KYBERNETIKA — VOLUME *16* (1980), NUMBER 3

Statistical Testing Procedure for Lengths of Formalized Proofs

IVAN KRAMOSIL

A statistical testing procedure is proposed, which enables to test, given a formula of a formalized theory, whether there exists a proof of this formula the length of which does not exceed an a priori given threshold value. Such a decision rule may be of great importance when applied to automated problem solving as it prevents us from looking for solutions which are inappropriate from applicational points of view.

1. INTRODUCTION

Some recent results in the domain of automated problem solving have proved interesting connections between problem solving and theorem proving (cf. [4] or [5] for more details and further references). Roughly said, looking for a solution of a problem we may describe this problem as well as our knowledge about the environment and our tools for solving it in an appropriate formal language, then we construct a special formula of this language and try to prove it. Supposing we are successful in this effort, we may derive a solution to the problem in question from the obtained proof; here we admit also the so called branching solutions or branching plans which take into consideration simultaneously several possibilities how to solve the problem, the actually one is being chosen during the execution of the solution.

After a short consideration we must admit that not only the existence of a solution itself, but also its complexity, length, cost, etc. may play a very important role when an automated problem-solving is to be practically applied. For the sake of simplicity we shall limit ourselves to the length of the solution in question as the decisive criterion of its applicational appropriateness. Here, using the notion of length for a branching plan we mean the number of occurrences of operators in the longest branch of this plan. If we study in more details the proofs of the corresponding assertions in [4] or [5] (namely the so called Second Correspondence Theorem), we can derive, that in case a solution to the problem in question exists, its length is

majorized by the length of the corresponding proof (length of a formalized proof is taken as the number of occurrences of formulas in this proof). So we are in the following situation: if the length of proof is too great, it is very difficult to find such a proof because of the well-known fact that theorem-proving procedures are of at least exponential space and time computational complexity. However, in such a case the corresponding solution is not too desirable or adequate because it may be also very complicated, hence, expensive or difficult to apply. On the other hand, an upper bound for the length of the proof in question can serve as an upper bound for the length of the solution, hence, an information about the length of the proof would be very useful when deciding whether to look for the proof itself or whether to give up such an effort. In this paper we present a statistical testing procedure which decides, whether the length of the shortest proof of a formula exceeds a given integer value or not. This procedure is based on an appropriate statistical deducibility testing procedure and can be seen as its modification and generalization.

2. STATISTICAL TESTING PROCEDURE FOR LENGTHS OF FORMALIZED PROOFS

Let us consider a formalized language $\mathscr{L}$; the same symbol will be used for the set of all well-formed formulas of this language. Let $\mathscr{T} \subset \mathscr{L}$ be the set of all theorems, as usual, $\mathscr{T}$ is supposed to be the minimal set of formulas from $\mathscr{L}$ containing a recursive set $\mathscr{A}_0 \subset \mathscr{L}$ of axioms and closed with respect to the usual logical deduction rules corresponding to the logical type and order of the language $\mathscr{L}$. The usual logical axioms of the logical calculus corresponding to $\mathscr{L}$ are supposed to belong to $\mathscr{A}_0$. The pair $\langle \mathscr{L}, \mathscr{T} \rangle$ or the triple $\langle \mathscr{L}, \mathscr{A}_0, \mathscr{R} \rangle$ will be called a *formalized theory*; $\mathscr{R}$ is the set of deduction rules.

Axioms and deduction rules enable to define the notion of formalized proof either in the classical sense of a certain sequence of formulas termined by the desired assertion, or in the resolution-based sense of a derivation of the empty clause from axioms enriched by the negation of the desired assertion. Then we are able to define, in an appropriate way, also the notion of the length of proof; in what follows, we shall suppose that such a definition has been adopted. At the intuitive level we shall work with the classical idea of length of proof taken as the number of formulas (occurrences of formulas) in a classical proof, however, the results will hold also for the resolution-based proofs with the number of resolutions necessary for obtaining the empty clause taken as the length of proof.

Definition 1. Let $\langle \mathscr{L}, \mathscr{T} \rangle$ be a formalized theory, denote, for each $a \in \mathscr{T}$, by $\mathscr{D}(a)$ the set of all formalized proofs (in the chosen but already fixed sense), set $\mathscr{D} = \bigcup_{a \in \mathscr{T}} \mathscr{D}(a)$. Let l be a mapping from $\mathscr{D}$ into the set $\mathscr{N} = \{0, 1, 2, \ldots\}$ of naturals,

for each $d \in \mathscr{D}$ the value $l(d)$ is called *the length of the proof d*. Define, moreover, for each $a \in \mathscr{L}$ the minimal length of proof of a, denoted, again, by $l(a)$ (this should not lead to misundertandings), as follows:

$$l(a) = \inf \{l(d) : d \in \mathscr{D}(a)\} . \tag{1}$$

We adopt the usual convention according to which, for $\mathscr{D}(a) = \emptyset$, ie.., $a \in \mathscr{L} - \mathscr{T}$, we set $l(a) = \infty$.

Definition 2. Let $R \geqq 1$ be an integer, let $a \in \mathscr{L}$. The *R-neighbourhood* of a will be denoted by $\mathscr{O}(R, a)$ and defined as follows:

$$\mathscr{O}(R, a) = \{x: x \in \mathscr{L}, l(x \to a) \leqq R\} \tag{2}$$

(the dependence of $\mathscr{O}(R, a)$ on the other parameters need not be expressed explicitly).

Theorem 1. If $a \in \mathscr{L} - \mathscr{T}$, then $\bigcup_{R=1}^{\infty} \mathscr{O}(R, a) \subset \mathscr{L} - \mathscr{T}$. If $a \in \mathscr{T}$ and $l(a \to a) = 1$, then $\mathscr{O}(R, a) \cap \mathscr{T} \neq \emptyset$ for each $R \geqq 1$.

