Siberian Advances in Mathematics
1991, v.1, N4, 92-121

ON EQUIVALENCE BETWEEN POLYNOMIAL CONSTRUCTIVITY OF MARKOV'S PRINCIPLE AND P=NP

V.Yu.Sazonov

Abstract

The theory of polynomial computability, in the form of a weak "nonexponential" intuitionistic arithmetics of binary words with formal Church's thesis and Markov's principle, is considered. Unlike the Heyting arithmetics with these principles, its constructivity occurs to be equivalent to P=NP and the statement of exponential complexity of NP-complete problems is not derivable. In addition it is demonstrated that even in the nonexponential arithmetics one can develop a partial recursive function theory along with Kleene's realizability theory. Moreover, here it is possible to distinguish between constructive and non-constructive finite objects.

Key words and phrases: polynomial computability, provable recursive function, exhaustive search problem.

This article is a complete and detailed version of [1], which develops [2,3]. Its main and basic result can be formulated even in the next seemingly doubtful but correct after appropriate stipulations form: constructivity of the Markov principle is equivalent to the equality P = NP. Recall that « P = NP ? » is a known problem of the complexity theory [4] concerning coincidence of the classes P and NP of predicates which are computable respectively on deterministic and nondeterministic Turing machines in polynomial time. (*Remark*: It is assumed that a non-deterministic (and particularly deterministic) Turing machine computes a predicate $Q(x)$ in polynomial time $p(n)$ if for any input x of the length n, $Q(x)$ is equivalent to the existence of a calculation path of the length $p(n)$ on which one can obtain the result "Yes".)

Since Markov's principle

$$M: \neg\neg\exists x\alpha \supset \exists x\alpha,$$

for a decidable formula α is known as a legitimate principle of the so called "Russian constructivism", it seems that the statement mentioned implies the solution of the « P = NP ? » problem and, moreover, in an unexpected form of equi~~valen~~alityce. However, we shall see that this result, probably, grounds non-constructivity of the Markov principle in the case when the potential feasibility abstraction generally accepted in constructive and also in classic mathematics is declined. As to the P ≠ NP hypothesis, here we only establish non-provability in a certain weak (in comparison with classical and constructive arithmetics) theory of the exponential complexity of NP-complete problems which is close to this hypothesis (compare with [2, 3]). This is the second basic result of this paper.

If the reader prefers an orderly and formal exposition then he will go directly to §2.

Translated from PRIM, 1989, v.12, 139-165

The author is very grateful to N.V.Belyakin and D.E.Pal'chunov for a number of useful remarks on the text.

§1. PRELIMINARY EXAMINATIONS. MOTIVATIONS AND STATEMENT OF RESULTS

We will consider the certain constructivity principle laid down only with respect to some formal theory in the frame of which the principle is formulated. Such theory usually appears to be, at least, the Heyting arithmetics HA containing the complete mathematical induction scheme (like the classic arithmetics PA) . We will be interested in theories with a sufficiently weak form of induction so that the realizability of exponential is not provable in such theories; i.e., one cannot derive that a standard Turing machine computing the exponential 2^n stops after a finitely many steps on any input n. So we can add an axiom that for some natural number n this Turing machine never stops (taking into account the computational practice and generally accepted negative attitude to exponential complexity, that is quite appropriate). In other respects these *nonexponential* theories lose not very much in comparison with some traditional systems like PA or HA and they are suitable for questions from discrete mathematics. For example, in them one may successfully develop the Turing machine theory and the partial recursive function theory PRF, prove the universal PRF theorem, consider the Kleene realizability theory, etc. One of the goals of this paper is to demonstrate the mentioned possibility.

Recently the interest to weak theories, the fragments of Peano arithmetics, etc., has grown up (see for example [5, 6]). We do not intend here to present a survey or a list of papers on the topic complete in any sense . We only explain that the approach suggested here as well as in [1-3, 7-9] is related to comprehension of a special role of the notion and theory of polynomial computability (PC) from the stand of mathematical foundations.

The starting instance here is the following variant PA$_{\Box}$ of the usual Peano arithmetics PA. First, let us change the axioms of PA concerning the successor operation so that for some natural number $\Box$, $\Box + 1 = \Box$ holds and this number $\Box$ will be the last number in the natural row $0, 1, 2, \ldots, \Box - 1, \Box$, described by this formal theory. There is no information on the concrete value of the number $\Box$ in these axioms. So any finite segment of the usual "standard" natural numbers (or even a non-standard finite segment) can be a model of this theory. In particular, one cannot prove here $3 \neq 5$. Second step is that we postulate that all possible recursive (and of course all primitive recursive) functions in the finite natural row $0, 1, \ldots, \Box$ are in the form of equalities $\vec{f} = \vec{T}(\vec{f})$, where $\vec{f}$s are the functions defined and $\vec{T}$s are arbitrary terms constructed from $\vec{f}$s and given operations $0, x+1, =,$ IF-THEN-ELSE. Third, we postulate , like in PA, the induction scheme, in which the recursive functions defined can participate. Note that, unlike the usual infinite natural row arithmetics PA, we had to add the recursive functions explicitly. (One can introduce functional and predicate parameters into the language PA$_{\Box}$, passing to the more general notion of relatively-recursive functions or, more exactly, recursive operators and functionals in the finite natural row.)

We may consider the theory obtained, PA$_{\Box}$, as the *polynomial computability theory*, since in [7,10] it was shown that (relatively) recursive functions in the finite row $0, 1, \ldots, \Box$ with the changeable upper bound $\Box$ are exactly all the functions on this natural row that are computable on a Turing machine (with respect to functional parameters) in polynomial time of the value $\Box$.(In [10] it was also proved that the primitive recursion (unlike the general recursion meant above) in the finite natural row corresponds to the computability notion with the logarithmic memory. Note that Mostowsky seems to be the first to consider the primitive recursion in the finite natural row [11]. Analogous results were obtained in [12-14] in connection with the relational data base theory.)

