数理解析研究所講究録
第 180 巻 1973 年 39-51



# Arithmetically definable analysis

静大理 八杉満利子

In the mimeographed notes [7], "A conservative extension of Peano arithmetic", Takeuti and Kreisel defined a conservative extension of Peano arithmetic and develope in it the so called calculus. They also suggest how to modify the system, retaining the proof theoretical strength unchanged, so complex analysis can be developed in the resulting system.

Their method suggests, as they indicate in their notes, that analysis is, in its essence, arithmetical. A completion of their program would mean an execution of the Hilbert's program: an attempt to ensure the reliability of classical mathematics in the sense that it be developed within the "finitary" veiwpoint (in some sense). Hilbert himself endeavoured to carry out his own program. A recent, successful attempt of the kind is seen in Bishop's work [1]. Here he reconstructs most part of analysis in a "constructive" manner. Although he denounces the formalists' approach from the outset, it is important to learn that the most part of his project (and calculus entirely) can be formulated in a conservative extension of Heyting arithmetic (cf. [3]). As we know, the formal systems of Heyting arithmetic and Peano arithmetic are proof-theoretically equivalent. Therefore I do not think we are obliged to comit one way or another, mathematical approach or formalists' approach, at this point. If the strength of Peano arithmetic is necessary anyway to do any part of mathematics and the equivalences (of proof-theoretical strength) among the different systems of this level can be established relatively straightforward, it should not be of any serious importance which standpoint one takes in developing mathematics, as long as a coherent direction based on a clear principle is observed.

In passing we wish to note that Bishop and Cheng have proposed an improved version of constructive measure theory in [2]; its logical structure is yet to be investigated.

Here we wish to continue a study of analysis along the line of [7]. Analysis can be naturally developed in their system; statements and proofs take the form of ordinary mathematics; only arbitrary quantifiers of higher type are eliminated. So in an existence statement, an object satisfying a condition is actually constructed. There are no strange notions or technical terms.

We shall outline how to develope the theory of ordinary differential equations and the theory of Lebesgue measure in a conservative extension of Peano arithmetic. The detail will appear later.

It is not, however, our goal to keep rewriting every portion of mathematics in this line. After certain amount of experience, we should be able to see the logical structure behind (actual) mathematics, hence to establish a more systematic way how to eliminate higher type quantifiers. I believe that its implication is more profound than we are now aware. I hope our trial here is only a start.

The author is indebted to Professor R. Kondo for answering many of her questions.

§ 1. We start with an exposition of the idea in [7]. Let us denote the conservative extension of Peano airhtmetic defined in [7] by S. The language of S consists of that of finite type theory, the language of Peano arithmetic, a unary predicate N and a binary predicate = . The logical system of S is the predicate calculus of finite types in which the comprehension abstracts are restricted to the arithmetical ones <u>without</u> higher type free variables. The mathematical axioms of S are those of Peano arithmetic, reading N(a) "a is a natural number", with the full induction and the full equality axiom. For instance, the mathematical induction is formulated as:

$\forall y_1 \ldots \forall y_n (A(0) \wedge \forall x(N(x) \supset (A(x) \supset A(x')) \supset \forall x(N(x) \supset A(x)))$.

The type 0 objects stand for rationals.

Developing a mathematical theory in the system S means to assume that all the mathematical objects in the theory are defined in terms of arithmetical abstracts, allowing some parameters, i.e. some higher type free variables. We say that such objects are arithmetically definable. Therefore in order to claim the existence of an object, we must construct an arithmetical object satisfying a certain condition. For example, an arithmetically definable real is defined by an abstract $\{r\}A(r)$, where r is a variable of type 0 and A is arithmetical (with some parameters) and where it is provable in S that $\{r\}A(r)$ defines a Dedekind cut (of rationals).

We shall abbreviate 'arithmetically definable' to 'ad'.

An interval $[a,b]$ is said to be arithmetically definable if a and b are ad reals. An ad function is defined by an arithmetical abstract $\{\gamma, r\}A(r, \gamma)$, where $\gamma$ is a variable of type

1 and the function value for the argument $\gamma$ is defined to be $\{r \mid A(r, \gamma)\}$. Intuitively this defines a real function $f(\gamma) = \{r/A(r, \gamma)\}$. The familiar functions such as +, -, x, ÷ are all arithmetically definable. The coninuity of a function is defined as usual in the $\varepsilon - \delta$ form, assuming that $\varepsilon$ and $\delta$ are rationals.