Proof. Deduction rules leads from theorems again to theorems, hence, for $a \in \in \mathscr{L} - \mathscr{T}$, $\mathscr{O}(R, a)$ may contain only non-theorems. If $a \in \mathscr{T}$ and $l(a \to a) = 1$, then $a \in \mathscr{O}(R, a)$ for each $R \geqq 1$ which proves the theorem. If $a \to a$ is an axiom and length l is taken as the number of formulas in a proof, the condition $l(a \to a) = 1$ is satisfied automatically. Q.E.D.

In what follows, the most basic notions of probability theory are supposed to be known. Let us describe a statistical deducibility testing procedure which enables to estimate, on statistical grounds, whether a formula from $\mathscr{L}$ is a theorem or not; the procedure is based on examining of the proofs of the tested formula using some at random sampled auxiliary axioms or premises.

Definition 3. Let $\langle \mathscr{L}, \mathscr{T} \rangle$ be a formalized theory, let $\langle \Omega, \mathscr{S}, P \rangle$ be a probability space. Let $a_1, a_2, \ldots, a_N$ be mutually independent and equally distributed random variables defined on $\langle \Omega, \mathscr{S}, P \rangle$, taking their values in $\mathscr{L}$ and such that for all $a \in \mathscr{L}$

$$P(\{\omega : \omega \in \Omega, \ a_1(\omega) = a\}) > 0 . \tag{3}$$

(This is possible due to the fact that the set of well-formed formulas of a formalized theory is always countable).

Let $M \leqq N$ be a natural, let $\mathscr{V} = \{\mathrm{t}, \mathrm{f}\}$, where t and f are two abstract values "true" and "false". Define, for each $a \in \mathscr{L}$, a random variable $T(a, \cdot)$ on $\langle \Omega, \mathscr{S}, P \rangle$, taking its values in $\mathscr{V}$, by setting

$$\{\omega : \omega \in \Omega, \ T(a, \omega) = \mathrm{t}\} = \{\omega : \omega \in \Omega, \ \sum_{i=1}^{N} \chi(\mathscr{O}(R, a), a_i(\omega)) \geqq M\} , \tag{4}$$

$$\{\omega : \omega \in \Omega, \ T(a, \omega) = \mathrm{f}\} = \{\omega : \omega \in \Omega, \ \sum_{i=1}^{N} \chi(\mathscr{O}(R, a), a_i(\omega)) < M\} .$$

Here $\chi(\mathcal{O}(R, a), \cdot)$ is the characteristic function (identifier) of the subset $\mathcal{O}(R, a) \subset \mathcal{L}$. The mapping $T = T(\mathcal{L}, \mathcal{A}_0, \mathcal{R}, R, M, N)$ of the Cartesian product $\mathcal{L} \times \Omega$ into $\mathcal{V}$ will be called *statistical deducibiltty testing procedure* (*in at random sampled extensions*) for the theory $\langle \mathcal{L}, \mathcal{T} \rangle$. When no misunderstanding threats we shall speak briefly about "test T".

Clearly, $\sum_{i=1}^{N} \chi(\mathcal{O}, (R, a), a_i(\omega))$ denotes the number of cases, when $a_i(\omega)$ belongs to $\mathcal{O}(R, a)$, hence, when we are able to prove a, using $a_i(\omega)$ and a proof of length at most R. If $T(a, \omega) = \mathfrak{t}$, the formula a is proclaimed to be a theorem, if $T(a, \omega) = \mathfrak{f}$, a is not proclaimed to be a theorem, hence, it is proclaimed to be a non-theorem. In both the cases such a decision is connected with a certain risk of error, some possibilities how to investigate this risk will be given below. The notion of statistical deducibility testing procedure will be used also in the case of a compound mapping $T(a(\cdot), \cdot)$ of the Cartesian product $\Omega \times \Omega$ into $\mathcal{V}$, where $a(\cdot)$ is a random variable defined on $\langle \Omega, \mathcal{S}, P \rangle$ and taking its values in the set $\mathcal{L}$ of formulas. In this case the tested formula itself results from a random sample; this fact enables to consider the qualities of the test T in a global sense, not only with respect to a particular formula.

The basic principles of the test defined above was proposed in 1959 by A. Špaček [3] and later developed (cf. surveyal work [1] on this subject). Until now, such a test has been always interpreted as a test of the potential provability, i.e., as a statistical decision procedure for answering the question whether there exists at least one proof of the tested formula no matter which its length or other qualities may be. However, because of the reasons mentioned in the introductory part the lengths of proofs play an important role in this work. Hence, let $N_0 > 0$ be an integer chosen in such a way that the proofs with lengths greater than N_0 are not acceptable or interesting for us (e.g., because of the practical impossibility to construct or apply the corresponding sequences of operators). Therefore, having a formula $a \in \mathcal{L}$, we do not want to know, whether $a \in \mathcal{T}$ or not (i.e., whether $l(a) < \infty$ or $l(a) = \infty$), but we are interested in the question, whether $l(a) \leqq N_0$ or $l(a) > N_0$. We propose to use the test T in this way:

(5)
$$\begin{aligned} &\text{if} \quad T(a, \omega) = \mathfrak{t}\,, \quad \text{proclaim, that} \quad l(a) \leqq N_0\,, \\ &\text{if} \quad T'a, \omega) = \mathfrak{f}\,, \quad \text{proclaim, that} \quad l(a) > N_0\,. \end{aligned}$$

Of course, the risk connected with this decision rule is not the same as the risk, connected with the original decision problem and can be even greater, however, we shall see that the difference is rather small, specially when N_0 increases. Said in other words, the information contained in the random event $T(a, \omega) = \mathfrak{t}$ contains also a lot of information about the value of $l(a)$ and we intend to excerpt it from the results of the test T. Our leading idea is to make the maximal profit of the rather great implementational effort and time and storage consumptions connected, at least at presence,

with the attempts to implement statistical deducibility testing procedures using a computer.

