Dokl. Akad. Nauk SSSR
Tom 227 (1976), No. 6

Soviet Math. Dokl.
Vol. 17 (1976), No. 2

ON THE PRINCIPLE OF CONSERVATION OF INFORMATION IN INTUITIONISTIC MATHEMATICS

UDC 517.12

L. A. LEVIN

1. Herein we consider a new intuitionistic axiomatic theory, based on the principle of conservation of information (the axiom schema (4.1)). This principle states that in the process of forming a free choice sequence there can be no unbounded growth of the quantity of information contained in it about the truth of arithmetic predicates. For this we use the concept of "quantity of information", introduced by A. N. Kolmogorov [2] on the basis of "algorithmic complexity" and later made more precise in [3]. Also studied in [3] was the "principle of conservation of information" in the form of laws of probability theory, and the Thesis 1 was formulated, according to which these laws are fulfilled, in general, in any process of an arbitrary physical nature. If we interpret intuitionistic sequences as sequences whose members can be obtained in some sort of process actually taking place in the physical world, then the thesis mentioned substantiates the naturalness of the adoption of the principle (4.1).

If we term as "elementary" a physical process generating a sequence that cannot be represented as the result of applying a computable operator to the result of a physical process "simpler" than the one under consideration, then, extrapolating the properties of familar natural phenomena, we can plausibly assume that:

1) any natural process generating a sequence can be "understood", i.e. can be represented in the form of a superposition of an "elementary" (in the sense above) physical process and a computable operator;

2) the sequence generated by an elementary physical process is always random according to some very simple probability distribution.

Then the theorem in [3] on the nongrowth of information in random and computable processes is sufficient for the justification of the principle of conservation of information.

2. Our theory $\mathfrak{A}$ Inf will be constructed by adding a group of axioms ((4.1), (4.2), and later (5.1)) to the calculus $\mathfrak{A}$, which we shall describe in this section and take as a basis. $\mathfrak{A}$ is formulated in the usual language of second-order arithmetic. This language is obtained by adding to the language of first-order arithmetic (see [1], §38) a countable list of second-order variables denoting sequences of natural numbers or functions, and adopting the following rules for the formation of terms and formulas: if α is a second-order variable, t is a term, and Φ is a formula, then $\alpha(t)$ is a term, and $\forall \alpha\Phi$ and $\exists \alpha\Phi$ are formulas. A formula will called *absolute* if it is constructed from equalities between terms with the aid of conjunction, negation and universal quantification on *first-order* variables. Absolute formulas have identical meanings in intuitionistic and classical theories. By a pair of terms (a_1, a_2) we shall mean the term $(a_1 + a_2)^2$

AMS (MOS) subject classifications (1970). Primary 02E05, 02C15, 94A15; Secondary 10N99, 02F99.

$+ a_1$. Obviously, this numbering of pairs is invertible. In the same fashion we give meaning to the expressions $(a_1, \ldots, a_n)$, $\alpha(a_1, \ldots, a_n)$, (α, β), etc. Suppose, for a number n and a term α, the formula $\exists t_0(\alpha(t_0) = n + 1 \,\&\, \forall t < t_0 \;\; \alpha(t) = 0)$ holds. Then, allowing liberties with the language, we can use the following notation for this fact: $n = \mathrm{pr}_t \alpha$ (n is equal to the projection on t of the term α). Handling the expression $\mathrm{pr}_t\alpha$ like a term will never cause any misunderstanding, in particular thanks to (2.2). The axioms for $\mathfrak{A}$ consist of the axioms of first-order arithmetic (see [1], Russian p. 467; Schema 8 is taken in the intuitionistic version 8′) and the following three principles of second order arithmetic:

Schema of choice:

$$(\forall n(\neg A \to \exists x P(x))) \to \exists \alpha \forall n(\neg A \to P(\mathrm{pr}_t \alpha(n, t))). \tag{2.1}$$

Leningrad principle:

$$\forall \alpha((\neg \forall n\, \alpha(n) = 0) \to \exists n\, \alpha(n) \neq 0). \tag{2.2}$$

Axiom of countability

$$\exists \alpha\; \forall \beta\; \exists k\; \forall n\, \beta(n) = \mathrm{pr}_t \alpha(k, n, t). \tag{2.3}$$

Axiom (2.3) asserts that the set of intuitionistic sequences is countable. Under the interpretation of intuitionistic sequences as sequences of results of real macroevents in the physical world, Axiom (2.3) corresponds to the customary statement on the separability of space-time. We shall not discuss the axioms of $\mathfrak{A}$ in detail, since this has been done many times in the literature, We observe only that for the construction of any "complete" (satisfying Theorem 1) calculus, it is necessary to take either these axioms (if only under double negation), or their negation, or their equivalence to some undecidable absolute statements of number theory. The last two variants seem to us less natural. It is well known that (2.1)–(2.3) are inconsistent with the principles of continuity and Bar-induction. In this, the calculus $\mathfrak{A}$ more resembles constructive analysis. The principle difference between them, however, lies in the absence from $\mathfrak{A}$ of Church's thesis. Its rejection is dictated by the desire to interpret the sequences of our theory as sequences of results of events occuring in nature. Of course, the calculus $\mathfrak{A}$, lacking both Bar-induction and Church's thesis, is still too weak. Nonetheless, we have

Proposition 1. *For any formula Φ there exists an absolute formula P such that* $\mathfrak{A} \vdash \Phi \sim \forall \alpha \exists \beta P$.