Other mathematical notions such as a domain, a sequence, a series, are defined in a similar manner.

To everybody's knowledge, the basis of calculus is the completeness of the system of reals, or the lub property (the least upper bound property): every bounded set of reals has the least upper bound. Logically this corresponds to the ( full) second order comprehension axiom (the existence of an arbitrary Dedekind cut of rationals). That calculus is essentially arithmetical means that it is sufficient to assume the lub property for an arbitrary, bounded and arithmetically definable set of (arithmetical) reals (hence the lub is also arithmetically definable), and the key factor of the sufficiency is the denseness of rationals in reals. Consider, as an instance, a function which is continuous around a number a. $\lim_{x \to a} f(x)$ is defined to be

$$\limsup_{x \to a} f(x) = \liminf_{x \to a} f(x)$$ when the equality holds. Due

to the denseness of rationals and continuity of f, $\limsup_{x \to a} f(x)$

can be expressed as $\{t\}(\forall r > 0\ \exists s(|s| \leq r \wedge A(s+r,t)))$, which is arithmetical.

This now implies that the differentiation is an arithmetical operation: $f'(a) = \lim_{h \to 0} \frac{f(x+h)-f(x)}{h} = \lim_{r \to 0} \frac{f(x+r)-f(x)}{r}$, where $r$ ranges over rationals.

The integral (of a continuous function defined in an interval) can be defined as the limit of an arithmetically definable sequence of areas of rectangles, hence is arithmetically definable. The fundamental theorem of the calculus is only a consequence of the definition.

Among the various existence statements of calculus, let us consider, as an exemplary case, the intermediate value theorem of a continuous function defined in a closed interval. Let a and b be arithmetically definable reals such that $a < b$ and let f be an arithmetically definable function which is continuous in $[a,b]$. **Further, suppose $f(a) < 0$ and $f(b) > 0$. Define $A =$** $\{r/a \leq r < b \wedge \forall s < r(f(s) < 0)\}$ and $A^o = \{t/\exists r(r \in A)\}$, where r,s and t stand for rationals as well as reals corresponding to the rationals r, s and t respectively. $A^o$ is arithmetically definable and defines a Dedekind cut of rationals. It is easy to see that $A^o$ defines the least number (between a and b) for which $f(A^o) = 0$. Thus we have presented an ad real satisfying the conditions.

In order to define a system of complex numbers, introduce an individual symbol i and a unary predicate r (r(a) reads "a is a real rational") to S. The type 0 objects of the extended system of complex numbers are interpreted as complex rationals. An arithmetical abstract of type 1 is said to deinfe a complex number if it represtnes a set of complex rationals satisfying the "Dedekind Condition". The familiar functions of complex numbers are ad; in particular $\bar{\alpha}$ is. Thus the notion of the real part and the imaginary part are derfinable: $\mathrm{Re}(\alpha) = \alpha + \bar{\alpha}/2$ and $\mathrm{Im}(\alpha) = \alpha - \bar{\alpha}/2i$.

Much part of complex analysis depends on the theory of real numbers and functions, hence can be arithmetically definable. For example the power series is an ad notion (when the coefficients are).

The complex integral can be defined by means of real integral. In proving Cauchy's theorem, the inductive definition of integrals along bisected rectangles can be expressed arithmetically.

We restrict the functions and their domains to ad ones; all the examples we see are ad. It is easy to see that for any differentiable (i.e. analytic) function (in some "nice" domain), say f, $\{f^{(n)}\}_n$ is an ad sequence of functions; this is due to Cauchy's integral formula;

$$f^{(n)}(z) = n!/2\pi i \int_C \frac{f(\zeta)\,d\zeta}{(\zeta - z)^{n+1}} .$$

The exponential and trigonometric functions are ad. In proving this, it can be demonstrated that those familiar reals such as e and $\pi$ are ad: $e^z = \sum_{n=0}^{\infty} z^n/n!$ ,

$\sin z = \dfrac{e^{iz} - e^{-iz}}{2}$ etc. $\pi$ is the smallest period of $e^z$;

this property can be written down arithmetically.