3. THE RISK CONNECTED WITH STATISTICAL DECISIONS ON THE LENGTH OF FORMALIZED PROOFS — GENERAL CONSIDERATIONS

Let us denote, for $i = 1, 2, \ldots$

$$\mathscr{T}^{(i)} = \{x: x \in \mathscr{L},\ l(x) = i\}\,, \quad \mathscr{T}^{(\infty)} = \{x: x \in \mathscr{L},\ l(x) = \infty\} = \mathscr{L} - \mathscr{T}\,. \tag{6}$$

Theorem 2. For each $a \in \mathscr{L}$,

$$\mathscr{O}(R, a) \subset \Big(\bigcup_{i=l(a)-R}^{\infty} \mathscr{T}^{(i)}\Big) \cup \mathscr{T}^{(\infty)}\,.$$

Proof. For $a \in \mathscr{L} - \mathscr{T}$ the assertion is proved in Theorem 1. Let $a \in \mathscr{T}$, let $i \leqq l(a) - R$, if there were some $x \in \mathscr{T}^{(i)} \cap \mathscr{O}(R, a)$, then a shortest proof of x, concatenated with a proof of $x \to a$ of the length at most R and terminated by a represents a proof of a the length of which is smaller than $l(a)$, hence, a contradiction. Q.E.D.

Theorem 3. Let a be a random variable defined on the probability space $\langle \Omega, \mathscr{S}, P\rangle$ and taking its values in $\mathscr{L}$, let for each $x \in \mathscr{L}$

$$P(\{\omega : \omega \in \Omega,\ a(\omega) = x\}) > 0\,. \tag{7}$$

Then, for each $x \in \mathscr{T}$ and each $R \geqq 1$, if $l(x) \to \infty$, then

$$P(\{\omega : \omega \in \Omega,\ a(\omega) \in \mathscr{O}(R, x) \cap \mathscr{T}\}) \to 0\,. \tag{8}$$

Proof. Using Theorem 2

$$P(\{\omega : \omega \in \Omega,\ a(\omega) \in \mathscr{O}(R, x) \cap \mathscr{T}\}) \leqq P\Big(\{\omega : \omega \in \Omega,\ a(\omega) \in \bigcup_{i=l(x)-R}^{\infty} \mathscr{T}^{(i)}\}\Big) =$$

$$= \sum_{i=l(x)-R}^{\infty} P(\{\omega : \omega \in \Omega,\ a(\omega) \in \mathscr{T}^{(i)}\}) \to 0\,, \quad \text{if} \quad l(x) \to \infty\,, \text{ as}$$

$$\sum_{i=1}^{\infty} P(\{\omega : \omega \in \Omega,\ a(\omega) \in \mathscr{T}^{(i)}\}) = P(\{\omega : \omega \in \Omega\,,\ \ a(\omega) \in \mathscr{T}\}) \leqq 1\,.$$

Q.E.D.

Consider a statistical deducibility testing procedure $\mathscr{T}$, let a be a fixed random variable satisfying (7). Denote

$$A_i = \{\omega : \omega \in \Omega,\ a(\omega) \in \mathscr{T}^{(i)}\}\,, \quad i = 1, 2, \ldots, \infty\,,$$

$$B = \{\omega : \omega \in \Omega,\ T(M, N, a(\omega), \omega) = \mathrm{t}\}\ .$$

Let a formula $a(0) \in \mathscr{L}$ be tested, then the probability of occurring just j formulas from $\mathscr{O}(R, a(0))$ among $a_1(\omega), a_2(\omega), \ldots, a_N(\omega)$, i.e., the probability that we will be able just j-times to prove $a(0)$ using $a_1(\omega), a_2(\omega), \ldots, a_N(\omega)$ as auxiliary hypotheses, reads:

$$\binom{N}{j} (P(\mathscr{O}(R, a(0))))^j (1 - P(\mathscr{O}(R, a(0))))^{N-j}\ , \tag{9}$$

where we denote

$$P(\mathscr{O}(R, a(0))) = P(\{\omega : \omega \in \Omega,\ a_1(\omega) \in \mathscr{O}(R, a(0))\})\ .$$

Hence, the probability that $a(0)$ will be proclaimed to be a theorem equals

$$\sum_{j=M}^{N} \binom{N}{j} (P(\mathscr{O}(R, a(0))))^j (1 - P(\mathscr{O}(R, a(0))))^{N-j}\ . \tag{10}$$

This expression can be understood also as $P(B/\{\omega : \omega \in \Omega, a(\omega) = a(0)\})$, which gives

$$P(B/A_j) = E(P(B/\{\omega : \omega \in \Omega,\ a(\omega) = a(0)\})/A_j) = \tag{11}$$

$$= \frac{\sum_{a(0) \in \mathscr{T}} \left(\sum_{j=M}^{N} \binom{N}{j} (P(\mathscr{O}(R, a(0))))^j (1 - P(\mathscr{O}(R, a(0))))^{N-j} \right) \ldots}{P(\{\omega : a(\omega) \in \mathscr{T}^{(j)}\})} \cdot$$

$$\cdot \frac{\ldots P(\{\omega : \omega \in \Omega,\ a(\omega) = a(0)\})}{P(\{\omega : a(\omega) \in \mathscr{T}^{(j)}\})}\ .$$

The well-known Bayes formulas read, in our case:

$$P(A_j/B) = P(B/A_j) \,.\, P(A_j) \,.\, [\sum_{j=1}^{\infty} P(B/A_j) \,.\, P(A_j) + P(B/A_\infty) \,.\, P(A_\infty)]^{-1}\ .$$

Above all, we are interested in the probability with which the minimal length of a proof for $a(\omega)$, sampled at random, does not exceed an a priori given N_0, i.e., we are interested in $P(\bigcup_{i=1}^{N_0} A_i/B)$. Substituting into (11) the following assertion can be immediately proved.