The essence of this characterization of polynomial computability is that the theory $PA_{\square}$, corresponding to it, thanks to the finiteness of the natural row that it describes, does not use the potential feasibility abstraction (i.e. the abstraction from the resource bounds existence itself). As a matter of a fact, this well founds the relation of the polynomial computability to the foundations of mathematics (see also [2, 7-9], where analogy of the Church thesis for polynomial computability is formulated in detail).

One can also examine an analogous variant $PA^2_{\square}$ of the second-order arithmetics with quantifiers on functional and predicate variables. (In [2, p.573] similar arithmetics was described as UBA.) Because of the known result [15] on the Σ^1_1-representation of the class $NP \supseteq P$ in finite ordered models, it is not necessary to consider all recursive functions in the finite natural row as initial.

Note that such parametric finiteness of the natural row is not an obstacle for development on its basis a discrete mathematics and, moreover, even some nonstandard variant of the infinitesimal analysis. The latter, for example, is convincingly demonstrated in [16].

Unlike the usual arithmetics, the first order quantifiers in the finite natural row do not lead to the effects similar to arithmetical undecidability. So, there is no sense to consider an intuitionistic variant $HA_{\square}$ of the arithmetics $PA_{\square}$. Things are not completely like this with the second order quantifiers which may lead out of the polynomial computability (i.e., recursively in the finite natural row). By force of mentioned Σ^1_1-representation of the class NP, this sentence is equivalent to the hypothesis $P \neq NP$. It is even intuitively clear, that a quantifier over unary predicates on $0, 1, \ldots, \square$ leads to the exhaustive search of the very large exponential number $2^{\square+1}$ of such predicates. Thus, it makes sense to pass to a constructive variant $HA^2_{\square}$ of the theory $PA^2_{\square}$ so if, for example, a formula $\forall P \exists Q \varphi(P, Q)$ is derivable, then the predicate Q is recursive relatively to P and therefore it is computable with respect to P in a polynomial, rather than exponential time.

Note that constructivity of the appropriate variant of the Markov principle $\neg\neg \exists P \varphi(P) \supset \exists P \varphi(P)$, where φ is a (polynomially decidable) first order formula in the finite natural row, is doubtful, because its usual constructive explanation or "realisation" turns into complete exponential exhaustive search of all predicates P until we find the predicate needed. So it is not so surprising that constructivity of such Markov principle may turn out to be equivalent to $P = NP$.

By the way, a fundamental question arises here: what should be the order of the exhaustive search through predicates P to realize such Markov principle? Is there another reasonable order different from lexicographic one? It turns out that among all the methods there is a *polynomially optimal* exhaustive searching method (see §4 and[2]), and it will play an essential role in the further construction.

However, this optimal exhaustive searching method is defined in terms of the binary words $\{0, 1\}^*$ having arbitrary length rather than in terms of the finite natural row. Just the same one can say about the Kleene realizability notion [17, 18] which we intend to use in studying the constructivity of the Markov principle and polynomial computability theory. So we consider these questions in a more traditional way (formally different but essentially similar) based on the (potentially) infinite set of binary words. (In the case of $\mathrm{HA}^2_{\Box}$ the Gödel interpretation [19] of finite functionals of the finite type over finite natural row or FORMULAE-AS-TYPES [20] technique application should be natural.)

So, consider the *quantifier-free theory T_0 of polynomial computability* over the set $\{0,1\}^*$ of all finite binary words. More exactly, let T_0 be the set of (for convenience all) true quantifier-free formulae constructed of polynomial computable functions PCF and predicates over the set $\{0,1\}^*$ plus the classic first order logic. By analogy, let T be (all) true in $\{0,1\}^*$ formulae in this language with *bounded quantifiers* $\forall x < t$, $\exists x < t$, where $<$ is the (polynomially computable) lexicographic linear order on $\{0,1\}^*$.

It is clear that such bounded quantifiers play a role of the second order quantifiers in the finite natural row so far as a restriction of the binary word length being accepted as a finite predicate, is essential here. If we require a variable x to run over unary words in $\{1\}^*$, then they will correspond to the first order quantifiers of the arithmetics $\mathrm{PA}_{\Box}$. It is easy to understand that such unary bounded quantifiers, unlike the bounded quantifiers $\forall x < t$, and $\exists x < t$, over binary words, are expressible in T_0 by quantifier-free formulae, since they maintain a polynomial computability.

Finally, denote intuitionistic variant of the theory T_0 by HT_0 (i.e., $\mathrm{HT}_0 =$ non-logical axioms of $\mathrm{T}_0 +$ intuitionistic logic). Note that only non-logical axioms of the theories T_0 and HT_0 are quantifier-free formulae. Unbounded quantifiers usage over the whole infinite universe of binary words is allowed in proofs and formulations.

As we shall see later on, it is possible to define the notion of a partial recursive function PRF and the Kleene notation $\{e\}(x)$ for the result of application of the algorithm e to the binary word x in these theories. Note that here the exponential is a PRF and its totality is not provable in T. Moreover, in $\mathrm{HT}_0, \mathrm{T}_0$ and T the class of *provable recursive functions (i.e. such* $\overset{\text{PRF}}{\textit{functions}}$ *that can be proved to be total) is exactly the class of functions computable in polynomial time.*

The *Kleene-Church Thesis* ECT (ECT_U) is, as usual, the axiom scheme

$$\forall x\, (\psi(x) \supset \exists y\, \varphi(x,y)) \supset \exists e\, \forall x\, (\psi(x) \supset !\, \{e\}(x) \wedge \varphi(x, \{e\}(x))),$$

where (to avoid a contradiction) the connectives $\vee$ and $\exists$ in ψ apply only to quantifier-free subformulae (in the case ECT_U quantifiers $\exists$ in ψ are of the form $\exists v \in \{1\}^*$).