§ 2. The theory of ordinary differential equation ~~onew~~ owes much to the fundamental thorem of calculus; the integral of an ad continuous function (defined in a nice domain) is ad and its derivative is the original function; hence the existence theorem can be proved in the system S. The initial value problem should be phrased so the solutions are arithmetical in the initial condition. For the method of successive approximation, we may assume that the sequence of approximations is an ad sequence (of functions).

We will mention here only a few points. The initial value problem being well-set should be expressed as follows. Let $y' = F(x,y)$ be a normal first order differential equation where F is ad and let D be an ad domain (of (c,x)). The initial value problem for this equation is said to be well-set in D if there is an ad function of three arguments, say $f(x_0,x,c)$, continuous in c such that for any $(x_0,c)$, $y = f(x_0,x,c)$ is a unique solution for the given differential equation.

We say that an ad function defined on a "nice" domain D, say F, satisfies a Lipschitz condition in D when there is a positive, ad real L such that
$\forall x,y,z((x,y) \in D \wedge (x,z) \in D \rightarrow |F(x,y) - F(x,z)| \leq L|y-z|)$.
Then the comparison theorem can be stated and proved as follows. Given an ad F and a, where F satisfies a Lipschitz condition for $x \geq a$ with L. If g and f are ad functions such that g is a solution of $y' = F(x,y)$, f satisfies $f'(x) \leq F(x,f(x))$ for $x \geq a$ and $f(a) = g(a)$. Then $f(x) \leq g(x)$ for $x \geq a$.

$f(a) = g(a)$ is the assumption. At the start of the proof, one supposes $f(\alpha) > g(\alpha)$ (with $\alpha$ as a parameter) in the given interval and let $x_0$ be the largest $x$ such that $a \leq x \leq \alpha$ and $f(x) \leq g(x)$. Then $f(x_0) = g(x_0)$. The only point is that $x_0$ be ad (with some parameters). Let $C(r)$ denote the formula $\forall s(a \leq r < s \leq \alpha \rightarrow f(s) > g(s))$ (where r and s stand for rationals). $C(r)$ is ad and the continuity of f and g and the denseness of rationals in reals imply that $f(s) > g(s)$ for any s satisfying the condition. Let $x_0 = \inf\{r/C(r)\}$, where the first r here stands for the real corresponding to the rational r, hence $x_0$ is ad. $f(x_0) = g(x_0)$ is provable in S and the rest of the usual argument goes through.

As an example of the superposition principle for the homogeneous linear differential equation: $u'' + pu' + qu = 0$ where p and q are ad, consider the Legendre differential equation: $d/dx\,[(1 - x^2)du/dx] + n(n+1)u = 0$. The singular points are $x = \pm 1$ (which are ad). Supposing u can be expanded in a power series $\sum_{k=0}^{\infty} a_k x^k$, the superposition principle yields an recurrent equation: $a_{k+2} = (k(k+1) - \lambda)a_k/(k+1)(k+2)$ where $\lambda$ is a parameter. Given $a_0$, we can express the even coefficients as: $a_{2k} = \prod_{l=0}^{k} (2l(2l+1) - \lambda)/(2(k+1))!$, which is ad. The odd coefficients can be also expressed arithmetically.

The method of successive approximations is described as follows. Given $x'(t) = F(x,t)$, the operator U is defined by $U(x(t)) = c + \int_a^t F(x(s),s)ds$ (the right hand side is ad), with c as a parameter. Let $x^0 = c$ and denote $x^n = U^n[x^0]$. Then $\{x^n\}_n$ converges uniformly for $|t-a| \leq T$ (where T is given).

Here we assume that $\{x^n\}_n$ is ad as a sequence of functions. This does not limit the applicability of this method; all the examples we have satisfy this condition and we do not forsee any counterexample. In ~~passing the~~ proving the statement above, we need to consider a constant $M = \sup_{|t-a| \leq T} |F(c;t)|$, but this is equal to $\sup_{|r-a| \leq T} |F(c;r)|$ where r stands for rationals. The rest of the mathematical argument goes through. As an example; the approximations for the equation $u(t) = 1 + \int_0^t su(s)ds$ is $x^n(t) = \sum_{k=0}^{n} t^{2k}/2^k.k!$, hence $\{x^n\}_n$ is ad as a squence of functions.