Theorem 4.

$$P(\{\omega : \omega \in \Omega,\ l(a(\omega)) \leqq N_0\}/\{\omega : \omega \in \Omega,\ T(M, N, a(\omega), \omega) = \mathrm{t}\}) = \tag{12}$$

$$= \frac{\sum_{j=1}^{N_0} \left(\sum_{a(0)\in\mathscr{T}(j)} \left(\sum_{j=M}^{N} \binom{N}{j} (P(\mathscr{O}(R, a(0))))^j (1 - P(\mathscr{O}(R, a(0))))^{N-j} \right) \dots \right.}{\sum_{j=1}^{*\infty} \left(\sum_{a(0)\in\mathscr{T}(j)} \left(\sum_{j=M}^{N} \binom{N}{j} (P(\mathscr{O}(R, a(0))))^j (1 - P(\mathscr{O}(R, a(0))))^{N-j} \right) \dots \right.} \cdot$$

$$\cdot \frac{\dots P(\{\omega : \omega \in \Omega,\ a(\omega) = a(0)\}))}{\dots P(\{\omega : \omega \in \Omega,\ a(\omega) = a(0)\}))} =$$

$$= \frac{E\left(\sum_{j=M}^{N} \binom{N}{j} (P(\mathscr{O}(R, a(0))))^j (1 - P(\mathscr{O}(R, a(0))))^{N-j} / \{\omega : l(a(\omega)) \leqq N_0\} \right) \dots}{E\left(\sum_{j=M}^{N} \binom{N}{j} (P(\mathscr{O}(R, a(0))))^j (1 - P(\mathscr{O}(R, a(0))))^{N-j} \right)} \cdot$$

$$\cdot \frac{\dots P(\{\omega : \omega \in \Omega,\ l(a(\omega)) \leqq N_0\})}{E\left(\sum_{j=M}^{N} \binom{N}{j} (P(\mathscr{O}(R, a(0))))^j (1 - P(\mathscr{O}(R, a(0))))^{N-j} \right)},$$

where $\sum_{j=1}^{*\infty} x_j$ denotes $(\sum_{j=1}^{\infty} x_j) + x_\infty$.

Denote by $f(N_0)$ the right side of (12), as an immediate consequence of (12) we can derive the following expression for the probability that a formula, proclaimed by T to be a theorem, actually is a theorem.

Theorem 5.

$$(13)\quad P(\{\omega : \omega \in \Omega,\ a(\omega) \in \mathscr{T}\}/\{\omega : T(M, N, a(\omega), \omega) = \mathrm{t}\}) = \lim_{N_0 \to \infty} f(N_0) = f(\infty) =$$

$$= \frac{\text{const}}{\text{const} + \sum_{a(0)\in\mathscr{L}-\mathscr{T}} \left(\sum_{j=M}^{N} \binom{N}{j} (P(\mathscr{O}(R, a(0))))^j (1\ P(\mathscr{O}(R, a(0))))^{N-j} \right) \dots} \cdot$$

$$\cdot \frac{\text{const}}{\dots P(\{\omega : \omega \in \Omega,\ a(\omega) = a(0)\})},$$

where

$$\text{const} = \sum_{j=1}^{\infty} \left(\sum_{a(0)\in\mathscr{T}(j)} \left(\sum_{j=M}^{N} \binom{N}{j} (P(\mathscr{O}(R, a(0))))^j (1 - P(\mathscr{O}(R, a(0))))^{N-j} \right) \cdot \right.$$

$$\left. \cdot P(\{\omega : \omega \in \Omega,\ a(\omega) = a(0)\}) \right).$$

4. THE RISK CONNECTED WITH STATISTICAL DECISION ON THE LENGTH OF FORMALIZED PROOFS — SPECIAL CASES

Even a simple insight into the general expressions derived above shows that these

formulas rather play the role of declarative expressions for the probability $P(\bigcup_{i=1}^{N_0} A_i/B)$, which are, however, inpracticable for its actual computation. First of all, it is caused by our ignorance of the probability distribution generated on the set $\mathscr{L}$ of formulas by the random variable a. Second, even knowing this distribution it is very difficult to compute $P(\mathscr{O}(R, a_0))$ for a given R, a_0 and it is practically impossible to express, in general, the value of this probability as an explicit function of a_0. Here we meet a problem of basic importance for every application of statistical or probabilistic methods in mathematical logic, namely, with the problem of incompatibility of formally logical and probabilistic structures on the set $\mathscr{L}$ of formulas. Intuitively said, sets of formulas which are easily definable in the logical structure, just the sets $\mathscr{O}(R, a)$, for example, can be very hardly described in probabilistic terms, it is why the values $P(\mathscr{O}(R, a))$ are hardly to compute. On the other hand, the subsets of $\mathscr{L}$ which can be easily defined in probabilistic terms, e.g., the set of all formulas which are sampled by a random variable, a or a_1, say, with the probability smaller than an a priori given $\varepsilon > 0$ can be hardly expressed as, say, the set of all logical consequences of a small and simple set of axioms. This incompatibility causes the fact that we have to be satisfied, when applying probability theory and statistics in mathematical logic, with rather rough estimations. This is also the case of this paper.

When desiring to replace the general expressions mentioned above by some more applicable ones, certain assumptions concerning the both structures on $\mathscr{L}$ seem to be inevitable. As we do not want to limit too much the generality of our results by limiting ourselves to a particular case of random variables a and a_1, we prefer to formalize our assumptions in the terms of the minimal lengths of proofs, i.e., using the variable $l(x)$. Hence, we do not suppose to have at our disposal the particular values of $P(\{\omega : a(\omega) = a(0)\})$ or $P(\mathscr{O}(R, a(0)))$, but rather their expected values for the sets of formulas with the same values of l. Denote

$$(14)\quad p_i = P(A_i) = P(\{\omega : l(a(\omega)) = i\}) = P(\{\omega : a(\omega) \in \mathscr{T}^{(i)}\}),\ i = 1, 2, \ldots, i = \infty,$$

$$\alpha = \sum_{i=1}^{\infty} p_i = P(\{\omega - a(\omega) \in \mathscr{T}\}),$$

$$e_i = P(\{\omega : a_1(\omega) \in \mathscr{O}(R, a(\omega))\}/\{\omega : a(\omega) \in \mathscr{T}^{(i)}\}).$$

The sequence $\{p_1, p_2, \ldots, p_\infty\}$ represents a probability distribution on the set $\{1, 2, \ldots\} \cup \{\infty\}$, let us consider the there following types of probability distributions.