3. Some notions in the algorithmic theory of information. The background is explained briefly and superficially; for more detail, see [3] (as well as [2], [5]).

A nonnegative real function $f(x)$ defined on finite sequences of natural numbers is called *enumerable* (from below) if the set of pairs (r, x), where r is a rational number less than $f(x)$, is recursively enumerable. A function $f(x, \alpha)$ is called *enumerable* (from below) if $f(x, \alpha) = \sup f'(x, (\alpha)_n)$, where x is a natural number, α is an infinite sequence of natural numbers, $(\alpha)_n$ is its segment of length n, and f' is an enumerable function. A function $f(x)$ will be called *computable* if the functions $f(x)$ and $1/f(x)$

are enumerable. The signs $\succcurlyeq$, $\preccurlyeq$, $\asymp$ denote inequality and equality to within an additive constant.

Proposition 2. *There exist maximal, to within a multiplicative constant, ~~semi~~-computable functions in the classes*: a) $\{f\colon \sum f(x) < \infty\}$; b) $\{f\colon \forall_\alpha \sum f(x, \alpha) < \infty\}$; c) $\{f\colon \forall s \sum f(sx) \leq f(s)\}$, *where* x *is a natural number,* α *is a sequence, and* sx *is the sequence obtained by adding* x *onto a finite sequence* s.

The first of these maximal functions is denoted by $P(x)$, the second by $P(x|\alpha)$, the third by $M(s)$; the integral parts of the absolute values of their logarithms are denoted respectively by $KP(x)$, $KP(x|\alpha)$ and $KM(s)$. Let α, β be finite or infinite sequences. Then the amount

$$I(\alpha:\beta) = \left[\log_2 \sum (P(x|\alpha)\cdot P(y|\beta)\cdot P(x,y)/P(x)\cdot P(y))\right]$$

is called the quantity of information in each of them about the other.

For finite s and any β, $KM(s) \succcurlyeq I(s\colon \beta)$ holds, so $KM(s)$ can serve as a characterization of the "full amount of information in s", or the "complexity of s". Let $f(s)$ be an arbitrary computable function such that $f(s) \geq \sum f(sx)$. Then $[-\log_2 f(s)] \succcurlyeq KM(s)$ by the definition of KM. For certain α there may exist a computable f for which this inequality becomes the equality $KM((\alpha)_n) \asymp [-\log_2 f((\alpha)_n)]$. Then with the help of f one can effectively compute $KM((\alpha)_n)$ to within an additive constant for all n (but generally KM is not computable). Such a sequence α is called *complete*. Thus complete sequences contain all the information about the complexity of their segments needed to compute it. The set of complete sequences is closed under computable, everywhere defined operators; any computable measure of its complement is equal to zero. The term "complete" is warranted, in particular, by the fact that any sequence can be "completed" without using any "prohibited" information; more precisely, we have

Proposition 3. *Let* β *be a sequence to which a universal recursively enumerable set is reducible, and let* α *be a sequence such that* $I(\alpha\colon \beta) < \infty$.

Then there exists a γ *such that the pair* (γ, α) *is complete and* $I((\gamma, \alpha) : \beta) < \infty$.

4. The information calculus $\mathfrak{A}$ Inf. Let $\mathcal{P}(n)$ be an absolute predicate with a single free variable n. A finite binary sequence p of length k is said to be *compatible* with $\mathcal{P}$ if, for any $n \leq k$, the nth number in p is zero if and only if $\mathcal{P}(n)$ holds (we denote this fact by writing $p \subset \mathcal{P}$). The abbreviation $I(\alpha\colon \mathcal{P})$ will be taken to mean $\sup I(\alpha\colon p)\colon p \subset \mathcal{P}$. Obviously the statement $I(\alpha\colon \mathcal{P}) \leq c$ can, for each concrete $\mathcal{P}$, be written in the form of an absolute predicate with free variables α and c.

The *principle of conservation of information* is an axiom schema ($\mathcal{P}$ is the parameter of this schema). Using the abbreviations introduced above, this principle can be written as

$$\forall\alpha\exists c \quad I(\alpha\colon \mathcal{P}) \leqslant c. \tag{4.1}$$

One more statment relative to the theory of information must be valid in $\mathfrak{A}$ Inf. We give it below as the last axiom of the theory, but we cannot prove its independence

(it may turn out that its double negation is a consequence of the preceding axioms). In §3 we defined the notion of a complete sequence. The property of "being complete" is expressible by an absolute predicate $\Pi(\alpha)$. Our last axiom demands that for sequences of our theory the completion mentioned in Proposition 3 must exist within the bounds of this theory:

$$\forall\alpha\, \exists\gamma \quad \Pi(\alpha, \gamma). \tag{4.2}$$

The double negation of this axiom follows from the weaker statement $\neg\exists\alpha\, \forall\gamma\ \neg\Pi(\alpha, \gamma)$, inasmuch as we can use the existence of a "universal" sequence by Axiom (2.3). Analogously, the double negation of the principle (4.1) follows from the statement $\neg\exists\alpha\, \forall c\ I(\alpha: \mathcal{P}) \geq c$. For our purposes it would be sufficient to limit ourselves to these weaker versions of the axioms, but we chose the formulations (4.1) and (4.2) because they are simpler.