§3. As we have observed in the discussion given above, the arithmetical nature of calculus depends on the following facts. ¶ Denseness of rationals in reals, hence the sufficiency of the lub property applied to an ad set of (ad) reals, indexed by rationals. This menas the sufficiency of quantification over type 0 variables, viz. the arithmetical quantification, if we may say so.

The arithmetical nature of the fundamental operations. The only basic operations in analysis are differentiation and integration, both of which are arithmetical.

A careful examination of the proofs of various existence statements has proved that for our purpose regarding reals as sets of rationals is most useful; an operation such as taking lim sup is reduced to taking countable unions and intersections.

§ 4. We shall outline how to define Lebesgue integral and measuraable functions (and sets) . It is more convenient for our purpose to employ the approach of Daniell integral; start with continuous functions on a compact interval (of reals) and their integrals,and gradually expand the class of integrable functions. The whole point is to avoid quantifiers over sequences of functions in the mathematical theory; instead, we always consider a function together with a few sequences of functions, the latter being regarded as a representation of the former.

A lucid explanation of Daniell integral is seen, for example, in [6] which we follow for a hile.

Let X be the space [0,1] and I be the integration operator on the continuous (and ad of course) functions on X. Suppose f and $\{f_n\}_n$ are ad functions on X. Let $U(f, \{f_n\}_n)$ be a formula expressing the relation: Each function $f_n$ is continuous and $f_n \uparrow f$. If $U(f, \{f_n\}_n)$ is provable (in S), then we say that $\{f_n\}_n$ is a representation of f . Statements concerning U which are naturally expected to be true, such as $U(f, \{f_n\})$ & $U(g, \{g_n\}) \rightarrow U(f + g, \{f_n + g_n\})$, are provable. Now define $I(f) = \lim_n I(f_n)$. This definition is justified, for the value is independent of the representations. I(f) is ad.

$-U(f, \{f_n\})$ is defined to be $U(-f, \{f_n\})$. If $-U(f, \{f_n\})$ then define $I(f) = -I(-f)$.

Among other properties concerning U and -U, we can show that if $-U(g, \{g_n\})$, $U(h, \{h_n\})$ and $g \leq h$, then $U(h-g, \{g_n + h_n\})$ and $I(h) - I(g) = I(h-g) \geq 0$.

Note that here all the functions are of finite value; $\infty$ is not allowed as a value.

The notion corresponding to summability (of finite functions) is expressed as follows. Let $S(f, \{g_n\}_n, \{h_n\}_n, \{g^n_m\}_{n,m}, \{h^n_m\})$ denote the relation: $\forall n(-U(g_n, \{g^n_m\}_m) \& U(h_n, \{h^n_m\}_m) \& (g_n \leq f \leq h_n) \& R(I(g_n)) \& R(I(h_n)) \& (0 \leq I(h_n) - I(g_n) < 1/n))$.
In the last clause, the explicit dependence of the subscripts of $h_n$ and $g_n$ (i.e. n) on the bound 1/n will turn out to be necessary. If $S(f, \ldots\ldots)$ is provable (in S), where f and all the function sequences are assumed to be ad, we say that $\frown\mathfrak{x}(\{g^n_m\}_m, \{h^n_m\}_m)$ is a representation of f; ~~and~~ it also follows that $\lim_m I(g_n) = \lim_n I(h_n)$ is provable. Define I(f) to be either of those limits. It takes only a straightforward, mathematical argument to show that I(f) is independent of its representation. Note that $I(f) < \infty$. The I thus extended has all the properties of I (with respect to the functions satisfying S(...)).