(I) *Poisson distribution with the parameter* λ, $0 < \lambda < \infty$, i.e.

$$(15)\quad p_i = \alpha \cdot e^{-\lambda} \lambda^{i-1}((i-1)!)^{-1},\quad i = 1, 2, \ldots,$$

$$p_\infty = 1 - \alpha,$$

(in fact, it is a relativized Poisson distribution with α playing the role of the other parameter).

(II) *Geometric distribution with parameters* λ, α, $0 < \lambda < 1$, $0 \leqq \alpha \leqq 1$, i.e.,

$$(16)\quad p_i = \alpha(1-\lambda)\lambda^{i-1}, \quad i = 1, 2, \ldots,$$
$$p_\infty = 1 - \alpha.$$

(III) *Equidistribution with parameters* K, α, $K \geqq 1$ *integer*, $0 \leqq \alpha \leqq 1$, i.e.,

$$p_i = \alpha K^{-1}, \quad i = 1, 2, \ldots, K,$$
$$p_i = 0, \quad i = K+1, K+2, \ldots,$$
$$p_\infty = 1 - \alpha.$$

When applying statistical deducibility testing procedures $T(M, N)$ we limit ourselves to the two simplest cases when either $M = N$ (*case A*) or $M = 1$ (*case B*) in order to avoid computational difficulties. The connections between the cases A and B and the case of general values M, N, $M \leqq N$ have been studied and the mentioned special cases have been proved to serve as good approximations of the general ones. Combining the cases A, B with the three considered probability distributions we obtain six possibilities to be studied in details in what follows.

First of all, let us take the last simplifying assumption. We can write $\mathscr{O}(R, a) = (\mathscr{O}(R, a) \cap \mathscr{T}) \cup (\mathscr{O}(R, a) \cap (\mathscr{L} - \mathscr{T}))$. Let us suppose, that $P(\mathscr{O}(R, a) \cap (\mathscr{L} - \mathscr{T})) = c \geqq 0$ for each $a \in \mathscr{L}$ and that $P(\mathscr{O}(R, a) \cap \mathscr{T})$ decreases geometrically with $l(a)$ increasing. This assumption is satisfied, e.g., if there is a set of non-theorems enabling to prove everything, e.g., the set $C_0 = \{x: x \in \mathscr{L}, l(\text{non}x) \leqq R\}$ can play this role, as we are able to prove $x \to a$ for each $x \in C_0$, $a \in \mathscr{L}$ by proving non$x$. The assumption that $P(\mathscr{O}(R, a) \cap \mathscr{T})$ decreases agrees with Theorem 3, the geometric character of this decreasing is supposed because of its computational simplicity. This gives

$$(17)\qquad e_i = c + (1-c)c_1^{i-1}, \quad 0 < c_1 < 1, \quad i = 1, 2, \ldots$$
$$e_\infty = c = \lim_{i \to \infty} e_i.$$

Hence, $P(\mathscr{O}(R, a)) = 1$ for each axiom $a \in \mathscr{A}_0 = \mathscr{T}^{(1)}$, which agrees with an intuition. We could adopt some more complex assumptions concerning the character of e_i, e.g.,

$$e_i = c + (1 - \alpha - c)c_2^{i-1} + c_1^{i-1}, \quad 0 < c_1, c_2 < 1, \quad i = 1, 2, \ldots, \quad e_\infty = c,$$

however, we shall limit ourselves to (17), as the computations given below can be easily modified to such or similar more sophisticated cases.

Now, let us study in more details the six particular cases described above.

Case IA (*Poisson distribution*, $M = N$)

Considering the Poisson distribution with the parameter λ, denote

$$\mathscr{P}(n, \lambda) = \sum_{i=n+1}^{\infty} e^{-\lambda} \frac{\lambda^i}{i!}.$$

There exist many more or less precise approximations of these residual sums which can be found in textbooks and monographies of mathematical statistics. Here we shall not treat this matter into more details and we shall consider the expressions $\mathscr{P}(n, \lambda)$ for primitive terms. Writing, for abbreviation, $\pi(x)$ instead $P(\mathscr{C}(R, x))$ and $p(x)$ instead $P(\{\omega : \omega \in \Omega,\ a(\omega) = x\})$, and using the convexity of the function x^n, $n > 1$, $x \in \langle 0, 1\rangle$ we obtain

$$P\left(\bigcup_{j=1}^{N_0} A_j/B\right) \geqq \frac{\sum_{j=1}^{N_0} \sum_{x \in \mathscr{T}(j)} (\pi(x))^N \cdot p(x)}{\sum_{j=1}^{\infty} \sum_{x \in \mathscr{T}(j)} (\pi(x))^N \cdot p(x) + \sum_{x \in \mathscr{L} - \mathscr{T}} (\pi(x))^N p(x)}, \tag{18}$$

using (12). The sum $\sum_{j=1}^{\infty}$ can be written as $\sum_{j=1}^{N_0} + \sum_{N_0+1}^{\infty}$ the both occurrences of $\sum_{j=1}^{N_0}$ in (18) can be minimized using convexity, the other expression in (18) can be majorized, Hence, denoting by $L(j)$ the random event $\{\omega : \omega \in \Omega,\ l(a(\omega)) = j\}$, we obtain

$$P\left(\bigcup_{j=1}^{N_0} A_j/B\right) \geqq \frac{\sum_{j=1}^{N_0} E((\pi(a(\omega)))^N/L(j)) \cdot \alpha e^{-\lambda} \lambda^j (j-1)!)^{-1}}{\sum_{j=1}^{N_0} E((\pi(a(\omega)))^N/L(j)) \cdot \alpha e^{-\lambda} \lambda^j (j-1)!)^{-1} \ldots}$$