Define now *two variants of the Markov principle*

$$\mathrm{M}: \neg\neg \exists x\, \alpha(x) \supset \exists x\, \alpha(x),$$

$$\mathrm{M}_U: \neg\neg \exists x \in \{1\}^* \alpha(x) \supset \exists x \in \{1\}^* \alpha(x),$$

where α is an arbitrary quantifier-free formula.

A formal theory is said to be *constructive* if for an arbitrary sentence of the kind

$$\forall \overline{x}\, (\chi(\overline{x}) \supset \exists y\, \varphi(\overline{x}, y)),$$

where χ is a *U*-Harrop formula (see the beginning of Section 3) its derivability implies that of the sentence

$$\forall \bar{x}\,(\chi(\bar{x}) \supset\, !t\,(\bar{x}) \wedge \varphi\,(\bar{x}\,, t\,(\bar{x})))$$

for some partial recursive term $t\,(\bar{x})$. The theory is said to be $\exists$-constructive if the previous is valid without χ or when $\chi \equiv$ TRUE. If, moreover, $t\,(\bar{x})$ is the PCF; then the theory is said to be $\exists$-constructive.

Now we can formulate the basic results of the article:

1. *The theories* $\mathrm{HT}_0, \mathrm{HT}_0 + \mathrm{M}_U, \mathrm{HT}_0 + \mathrm{ECT}_U, \mathrm{HT}_0 + \mathrm{ECT}_U + \mathrm{M}_U$ *are constructive and, moreover, polynomially* $\exists$*-constructive* (see 7.4(b) and 6.5(b)).

2. *The theory* $\mathrm{HT}_0 + \mathrm{ECT}_U + \mathrm{M}\ (= \mathrm{HT}_0 + \mathrm{ECT} + \mathrm{M}_U = \mathrm{HT}_0 + \mathrm{ECT} + \mathrm{M})$ *is (polynomially* $\exists$*)-constructive if and only if* $\mathrm{P} = \mathrm{NP}$. *The same is true also for the theory* $\mathrm{HT}_0 + \mathrm{ECT}$ (see 6.7).

3. *The theory* $\mathrm{HT}_0 + \mathrm{ECT} + \mathrm{M}$ *is a conservative extension of* T_0 *and* HT_0 *with respect to* Π_2*-sentences. In particular, the class of all its provable-recursive functions is exactly* PCF, *and realizability of exponential is not provable in it (see 6.7)).*

4. $\mathrm{HT}_0 + \mathrm{ECT} \vdash \exists e\, \mathrm{SA}\,(e)$, *where* $\mathrm{SA}\,(e) =$ « *e is a deterministic algorithm for searching a satisfying tuple for satisfable propositional formulae* » (see 2.1(a))

5. *In particular by the sentences* 3 *and* 4 *it follows that all nonmonotonic superpolynomial upper bounds for a search time of such search algorithms* (see 6.8) *are not provable in the theory* $\mathrm{HT}_0 + \mathrm{ECT} + \mathrm{M}$ *(and also in* T_0 [2]).

6. *The following theories are constructive*:

$$\mathrm{HT}_0 + \mathrm{SA}\,(e)\,,\quad \mathrm{HT}_0 + \mathrm{SA}\,(e) + \mathrm{M} = \mathrm{HT}_0 + \mathrm{SA}\,(e) + \mathrm{M}_U\,,$$

$$\mathrm{HT}_0 + \mathrm{SA}\,(e) + \mathrm{ECT} = \mathrm{HT}_0 + \mathrm{SA}\,(e) + \mathrm{ECT}_U\,,$$

$$\mathrm{HT}_0 + \acute{\mathrm{SA}}\,(e) + \mathrm{ECT} + \mathrm{M}\,,$$

where e is a new constant which denotes some certain (unknown) search algorithm (see 7.4 (a) and 6.5 (a)). *However after replacing* $\mathrm{SA}\,(e)$ *by* $\exists\, e\, \mathrm{SA}\,(e)$ *in all these theories, constructivity of each of them is equivalent to* $\mathrm{P} = \mathrm{NP}$(see (3.2)).

7. *The theory* $\mathrm{HT}_0 + \mathrm{M}$ *is polynomially* $\exists$*-constructive* (see 7.6).

8. *Constructivity (without* « $\exists$ » !) *of the theory* $\mathrm{HT}_0 + \mathrm{M}$ *is equivalent to the equality* $\mathrm{P} = \mathrm{NP}$ (see 7.5).

Thus, we see that only "unary" variants ECT_U and M_U of the Church thesis and the Markov principle can be considered as constructive (and even polynomially $\exists$-constructive) in our framework without any reserve. To prove constructivity of ECT and M, the statement P = NP which appears to be equivalent to constructivity of ECT and M, or the hypothetical search algorithm (compare with the notes in the end of §13), or the exponential feasibility axiom, which obviously guarantees existence of such search algorithm, is to be involved.

Subjectively ECT_U differs from ECT by a rather technical but important refinement, and it is difficult to connect a certain concrete sense with it right away. The role of this refinement one can make more precise in the process of the proof. The difference between M_U and M from our point of view is rather principal and intuitively justified: in the first case we mean the unary words exhaustive search and in the second - the binary words exhaustive search (in some order that is not specified in the Markov principle).