Consider the theorem: f and $\{f_n\}_n$ are ad. Suppose, for each n, the function $f_n$ satisfies $S(f_n, \ldots.)$ with some appropriate function sequences, $f_n \uparrow f$ and $\lim I(f_n) < \infty$. Then f satisfies $S(f, \ldots)$ with some appropriate ad function sequences and $I(f_n) \uparrow I(f)$. Let us assume $f_0 = 0$, hence $f_n \geq 0$. Suppose $\forall n S(f_n, \{k^n_m\}_m, \{\hat{k}^n_m\}_m, \ldots)$, where we do not write ... explicitly. We shall concentrate on the first two functions sequences. Define $h^n_m = k^n_{2m} = \hat{k}^{n-1}_{2m}$ and $\hat{h}^n_m = \tilde{k}^n_{2m} - k^{n-1}_{2m}$. They are obviously ad and $I(h^n_m)$ $\downarrow I(f_n - f_{n-1})$ and $I(\hat{h}^n_m) \uparrow I(f_n - f_{n-1})$. Let $\varphi(n,m) = 2^n.m$. Then $0 < I(h^n_{\varphi(n,m)}) - I(\hat{h}^n_{\varphi(n,m)}) < 1/\varphi(n,m)$.
Therefore $I(h^n_{\varphi(n,m)}) < I(f_n - f_{n-1}) + 1/\varphi(n,m)$.
$f_n \leq \sum_{i=1}^{n} h^i_{\varphi(i,m)}$ and $\sum_{i=1}^{n} I(h^i_{\varphi(i,m)}) < I(f_n) + \sum_{i=1}^{n} 1/\varphi(i,m)$.
Let $\ell_m = \sum_{i=1}^{n} h^i_{\varphi(i,m)}$. $\ell_m$ is ad and is a U-function (the meaning of this abbreviated expression must be obvious). $I(\ell_m) =$

$\sum_{i=1}^{\infty}$ I($h_{\varphi(i,m)}^{i}$)) and $f \leq \ell_m$ . $I(\ell_m) \leq \lim_n I(f_n) + 1/m$. With a symmetric argument, we can define -U-functions $\tilde{\ell}_m$ such that $\tilde{\ell}_m \leq f$ and $I(\tilde{\ell}_m) \geq \lim I(f_m) - 1/m$. Therefore $\lim_n I(f_n) = I(f)$ and $S(f, \{\tilde{\ell}_{2m}\}, \{\ell_{2m}\}, \ldots)$, where ....is defined appropriately (depending on the construction of $\ell_m$ and $\tilde{\ell}_m$).

We now introduce $\infty$ ( = the set of all rationals) as an extended real, and allow the functions to assume the value $\infty$ also. An ad function on X is mearuable if for each $\ell$ ( a natural number) $(f \wedge \ell) \vee (-\ell)$ is an S-function with some appropriate function sequence, which we denote by $\Phi(\ell)$ collectively, where $\Phi(\ell)$ is ad in $\ell$. I(f) is defined to be $\lim_{\ell} I((f \wedge \ell) \vee (-\ell))$.

If f is an S-function, then it is measurable.

X can be an arbitrary compact interval, say $X_p$ = [-p,p] where p is a positive integer.

Let f be a non-negative ad function of reals. f may assume the value $\infty$ . f is said to be measurable if $\forall p S(f \upharpoonright X_p, \Phi(p))$ where $f \upharpoonright X_p$ denotes f restricted to the domain $X_p$ and $\Phi(p)$ denotes appropriate function sequences which are ad in p. I(f) is defined to be $\lim I(f \upharpoonright X_p)$. f is said to be integrable if $I(f) < \infty$ .

Let f be an ad function of reals such that its positive part $f^+$ and the negative part $f^-$ are integrable.

Then define $I(f) = I(f^+) - I(f^-)$.

The measure of a set (of reals) is defined to be the integral of its characteristic function.

Reference

1. E. Bishop, Foundations of constructive analysis, McGraw-Hill Book Co., 1967.

2. E. Bishop and H. Cheng, Constructive measure theory, Memoirs of the American Mathematical Society, No. 116,1972.

3. N. Goodman and J. Myhill, The formalization of Bishop's constructive mathematics, Toposes, Algebraic geometry and Logic, Lecture notes in Mathematics, 274,1972, Springer-Verlag, pp83-96.

4. D. Hilbert, Über das Unendliche, Math. Ann. Vol. 95, 1926, pp 161-190.

5. D. Hilbert, Die Grundlagen der Mathematik, Abhandlungen aus dem Math. Seminar der Hamburgischen Univ., Vol. 6,1928, pp 65-85.

6. L. Loomis, An introduction to abstract harmonic analysis, Van Nostrand Co.

7. G. Takeuti and G. Kreisel, A conservative extension of Peano arithmetic, Mimeographed notes, 1972.