$$\frac{\sum_{j=1}^{N_0} E((\pi(a(\omega)))^N/L(j)) \cdot \alpha e^{-\lambda} \lambda^j (j-1)!)^{-1}}{\ldots + E((\pi(a(\omega)))^{N_0}/L(N_0)) \cdot \mathscr{P}(N_0, \lambda) + (1-\alpha) c^N} \geqq$$

$$\geqq \frac{\left[\sum_{j=1}^{N_0} c\alpha e^{-\lambda} \lambda^{j-1} ((j-1)!)^{-1} + \sum_{j=1}^{N_0} c\alpha e^{-\lambda} (\lambda c_1)^{j-1} ((j-1)!)^{-1}\right]^N}{\left[\sum_{j=1}^{N_0} c\alpha e^{-\lambda} \lambda^{j-1} ((j-1)!)^{-1} + \sum_{j=1}^{N_0} c\alpha e^{-\lambda} (\lambda c_1)^{j-1} ((j-1)!)^{-1}\right]^N + \ldots}$$

$$\frac{\left[\sum_{j=1}^{N_0} c\alpha e^{-\lambda} \lambda^{j-1} ((j-1)!)^{-1} + \sum_{j=1}^{N_0} c\alpha e^{-\lambda} (\lambda c_1)^{j-1} ((j-1)!)^{-1}\right]^N}{\ldots \alpha(c + (1-c) c_1^{N_0}) \cdot \mathscr{P}(N_0, \lambda) + (1-\alpha) c^N}.$$

From this inequality immediately follows

Theorem 6. Under the conditions IA

$$P(\{\omega : \omega \in \Omega,\ l(a(\omega)) \leqq N_0 / \{\omega : T(N, N, a(\omega), \omega) = t\}) \geqq \tag{19}$$

$$\geqq \frac{[c\alpha(1 - \mathscr{P}(N_0 - 1, \lambda)) + (1-c)\alpha(1 - \mathscr{P}(N_0 - 1, \lambda)) e^{-\lambda(1-c_1)}]^N}{[c\alpha(1 - \mathscr{P}(N_0 - 1, \lambda)) + (1-c)\alpha(1 - \mathscr{P}(N_0 - 1, \lambda)) e^{-\lambda(1-c_1)}]^N + \ldots}$$

$$\frac{[c\alpha(1 - \mathscr{P}(N_0 - 1, \lambda)) + (1-c)\alpha(1 - \mathscr{P}(N_0 - 1, \lambda)) e^{-\lambda(1-c_1)}]^N}{\ldots \alpha(c + (1-c) c_1^{N_0})^N \mathscr{P}(N_0, \lambda) + (1-\alpha) c^N}.$$

Theorem 7. Under the conditions IA

$$(20) \qquad P(\{\omega : \omega \in \Omega,\ a(\omega) \in \mathscr{T}\}/\{\omega : T(N, N, a(\omega), \omega) = \mathrm{t}\}) \geqq \geqq f(N) = \alpha^N(\alpha^N + (1-\alpha)\, c^N)^{-1},$$

where

$$\lim_{N\to\infty} f(N) = 1, \quad \text{if} \quad c < \alpha, \quad \lim_{N\to\infty} f(N) = 0, \quad \text{if} \quad c > \alpha,$$

$$\lim_{N\to\infty} f(N) = (2-\alpha)^{-1}, \quad \text{if} \quad c = \alpha.$$

Proof. The assertion follows by taking the limit value of (20) for $N_0 \to \infty$, as $\mathscr{P}(N_0, \lambda) \to 0$ for each λ. $f(N)$ can be expressed as $(1 + (1-\alpha)(c\alpha^{-1})^N)^{-1}$, which gives immediately the assertions concerning the limit values for $N \to \infty$. Q.E.D.

Let us introduce an illustrative example. Consider a formalized theory $\langle \mathscr{L}, \mathscr{T} \rangle$ which is complete in the sense that each formula either is a theorem or the negation of a theorem. Let the random variable a sample each formula with the same probability as its negation, let a do not sample (i.e., samples with zero probability) formulas which have the form of a multiple negation (this is equivalent to the demand of preliminary deletion of all double negations in $\mathscr{L}$). Then, clearly, $c \leqq \frac{1}{2}$, $\alpha \leqq \frac{1}{2}$, hence, even in the extremum case $c = \alpha = \frac{1}{2}$, (20) gives

$$P(\{\omega : \omega \in \Omega,\ a(\omega) \in \mathscr{T}\}/\{\omega : \omega \in \Omega,\ T(N, N, a(\omega), \omega) = \mathrm{t}\}) \geqq \tfrac{2}{3},$$

no matter which the values of the other parameters may be. Modifying the random variable in such a way that $c < \alpha$ and choosing appropriately N we can always assure an apriori given degree of reliability with which a formula proclaimed to be a theorem actually possesses the property of theoremhood.

Case IIA (Geometric distribution, $M = N$)

Theorem 8. Under the conditions IIA

$$(21) \qquad P(\{\omega : \omega \in \Omega,\ l(a(\omega)) \leqq N_0\}/\{\omega : \omega \in \Omega,\ T(N, N, a(\omega), \omega) = \mathrm{t}\}) \geqq$$

$$\geqq \frac{[c(1-\lambda^{N_0}) + (1-c)(1-(c_1\lambda)^{N_0})]^N}{[c(1-\lambda^{N_0}) + (1-c)(1-(c_1\lambda)^{N_0})]^N + (c + (1-c)\, c_1^{N_0})^N \lambda^{N_0} + (1-\alpha)\,\alpha^{-1}c^N}.$$

Proof. Similarly as in the case IA we deduce that

$$P\Big(\bigcup_{i=1}^{N_0} A_i/B\Big) \geqq$$

$$\geqq \frac{\sum_{i=1}^{N_0} (c + (1-c)\, c_1^{i-1})^N \alpha(1-\lambda)\,\lambda^{i-1}}{\sum_{i=1}^{N_0} (c + (1-c)\, c_1^{i-1})^N \alpha(1-\lambda)\,\lambda^{i-1} + (c + (1-c)\, c_1^{N_0})^N \sum_{i=N_0+1}^{N} \alpha(1-\lambda)\,\lambda^{i-1} +}$$

$$+ (1 - \alpha)\, c^N$$

and (21) can be deduced from this inequality by simple analytical calculations. Q.E.D.

