial Time Computable Functionals

Arithmetic for polynomial time computable functionals was first suggested by Cook[3] in 1975. This system PV is equational system of polynomial time computable function. But this system is quantifier free.

In 1985 Buss[1] introduced a system S^1_2 which is based on classical first order predicate calculus. Buss proved that if

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

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

are provable in S^1_2 then a function f which is $\forall \vec{x} A(\vec{x}, f(\vec{x}))$ is a polynomial time computable function. We call this "we can Σ^{b+}_1-define the function f". In 1986 Buss[2] developed an intuitionistic version IS^1_2B of S^1_2. Buss proved relation for polynomial time computable functions and arithmetic same as S^1_2. But definition of IS^1_2B is complicated. And class P which is defined by p-types and $\Box^P_1$-functionals is complicated. Therefore in 1993 Cook[4] developed an another intuitionistic version IS^1_2. Definition of IS^1_2 is simple. And Cook used function algebra as a definition of P. By use this Cook proved "we can Σ^{b+}_1-define the function f in IS^1_2". And Cook proved IS^1_2 and IS^1_2B are equivalent.

3 Intuitionistic logic

The system HA for computable functions and the system IS_2^1 and IS_2^1B for polynomial time computable functions are based on intuitionistic logic. For this the difference between classic logic and intuition principle logic is explained by an example. The example is as follows. in order to prove $\exists x A(x)$, there are two methods. One is to find x such that $A(x)$ is true. Another is to prove that if assume $\forall x \neg A(x)$ then arise contradiction. In intuitionistic logic, in order to prove $\exists x A(x)$, there is only a method. It is to to find x such that $A(x)$ is true. Another method which is to prove that if assume $\forall x \neg A(x)$ then arise contradiction is not allowed. That is, it means that the proof based on intuitionistic logic had proved concrete existence in finite. Therefore it is necessary to prove on intuitionistic logic.

4 Feasibly constructive proof

There is a big difference between Σ_1^{b+}-definable function "is" polynomial time computable function and there "exists" a polynomial time computable function which is Σ_1^{b+}-definable. Hence we hoped that existence of polynomial time computable function is guaranteed. So we used two techniques same as computable function for this proof. And we proved by *Dialectica* interpretation and realizability that

> if a formula $\forall \vec{x} \exists y A(\vec{x}, y)$ is provable in IS_2^1, then there exists
> a polynomial time computable function f which satisfies $\forall \vec{x} A(\vec{x}, f(\vec{x}))$.

5 future subject

One of study of computational computability is to study the including relation of some classes. In this study there is the famous problem "$P = NP$ problem". This is a problem which relation between P and NP is "$P = NP$?" or "$P \subsetneqq NP$?" There are some classes besides P and NP. In these classes we direct my attention to classes which is definable by function algebra. For example, class K, T and $\mathcal{E}$ are definable by function algebra. In these classes it does not solve whether it is $T = K$ or $T \subsetneqq K$. So I want to express functions of each class by logical arithmetic like functions of class P by IS_1^2, and we want to solve including relation of some classes. Therefore first we find suitable hierarchy like Π_i^b and Σ_i^b in IS_2^1 because we know that class P and hierarchy are close relations. Next we construct logical arithmetic based on hierarchy. Next we show by use of function algebra that a function f is Σ'-definable iff a function f is a function of each class in each system. And we prove in system by realizability and *Dialectica* interpretation that there exists a function of each class which can Σ'-define. Finally using these, I want to solve the relation of some classes. Then we need to study pure logic because we might be able to use tools of pure logic for study of computational complexity like realizability and *Dialectica* interpretation.

References

[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.Troelstra, *Metamathematical investigation of intuitionistic arithmetic and analysis*, Springer-Verlag Lecture Notes in Mathematics, No.344, 1973.