In the proof of most results mentioned, the usual Kleene realizability notion adapted to nonexponential theories is essential. To make all the springs visible we have to give an account of the well-known theory (following, basically, [17, 18]).There are too many items to refer, so we restrict ourselves to a general reference. It is connected with a number of details that are lumped together by the traditional view of the exponential as a feasible arithmetic operation. For example, one can speak strictly enough about such notions as *long, short, constructive,* and *non-constructive* binary words, though these notions seem to be non-formalizable. (See §4 and §1 of Appendix about connections with the Kolmogorov complexity.)

Note that not in every nonexponential theory (based on HT_0 or T_0) the result on non provability of the lower exponential bound for the time of work of a search algorithm (like in the p.5) can be obtained (compare with [21]), though nonexponentiality plays an essential role here (see also a discussion on independency for « P = NP ? ». [2]). The examples are T (see correction to [2] in [3, p.490]), $T_0 + \Delta-$Coll (see 2.3, 2.4 and 4.7 and also [2]), HT_0 + ECT + M + bounded induction (see § of Appendix). Finally ~~not is~~ for ~~a single~~ none of the theories considered ~~there can be~~ we are able to prove~~d~~ the more strong result on non provability of the lower exponential bound for deterministic algorithms that recognize certain NP-complete set.

Thus, for weak non-exponential theories proving independency of problems, which are close to « P = NP ? », becomes a slightly easier task, and "slightly" means that the concrete sense remains actually the same in the context of the theories involved.

However, it may seem that if, nevertheless, these problems are resolvable (in ZF ?) then, by limiting mathematics to its non-exponential scope, one misses the goal, since resolvability may be lost. But reasoning in such a way against the limitation of the traditional mathematics, one may finally postulate (ad hoc) as strong principles as possible; for example large cardinals axiom, the continuum hypothesis (or, may be, its negation?); determinacy axiom, etc. Most probably, in the case considered these axioms, as well as the exponential feasibility axiom, do not concern the matter. So we prefer not to introduce them without special need. Note that the limitation of the theory leads to an extension of the class of its interpretations and that of the notions that are comprehensible within it.

We see now that the non-exponential approach proposed here is based on reconsidering such basic mathematic notions as natural numbers and binary words. It also can be characterized as a look at the complexity theory through the prism given by foundations of mathematics. In connection with this the following analogy between the « P = NP ? » problem and the continuum hypothesis seems to be useful: in the former case binary words and bounded quantifiers over them are considered, and in the latter- infinite binary words, and it appears that in both cases the notion of the constructive binary word plays an important role. As also for the continuum of infinite binary words we can, for example, pose the following non-formal questions: To what extent the practically infinite set of binary words, which have the length equal, say, to one thousand, is definite? Can we mean its arbitrary element to be the result of a random coin toss? How to formulate this mathematically? Recall that the solution of the continuum problem given by K.Gödel and P.Cohen consists in the search for reasonable answers to such questions in the infinite case. This comprehension of complexity of the finite objects structure in the terms of foundations of mathematics (not just in those of the algorithm theory) could probably result in a solution of the « P = NP ? » problem (as well as other complexity theory problems).

§2. POLYNOMIAL COMPLEXITY THEORY AND PARTIAL RECURSIVE FUNCTIONS

Denote the set of all binary words by $\{0,1\}^*$. Unary words $\{1\}^* \subseteq \{0,1\}^*$ are identified with natural numbers. Let $p_1, p_2, \ldots$ be all functions and predicates over $\{0,1\}^*$ which are computable (on a deterministic Turing machine) in the polynomial time of length of an argument. List some of them:

$x = y$ the equality of binary words;

$\varnothing$ - the empty word (0-ary function);

$\sigma_0(x)$, $\sigma_1(x)$ - operations, adjoining 0 and 1 to the word;

$\mathrm{Un}(x)$ — «x is a unary word »;

$|x|$, $|x|^2$ - the length and the length squared of the word x (thus, we have $\mathrm{Un}(|x|)$ and $\mathrm{Un}(|x|^2)$)

xy (or $x+y$-concatenation);

$x^{|y|}$ the word x repeated $|y|$ times,

x', $x \leq y$ the lexicographic successor function and order ($\varnothing < 0 < 1 < 00 < 01 < < 10 < 11 < \ldots$),

$B(i) = B_i$ — i-th binary word in the lexicographic ordering,

$\hat{x}$ the result of replacing of each occurrence of the symbol $\delta \in \{0,1\}$ in the word x for $\delta\delta$,

$<x,y> \rightleftharpoons \hat{x}01y$ and $«i,j» \rightleftharpoons B^{-1}(<B_i, B_j>)$ - the binary and unary coding of pairs of binary and unary words respectively (having polynomially computable projections),

$\exp(x,y)$- the predicate $2^{|x|} < |y|$,

$x[y]$ - the statement about truth of the "propositional formula" (coded by the word) x on the "argument" y,

$H(e,n)$ - "the algorithm, more exactly, the *initial Turing machine* e stops after $\leq |n|$ steps" (here we consider e as a pair $e = <u,v>$, where u is a binary code of the usual Turing machine and v is a binary word written on its tape),

$M(e,n)$ - the result of the algorithm e (i.e., contents of the output tape) at $|n|$-th step (we mean that a certain binary word in the alphabet $\{0,1\}$ to be written on the output tape of the Turing machine at any step),

$e * x$ - an algorithm e along with additional initial information x (formally, for $e = <u,v>$ we put $<u,v> * x \rightleftharpoons <u, <v,x>>$).

Note that any PCF $f(x)$ is termally expressible only over operations $\varnothing$, σ_0, σ_1, $|\cdot|^2$, M and $*$; more exactly, as $f(x) = M(e * x, |x|^k + c)$, where terms e and c are constructed from $\varnothing$, σ_0 and σ_1; k-th degree $|x|^k$ - from x and $|\cdot|^2$ (for k of the kind 2^m).