Theorem 9. Under the conditions IIA

$$P(\{\omega : \omega \in \Omega,\ a(\omega) \in \mathscr{T}\}/\{\omega : \omega \in \Omega,\ T(N, N, a(\omega), (\omega) = \mathrm{t}\}) \geqq \tag{22}$$
$$\geqq (1 + (1 - \alpha)^N \,.\, \alpha^{-N})^{-1} = f(\alpha, N)\,,$$

where $\lim_{N \to \infty} f(\alpha, N) = 1$ for each α, $0 < \alpha \leqq 1$, $\lim_{\alpha \to 1} f(\alpha, N) = 1$ for each N.

Proof. (22) follows from (21) when $N_0 \to \infty$, also the assertions concerning $f(\alpha, N)$ can be deduced by corresponding limit transitions. Q.E.D.

Intuitively said, when a formula is proclaimed to be a theorem, the reliability of this decision increases if N and M increase (remember that $M = N$ in Case A) or if α, i.e., the a priori probability of sampling a theorem, increases. Both these conclusions agree with the intuitive point of view. The difference between Theorem 9 and Theorem 7 (when the limit value of the reliability did not equal, in general, one) is caused by the fact that the geometric distribution prefers theorems with shorter proofs, as in this case p_i is a descending function of i. On the other hand, in the case of the Poisson distribution with the value λ of parameter the preferred theorems are those with the lengths of proofs approximately equal λ, as λ is the mean value of the considered Poisson distribution.

Case IIIA (Equiprobable distribution, $M = N$)

Theorem 10. Under the conditions IIIA, setting $N_1 = \min(N_0, K)$,

$$P(\{\omega : \omega \in \Omega,\ l(a(\omega)) \leqq N_0\}/\{\omega : \omega \in \Omega,\ T(N, N, a(\omega), \omega) = \mathrm{t}\}) \geqq \tag{23}$$
$$\geqq \frac{\alpha[N_1 K^{-1} c + (1 - c) K^{-1}(c_1^{N_1} - 1)(c_1 - 1)^{-1}]^N}{\alpha[N_1 K^{-1} c + (1 - c) K^{-1}(c_1^{N_1} - 1)(c_1 - 1)^{-1}]^N + (c + (1 - c)\, c_1^{N_1})\, \alpha(K - N_1) K^{-1} + (1 - \alpha)\, c^N}\,.$$

Proof. Similarly as in the case IA we deduce that

(a)

$$P\Big(\bigcup_{i=1}^{N_0} A_i / B\Big) \geqq \tag{24}$$
$$\geqq \frac{\alpha[N_0 K^{-1} c + (1 - c) K^{-1}(c_1^{N_0} - 1)(c_1 - 1)^{-1}]^N}{\alpha[N_0 K^{-1} c + (1 - c) K^{-1}(c_1^{N_0} - 1)(c_1 - 1)^{-1}]^N + (c + (1 - c)\, c_1^{N_0})\, \alpha(K - N_0) K^{-1} + (1 - \alpha)\, c^N}$$

supposing that $N_0 < K$,

(25) $$P\Big(\bigcup_{i=1}^{N_0} A_i/B\Big) \geqq$$

$$\geqq \frac{\alpha[c + (1-c)K^{-1}(c_1^K - 1)(c_1 - 1)^{-1}]^N}{\alpha[c + (1-c)K^{-1}(c_1^K - 1)(c_1 - 1)^{-1}]^N + (1-\alpha)c^N} = f(K, N)$$

supposing that $N_0 \geqq K$; this expression serves also as the limit value of (24) for K fixed and $N_0 \to \infty$. Combining (24) and (25) we obtain (23). Q.E.D.

Theorem 11. Under the conditions IIIA

$$P(\{\omega : \omega \in \Omega,\ a(\omega) \in T\}/\{\omega : \omega \in \Omega,\ T(N, N, a(\omega), \omega) = \mathrm{t}\}) \geqq f(K, N)$$

(cf. (25)), where

$$\lim_{N\to\infty} f(K, N) = 1 \quad \text{for each } K\,, \quad \lim_{K\to\infty} f(K, N) = \alpha \quad \text{for each } N\,.$$

Proof. The first assertion follows immediately from the fact that $f(K,N)$ in (25) does not depend on N_0. The limit assertions for $f(K, N)$ can be derived by immediate computations. Q.E.D.

Now, we shall investigate, in a similar way, also the Case B, i.e., the case when $M = 1$. We can suppose that $N \geqq 2$, as if $N = 1$, then $M = N$ and this case is covered by Case A. Set $M = 1$ into (12) and compute; using the abbreviations introduced in Case IA:

(26) $$P\Big(\bigcup_{i=1}^{N_0} A_i/B\Big) =$$

$$= \frac{\sum_{j=1}^{N_0} \sum_{x\in\mathscr{T}(j)} [1 - (1 - \pi(x))^N] \cdot p(x)}{\sum_{j=1}^{N_0} \sum_{x\in\mathscr{T}(j)} [1 - (1 - \pi(x))^N] \cdot p(x) + \sum_{x\in\mathscr{L}-\mathscr{T}} [1 - (1 - \pi(x))^N] \cdot p(x)} \geqq$$

$$\geqq \frac{\sum_{j=1}^{N_0} (1 - (1 - c - (1-c)c_1^j)^N) \cdot P(A_j)}{\sum_{j=1}^{N_0} (1 - (1 - c - (1-c)c_j^1)^N) \cdot P(A_j) + (1-\alpha)(1 - (1-c)^N)} \geqq$$

$$\geqq \frac{P\Big(\bigcup_{j=1}^{N_0} A_j\Big)(1 - (1-c)^N)(1 - c_1^{N_0})^N}{P\Big(\bigcup_{j=1}^{N_0} A_j\Big)(1 - (1-c)^N(1 - c_1^{N_0})^N) + P\Big(\bigcup_{j=N_0+1}^{\infty} A_j\Big)(1 - (1-c)^N(1 - c_1^{N_0})^N) +} =$$

$$+ (1-\alpha)(1 - (1-c)^N) =$$

$$= \frac{P(\bigcup_{j=1}^{N_0} A_j)}{\alpha + (1-\alpha)\dfrac{1-(1-c)^N}{1-(1-c)^N(1-c_1^{N_0})^N}} .$$

This result and its particular consequences can be expressed as follows.