5. **Absoluteness. Consistency and completeness relative to classical arithmetic.**

Definition. We shall say that a theory G is *absolute* if for every closed formula Φ there is an absolute (see §2) formula P such that $G \vdash \neg\neg(\Phi \rightarrow P)$.

Constructive analysis is an example of a theory known to be absolute. This is the theory obtained from $\mathfrak{A}$ by replacing (2.3) with Church's thesis (CT):

$$\forall\beta\, \exists k\, \forall n \quad \beta(n) = u(k, n), \tag{5.1}$$

where $u(k, n)$ is a universal partially recursive function. ((5.1) is obtainable from (2.3) by imposing the condition of general recursivness on α.) Our theory $\mathfrak{A}$ Inf is of course not absolute, inasmuch as the formula $\neg\neg$(CT) is not deducible in it, nor is it refutable, nor can it be reduced to any absolute formula. This formula, however, is the only one of this sort; namely we have the

Basic Lemma. *For any closed formula Φ there exist four absolute formulas P_1, P_2, P_3, P_4 such that these statements are deducible in* $\mathfrak{A}$ Inf:

$$\neg\neg(P_1 \vee P_2 \vee P_3 \vee P_4); \quad \neg\neg(P_1 \supset \Phi); \quad \neg\neg(P_2 \supset \neg\Phi);$$
$$\neg\neg(P_3 \supset (\Phi \infty (\mathrm{CT}))); \quad \neg\neg(P_4 \supset (\Phi \infty \neg(\mathrm{CT}))).$$

To get a "complete" theory it is necessary to take an axiom implying the truth or the falsity of (CT). It turns out that this is sufficient as well. The theory $\mathfrak{A}$ Inf + (CT) is equivalent to constructive analysis, and is consequently absolute. It is of little interest for our purposes, since by admitting of Church's thesis we exclude from consideration those sequences not specifiable by algorithms (for instance, the random sequences). To the degree that (CT) is a very strong axiom, the axiom $\neg$(CT) is, inversely, very weak. Thus it is unexpected, but the theory $\mathfrak{A}$ Inf+ $\neg$(CT) is also absolute. This fact follows from the Basic Lemma and is strengthened in the following theorem.

Theorem 1. *The class of absolute closed formulas deducible in* $\mathfrak{A}$ Inf + $\neg$(CT) *coincides with the class of absolute theorems of classical arithmetic (of the first*

order). No essential extension (i.e. one containing new theorems of the form $\neg\neg\Phi$) *of the theory* $\mathfrak{A}$ Inf+ $\neg$(CT) has this property.

Thus the theory $\mathfrak{A}$ Inf+ $\neg$(CT) is in a definite sense complete and has a property which can be called consistency and completeness relative to classical arithmetic. The basic goal of the construction of this theory was the study of the axiom schema (4.1). We wished to demonstrate the strength of this schema when added to a theory satisfying Theorem 1. This does not exclude the possibility of making such an addition in some other natural fashion. We chose this one by analogy with the usual axiomatic constructive analysis.

A number of discussions rendered a helpful influence on the present article: in the seminar of A. A. Markov (Corresponding Member of the Academy of Sciences of the USSR) during 1969–73, at the symposium on the foundations of mathematics at Obninsk in 1971, in A. G. Dragalin's seminar and elsewhere. The author expresses his deep gratitude to all the participants of these discussions. He is grateful to G. Gargov for bibliographical references.

Received 7/JULY/75

BIBLIOGRAPHY

1. Stephen Cole Kleene, *Mathematical logic*, Wiley, New York, 1967; Russian transl., "Mir", Moscow, 1973. MR 36 #25.

2. A. N. Kolmogorov, Problemy Peredači Informacii 1 (1965), no. 1, 3; English transl., Selected Transl. Math. Statist. and Probability, vol. 7, Amer. Math. Soc., Providence, R. I. 1968, p. 293. MR 32 #2273.

3. L. A. Levin, Problemy Peredači Informacii 10 (1974), no. 3, 30 = Problems of Information Transmission 10 (1974), 206.

4. Stephen Cole Kleene and Richard Eugene Vesley, *The foundations of intuitionistic mathematics, especially in relation to recursive functions*, North-Holland, Amsterdam, 1965. MR 31 #1190.

5. L. A. Levin, Dokl. Akad. Nauk SSSR 227 (1976), 804 = Soviet Math. Dokl. 17 (1976), 522.

6. G. Kreisel and A. S. Troelstra, Ann. Math. Logic 1 (1970), 229. MR 41 #8210.

Translated by B. F. WELLS