Let P be a model $<\{0,1\}^*; p_1, p_2, \ldots>$ of the signature $p_1, p_2, \ldots$ and T_0 be the set of all quantifier-free formulae of this signature true in P. Analogously let T_0 be the set of allformulae true in P (possibly, with free variables) with bounded quantifiers $\forall x < t$, $\exists x < t$, where a (signature) term t does not contain the variable x.

Of course, instead of (classical) theories T_0 and T, it would be more natural to consider some of their subtheories defined by a finite set of axiom schemes with a finite number of symbols for polynomially computable functions and predicates p_k. But to the rest of the presentation it bears no serious importance. Denote by HT_0 an intuitionistic variant of the theory T_0, i.e. non logical axioms of T_0 noted above + the intuitionistic logic (with equality). Unlike the intuitionistic aruthmetics HA, the theory HT_0 does not contain (explicitly) a (lexicographic) induction axiom

$$\varphi(\varnothing) \wedge \forall x < y\,(\varphi(x) \supset \varphi(x')) \supset \varphi(y).$$

Here we are interested only in rather weak versions of the induction axiom, more exactly, in *the quantifier-free induction* (φ has no quantifiers) and *the bounded induction* (φ has only bounded quantifiers $\forall x < t$, $\exists x < t$, where x does not occurs in the term t.) Obviously, the bounded induction is simply contained in the theory T as an axiom scheme.

By analogy, the following is true for HT_0:

Proposition 2.1 (cf. [2; 3, p.490]).

(a) *The quantifier-free lexicographical induction is provable in* HT_0.

(b) *The quantifier-free and lexicographical induction schemata are equivalent in an appropriate finite fragment of the theory* HT_0 *to quantifer-free and bounded linear induction axioms*:

$$\varphi(\varnothing) \wedge \forall x\,(\varphi(|x|) \supset \varphi(|\sigma_1(x)|)) \supset \forall x\,\varphi(|x|),$$

where the formula φ *is quantifier-free or bounded respectively.*

Proof. (a) Using polynomial computability of the predicate $\varphi(x)$, one can compute in a polynomial time by the dichotomy method a certain value $x = f(y) < y$ such that the following formula

$$[\varphi(\varnothing) \wedge \neg\varphi(y) \supset \varphi(f(y)) \wedge \neg\varphi((f(y))')] \wedge [f(y) < y]$$

is true in the model P.

The induction axiom on the formula φ follows from this and the next quantifier-free formulae $\neg\neg\varphi(y) \supset \varphi(y)$, which are axioms of the theory HT_0.

See the proof of (b) in 8, p.2.

We point out another (equivalent) variant of the linear induction:

$$\varphi(\varnothing) \wedge \forall x\,(\varphi(x) \supset \varphi(x0) \wedge \varphi(x1)) \supset \forall x\,\varphi(x).$$

Unsolved questions. 1. *Is the bounded induction provable in* T_0? Note that the negative answer (which seems to be more likely) would imply $P \neq NP$.

2. *Is the lexicographically least word principle for quantifier-free* φ

$$\varphi(x) \supset \exists y \le x\,(\varphi(y) \wedge \forall z < y\,\neg\varphi(z))$$

provable in T_0?

The answer also seems to be negative.

Finally note that the class of quantifier-free formulae φ's is closed with respect to bounded unary quantifiers. We mean that, for example, a formula of the kind $\exists x \le t\,(\mathrm{Un}(x) \wedge \varphi(x))$, where φ is quantifier-free, is equivalent in HT_0 to the quantifier-free formula $\varphi(\mu x \le t\,(\mathrm{Un}(x) \wedge \varphi(x)))$, where $\mu x \le t\,(\mathrm{Un}(x) \wedge \varphi(x))$ denotes PCF. The latter yields the least unary word which satisfies $x \le t \wedge \varphi(x)$, if this word exists, and the maximal unary $x \le t$ otherwise.

The following two propositions demonstrate adequacy of the theories T_0 and T with respect to polynomial computability.

Proposition 2.2. *If* $\mathrm{T}_0 \vdash \exists y \varphi(\bar{x}, y)$ *for a quantifier-free formula* φ *then* $\mathrm{HT}_0 \vdash \varphi(\bar{x}, t(\bar{x}))$ *for some signature (and, hence, polynomially computable) term* t. *Particularly the same* Σ_1*-formulae* (Π_2*-sentences) are provable in the theories* T_0 *and* HT_0; *and also provable that total* PRF *are exactly* PCF.

Proof. By the Herbrand Theorem we have $\mathrm{T}_0 \vdash \bigvee_{i=1}^{k} \varphi(\bar{x}, t_i(\bar{x}))$, and it implies that $\mathrm{T}_0 \vdash \varphi(\bar{x}, t(\bar{x}))$ is valid for some terms $t_1, \ldots, t_k, t$. Since the "tertium non datur" principle is provable in T_0 for quantifier-free formulae, the last proof may be transformed into an intuitionistic one. (An even simpler way of proof is as follows: since a quantifier-free formula $\varphi(\bar{x}, t(\bar{x}))$ is true in P, it is actually an axiom of HT_0).

Proposition 2.3 [2, p.573]. *If a formula* $\exists y \varphi(\bar{x}, y)$ *is provable in the theory* T, *possibly using the principle*

$$\Delta\text{-Coll}: \forall x < a \, \exists y \psi \supset \exists b \, \forall x < a \, \exists y < b \, \psi,$$

where φ *and* ψ *do contain only bounded quantifiers, then for some signature term* t *the formula* $\exists y < t(\bar{x}) \, \varphi(\bar{x}, y)$ *is provable in* T *(without* Δ*–Coll).*

Proof for ~~the~~ most general case is worked out in [21].

An analogous result, but without Δ–Coll, was obtained in [23].