Theorem 12. Consider a statistical deducibility testing procedure with $M = 1$, i.e., the Case A. Then, denoting

$$p_{N_0} = P(\{\omega : \omega \in \Omega,\ l(a(\omega)) \leqq N_0\} / \{\omega : \omega \in \Omega,\ T(1, N, a(\omega), \omega) = \mathrm{t}\}) ,$$
$$p_\infty = P(\{\omega : \omega \in \Omega,\ a(\omega) \in \mathscr{T}\} / \{\omega : \omega \in \Omega,\ T(1, N, a(\omega), \omega) = \mathrm{t}\}) ,$$

the following assertions hold:

(a)

$$p_{N_0} \geqq \frac{\sum_{j=1}^{N_0} P(\{\omega : \omega \in \Omega,\ l(a(\omega)) = j\})}{\alpha + (1-\alpha)\dfrac{1-(1-c)^N}{1-(1-c)^N(1-c_1^{N_0})^N}} ,$$

(b)

$$p_\infty \geqq \alpha ,$$

(c)

$$\lim_{N\to\infty} P(\{\omega : \omega \in \Omega,\ l(a(\omega)) \leqq N_0\} / \{\omega : \omega \in \Omega,\ T(1, N, a(\omega), \omega) = \mathrm{t}\}) \geqq \alpha ,$$

(d) setting

$$K_1(N, N_0) = \alpha + (1-\alpha)\frac{1-(1-c)^N}{1-(1-c)^N(1-c_1^{N_0})^N} ,$$

and considering the Case I (i.e., Poisson distribution), then

$$p_{N_0} \geqq (K_1(N, N_0))^{-1}\, \alpha \mathscr{P}(N_0 - 1, \lambda) ,$$

(e) considering the Case II (i.e., geometric distribution), then

$$p_{N_0} \geqq (K_1(N, N_0))^{-1}\, \alpha(1-\lambda_{N_0}) ,\quad \lim_{N\to\infty} p_{N_0}(N) = \alpha(1-\lambda_{N_0}) ,$$

(f) considering the Case III (i.e., equiprobable distribution), then

$$p_{N_0} \geqq (K_1(N, N_0))^{-1} \,.\, \alpha \,.\, K^{-1} \,.\, \min(N_0, K) ,$$

where $K = \max\{i : p(A_i) > 0\}$ is the parameter of the equiprobable distribution.

Proof. Assertion (a) is nothing else than (26), (b) and (c) follow from (a) by taking

the corresponding limit values. Assertions (d), (e) and (f) follow also immediately from (a) when substituting the values for the corresponding probability distributions. Q.E.D.

5. CONCLUSIVE REMARKS

The closing section of this paper offers a possibility to mention another point of view from which a statistical testing or estimation of lengths of formalized proofs may be seen as a rather important matter. When considering the class of deduction rules which generate, starting from axioms, the set of all theorems, we have always supposed that this class contains usual deduction rules of predicate logic and, perhaps, some more rules consistent with those former ones. All our statistical reasoning, estimations, etc., which depend on the adopted deduction rules by the mean of sets $\mathcal{O}(R, a)$, can be, however, repeated also in case we admit also inconsistent deduction rules, i.e., rules which can lead also from true premises to false conclusions. E.g., the statistical induction, which implies from the validity of a finite number of instances of a formula, its general validity can be seen, after an appropriate formalization, as such a rule, also a statistical deducibility testing procedure itself can be seen in such a way. A slightly different intuitive background for such deduction rules offers the fuzzy logic [2].

In every such case the reliability of a proof operating with such not quite reliable deduction rules decreases when the number of applications of such rules increases. On the other hand, such deduction rules can be very "powerful" in the sense that they offer short proofs of formulas, which are provable also without these rules, but only using very long and inpracticable proofs. In such cases, hence, any information about the length of a proof contains also a lot of information about the validity of the conclusions of the proof in question. In other words said, a statistical estimation of the length of a proof is, under such conditions, nothing else than a statistical deducibility testing procedure which tests the derivability of the conclusions of the tested proof using only the usual, reliable deduction rules. Hence, the qualitative difference between the cases $N_0 < \infty$ and $N_0 = \infty$ disappears. It seems to be very interesting and desirable to investigate various statistical deducibility testing procedures also from this point of view which touches the very deep logical and philosophical foundations of mathematics and which proves itself to be very close to some basic ideas of the so called alternative set theory.

(Received August 20, 1979.)

REFERENCES

[1] I. Kramosil: Statistical Approach to Proof Theory. Supplement to Kybernetika, *15* (1979).
[2] J. Pavelka: On Fuzzy Logic I, II, III. To appear in Zeitschrift für Mathematische Logik und Grundlagen der Mathematik.

[3] A. Špaček: Statistical Estimation of Provability in Boolean Logics. In: Transactions of the Second Prague Conference on Information Theory..., NČSAV (Publishing House of the Czechoslovak Academy of Sciences), Prague 1960.

[4] O. Štěpánková, I. M. Havel: A Logical Theory of Robot Problem Solving. Artificial Intelligence *7* (1976), 129—161.

[5] O. Štěpánková, I. M. Havel: Incidental and State-Dependent Phenomena in Robot Problem Solving. Kybernetika *13* (1977), 6, 421—438.

Dr. Ivan Kramosil, CSc., Ústav teorie informace a automatizace ČSAV (Institute of Information Theory and Automation — Czechoslovak Academy of Sciences), Pod vodárenskou věží 4, 182 08 Praha 8. Czechoslovakia.