Denote the sentence $\forall x \exists y \exp((x, y)$ expressing feasibility of exponential by EXP. Note that in HT_0 EXP is equivalent to the sentence about standard binary words coding by unary words feasibility: $\forall x \exists i \in \mathrm{Un}\,(x = B_i)$. Because of following Corollary 2.4 of Proposition 2.4, both are unfeasible in these theories (compare with 4.7).

Corollary 2.4. *The statements* EXP *and* $\forall x \exists i \, (x = B_i)$ *are not provable in the theory* $T + \Delta$–Coll.

This corollary does in no way witness the defectivity of the theories T_0 and T, though one could have made such a conclusion, taking into account that not all the "truths", like EXP, are provable in these theories. First, it is far from being clear what the mathematical "truths" are. Second, the statement EXP seems to be "false", rather than otherwise. However, we are not going to postulate $\neg$ EXP as a new axiom.

By virtue of Corollary 2.4, it is natural to name "*short*" the binary words x of the kind B_i, i.e., such words that $\exists y \exp(x, y)$, ("*short*" in the frame of the theory T_0, or HT_0, T, etc; but not in the model P, where EXP is true, and hence, $\forall x \exists i \, (x = B_i)$). And also it is consistent to suppose that these are not all the possible words. If the words x and y are short; then their concatenation xy is obviously a short word , but $|x|^2$ may happen to be not short.

It is reasonable to name *small* or *feasible* the natural numbers having a short unary representation. (The first mathematically rigorous and sufficiently satisfactory formalization of the feasible natural number notion was proposed in [23].) In the theory HT_0 the statement, that the value of a signature term without variables is a short word, is provable. One can verify this for T_0 by considering, e.g., an arbitrary and, generally speaking, "non standard" model of the theory T_0, because in it the "standard" words and numbers, which are values of such terms, are necessarily short. The completeness theorem for the predicate logic then provides the required result.

While speaking about standard and nonstandard natural numbers, we use inverted commas since these notions do have an exact sense only with respect to a certain imaginary universe of sets, from which models of the Peano arithmetics and other formal theories are taken. The Gödel theorem on ~~sufficient~~ essential incompleteness of arithmetic axioms and other known results in the foundations of mathematics and set theory along with considerations of the non-exponential and even finite natural row lead to the more consequential point of view that any natural row is nonstandard.

Unluckily, our formal definition of short binary words (as also the one used in [23],) does not fully reflect the intuitive content of this notion. Thus, the constant signature numeric term $(\ldots(2^2)^2\ldots)^2$, obtained, e.g., by tenfold repetition of squaring, defines the actually unfeasible number $2^{2^{10}}$ which we should, nevertheless, accept as feasible in the sense of our formal definition.

Strictly speaking, we should construct only proofs of feasible length in the theories considered. Of course, this would require a total revision of the exposition. Anyway, the reference to the completeness theorem for predicate logic made above appears to be incorrect in this case.

All these informal considerations are adduced here because they correspond to the essence of this paper. However, for simplicity and because of technical reasons in the basic text, we keep to traditions in syntax and semantics.

Note that in spite of nonexponentiality, the natural row considered (consisting of unary words) contains an exponential as a computable partial function defined (or $\neq \infty$) only for feasible (small) numeric values of argument; but it may assume, in general, also unfeasible (large) values. Strictly speaking, in mathematics and its applications totality of the exponential is not so important as equations it satisfies; mathematical apparatus, in which it, somehow, participate, etc.

In this article we will see how unfeasibility of the exponential influences the first elements of recursive function theory and the Kleene realizability theory.

We introduce the following abbreviations:

$$(\{e\}=y) \rightleftharpoons \exists n\,(M(e,n)=y \wedge H(e,n)),$$

$$!\,\{e\} \rightleftharpoons \exists n\,H(e,n)\ (\leftrightarrow \exists y\,(\{e\}=y)),\ \{e\}(x) \rightleftharpoons \{e*x\},\ \{e\}(\bar{x}) \rightleftharpoons \{e*\bar{x}\},$$

where $e^*(x_1,\ldots,x_k) \rightleftharpoons (\ldots((e*x_1)*x_2)*\ldots*x_k)$, $k \geq 1$.
Obviously,

$$<u,v>*(x_1,\ldots,x_k) = <u,<v,x_1,\ldots,x_k>>,$$

where $<x_1,\ldots,x_k> \rightleftharpoons <<x_1,\ldots,x_{k-1}>,x_k>$, $k=3,4,\ldots.$

We give a usual inductive definition of the notion of a partial recursive term (PRT):

1) variables are PRTs;

2) if f is a signature k-ary $k \geq 0$ function, and $t, s_1,\ldots,s_k$ are PRT; then $f(s_1,\ldots,s_k)$ and $\{t\}(s_1,\ldots,s_k)$ are PRTs.

For every PRT r, the formula $(r=z)$, where z is the variable non occurring in r, is defined inductively as usual:

$$(\{t\}(\bar{s})=z) \rightleftharpoons \exists u\,\bar{v}\,(t=u \wedge \bar{s}=\bar{v} \wedge \{u\}(\bar{v})=z),\ (f(\bar{s})=z) \rightleftharpoons \exists \bar{v}\,(\bar{s}=\bar{v} \wedge f(\bar{v})=z).$$

We define

$$!\,t \rightleftharpoons \exists z\,(t=z), \qquad (t=s) \rightleftharpoons \exists\,(t=z \wedge s=z),$$

$$p(\bar{s}) \rightleftharpoons \exists \bar{v}\,(\bar{s}=\bar{v} \wedge p(\bar{v})), \quad (t \cong s) \rightleftharpoons \forall z\,(t=z \leftrightarrow s=z).$$

The first three of these are equivalent to Σ_1-formulae in HT_σ.

Proposition 2.5. *Given any* PRT t *and (possibly empty) list of variables x's one can effectively construct a signature term $\Lambda\bar{x}.t$ that does not contain (free) the variables $\bar{x}$'s and such that* $\mathrm{HT}_0 \vdash \{\Lambda\bar{x}.t\}(\bar{x}) \cong t$.

Note that the term $\Lambda\bar{x}.t$ is a signature term, i.e., a PCF of its free variables and not only primitive recursive as it is usually stated (compare, for example, to the Proposition 5.3 in [17]).

Proposition 2.5 is based on existence of a universal algorithm u_k (concrete for any $k = 0, 1, 2, \ldots$), for which the following is true:

Proposition 2.6. $\mathrm{HT}_0 \vdash \{u_k\}(e, \bar{x}) \cong \{e\}(\bar{x})$, $\bar{x} = x_1, \ldots, x_k$.

One may take (to within a little detail) a usual universal Turing machine as u_k and here we have to establish a polynomial estimation s_k for the time of modelling, that is, to convince us that the following is true in $\boldsymbol{P}$.

Proposition 2.7.

$$H(e * \bar{x}, n) \supset (H(u_k * (e, \bar{x}), s_k(e, \bar{x}, n)) \wedge M(e * \bar{x}, n) = M(u_k * (e, \bar{x}), s_k(e, \bar{x}, n))). \quad \Box$$

Proposition 2.8. $H(u_k * (e, \bar{x}), n) \supset H(e * \bar{x}, n)$. $\Box$

In a general case Proposition 2.5 may be proved by induction on the complexity of a term t. For example, an algorithm $\Lambda\bar{x}.\{t_1\}(t_2)$ is constructed from the algorithms $\Lambda\bar{x}.t_1$, $\Lambda\bar{x}.t_2$ and the universal algorithm u_1.

We may (re)define the algorithm $\Lambda\bar{x}.t$ so that it would satisfy Proposition 2.5 and be *short with respect to free binary arguments of the term* $\Lambda\bar{x}.t$. It means that if $\bar{i}, \bar{y}$ form the list of all variables of the term t, which are not in $\bar{x}$, then for some $r(\bar{i})$ the following is valid (in $\boldsymbol{P}$:)

Condition 2.9. $\mathrm{Un}(\bar{i}) \supset \Lambda\bar{x}.t = B_{r(\bar{i})} * \bar{y}$.

Indeed, $\{\Lambda\bar{x}.t\}(\bar{x}) \cong \{\Lambda\bar{y}\bar{x}, t\}(\bar{y}.\bar{x}) \cong \{(\Lambda\bar{y}\bar{x}, t) * \bar{y}\}(\bar{x})$ and since $\Lambda\bar{y}\bar{x}.t$ is a PCF that depends only on unary arguments $\bar{i}$, one can use the next proposition (where $p(\bar{i}) \rightleftharpoons \Lambda\bar{y}\bar{x}.t$ and $\bar{z} = \bar{y}\bar{x}$).

Proposition 2.10. *For any* PCF $p(\bar{i})$ *of a unary argument i and for* $k = 0, 1, 2, \ldots$ *there are* PCF $r_k(i)$ *and* $s_k(i, \bar{z}, n)$, *where* $\bar{z} = z_1, \ldots, z_k$ *are such that*

(a) $\mathrm{HT}_0 \vdash \{p(i)\}(\bar{z}) \cong \{B_{r(i)}\}(\bar{z})\ (\cong \{B_{r(i)} * \bar{y}\}(\bar{x}))$,

(b) $P \models H(p(i) * \bar{z}, n) \supset H(B_{r(i)} * \bar{z}, \bar{s}(i, \bar{z}, n))$,

(c) $P \models M(p(i) * \bar{z}, n) \supset M(B_{r(i)} * \bar{z}, s(i, \bar{z}, n))$.

Proof. Let π_k be a program for a usual noninitial Turing machine which first transforming an argument $< v, z_1, \ldots, z_k >$ into $< p(B^{-1}(v)), z_1, \ldots, z_k >$; and then, in the case the result is defined, applies the universal program u_k to the result. As a consequence of 2.6, we have that (when $v = B_i$) $\{p(i)\}(\bar{z})$ the result of the algorithm $< \pi_k, B_i >$ on the argument $\bar{z}$. So we define $r_k(i) \rightleftharpoons B^{-1} < \pi_k, B_i >$. The polynomial computability of such function $r_k(i)$ follows from Proposition 2.2, since $< \pi_k, B_i >$ is a short word and, hence, the totality of the function $r_k(i)$ can be proved in HT_0). Finally, the estimation required, s_k, follows from 2.2.

Note that the initiality of the Turing machine is essential in this proof. Indeed, here the linear dependency of the initial program $< \pi_k, B_i > = \pi_k 01 B_i$ with respect to

$|B_i|$ plays an important role. Thanks to it, the word $<\pi_k, B_i>$ is short for any i. In the case of the usual Turing machine we are to consider a non-initial program $\bar{\pi}_k(B_i)$ which is obtained from π_k by adding additional commands which write down the word B_i at the tape instead of the program $<\pi_k, B_i>$. But these commands require a non-linear (more exactly quadratic) with respect to $|B_i|$ part of the program $\bar{\pi}_k(B_i)$ and so we can not guarantee a polynomial computability and even totality of the required function $r_k(i)$ such that $\bar{\pi}_k(B_i) = B_{r_k(i)}$.

Proposition 2.11 (on the unary μ-operator). *Given any quantifier-free formula* $\varphi(x)$ *one can construct* a PRT s *containing the same variables as* φ *and a new variable* x *such that* $\mathrm{HT}_0 \vdash s = x \leftrightarrow \mathrm{Un}(x) \wedge \varphi(x) \wedge \forall y \in \mathrm{Un}\,(y < x \supset \neg\varphi(y))$. □

We denote this term s by $\mu x \in \mathrm{Un}.\varphi(x)$.

Proposition 2.11 can be extended to the case of a partial recursive predicate in the role of φ by adding the unary collection principle for quantifier-free α to HT_0 :

$$\forall i < n \exists j \alpha \supset \exists m \forall i < n \exists j < m \alpha ,$$

where i, j, n, m run over unary words. In this case we can guarantee the upper bound m existence and it means the finiteness of the total time $\leq n \cdot m$ of calculation of values $\varphi(\varnothing), \varphi(1), \varphi(11), \ldots$ up to any unary argument value n such that all the previous values are already defined.

Note that we can not guarantee in HT_0 the recursiveness of the general (not "unary") μ-operator $\mu x.\varphi(x)$, since its (direct) definition is obviously connected with the exponential exhaustive search of binary words. More exactly, because of non-feasibility of the exponential, the direct definition of $\mu x . \varphi(x)$ by the exhaustive search $B_\varnothing, B_1, B_{11}$ appears to be incorrect. Thus, a natural proposition $y = \mu x\,(x = y)$ would be equivalent to the sentence $\exists i\,(B_i = y)$, which is equivalent to the feasibility of the exponential.

Now we prove a proposition on the representation of provably-total Σ_1-functions which strengthens 2.2.

Proposition 2.12. *Suppose that for a new constant* e *and some quantifier-free formulae* $\alpha(e, x, y)$, $\beta(e, x, y)$ *and* a PRT $f(e, x) = f_e(x)$ *depending only on the variables mentioned the following formulae*

$$\exists y \alpha(e, x, y) \supset\, !f_e(x),\ f_e(x) = y \supset \alpha(e, x, y),\ \forall x\, !f_e(x) \supset \forall x \exists y \beta(e, x, y)$$

are derivable (classically) in the theory $\mathrm{T}_0 + \mathrm{Ax}(e)$, *where* $\mathrm{Ax}(e)$ *are some quantifier-free axioms with respect to e.*

Then for some superposition $t_e(x)$ *of the signature functions,* the PRF f_e *and the constant* e *there is (an intuitionistic) proof of*

$$\mathrm{HT}_0 + \mathrm{Ax}(e) + \forall x\, !f_e(x) \vdash \forall x \beta(e, x, t_e(x)).$$

Proof (a sketch). In the frame of the intuitionistic theory $\mathrm{HT}_0 + \mathrm{Ax}(e) + \forall x\, !f_e(x)$ considered we may use f_e as if it was a new signature functional symbol which (by condition of the proposition and because $f_e(x) = y$ is a Σ_1-formula) intuitionistically satisfies the sentence $\forall x \alpha(e, x, f_e(x))$. By condition, in the theory $\mathrm{T}_0 + \mathrm{Ax}(e) + \forall x \alpha(e, x, f_e(x))$ (where f_e is a functional symbol) $\forall x\, !f_e x$ is provable (here f_e is not a functional symbol) and hence $\forall x \exists y \beta(e, x, y)$ is classically provable. As in

Proposition 2.2 using the Herbrand theorem, we obtain an intuitionistic proof in the theory $\mathrm{HT}_0 + \mathrm{Ax}(e) + \forall x\, \alpha(e, x, f_e(x))$ and hence we obtain a proof of the proposition $\forall x\, \beta(e, x, t_e(x))$ in the theory $\mathrm{HT}_0 + \mathrm{Ax}(e) + \forall x\, !f_e(x)$ for some superposition $t_e(x)$ of the type required. □

§3. THE FORMAL KLEENE-CHURCH THESIS AND MARKOV'S PRINCIPLE IN THE FRAME OF POLYNOMIAL COMPUTABILITY THEORY

As to the intuitionistic arithmetics HA, the following variants of the formal Kleene-Church (see [17,18]) thesis may also be added to the theory HT_0 considered:

$$\mathrm{CT}(\varphi): \forall x \exists y\, \varphi(x, y) \supset \exists e \forall x \exists y (\{e\}(x) = y \wedge \varphi(x, y)),$$

$$\mathrm{CT}(\chi, \varphi): \forall x (\chi(x) \supset \exists y\, \varphi(x, y)) \supset \exists e \forall x (\chi(x) \supset \exists (\{e\}(x) = y \wedge \varphi(x, y))),$$

where we put some restrictions on χ to avoid a contradiction with HT_0 (as in the case of HA [17, p.51]).

A formula χ is said to be *negative* (respectively *a Harrop formula*), if it does not contain existential quantifiers (respectively if all its existential quantifiers are situated within antecedents of implications (*Remark:* In this definition we assume that in χ negation is expressed by implication and disjunction is expressed by existential quantifier).

A formula χ is said to be *almost negative* (respectively *U-negative*) if it contains the existential quantifiers only of the type $\exists \overline{x}\, \alpha(\overline{x})$ (respectively $\exists \overline{x} \in \mathrm{Un}\, \alpha(\overline{x})$, where α is a quantifier-free subformula). If all the existential quantifiers of other type are not within antecedents of implications of χ, then χ is said to be *an almost Harrop formula* (*U-harrop* respectively). We define

ECT ($\overline{\mathrm{ECT}}$) - all examples $\mathrm{CT}(\chi, \varphi)$ with an almost negative (respectively almost Harrop) formula χ.

ECT_U ($\overline{\mathrm{ECT}}_U$) - all examples ECT ($\overline{\mathrm{ECT}}$) with a U-negative (respectively U-Harrop) formula χ.

Later on in Corollary 6.9 we prove that the scheme ECT (ECT_U) is equivalent to the formally more general scheme $\overline{\mathrm{ECT}}$($\overline{\mathrm{ECT}}_U$).

We formulate two variants of the Markov principle:

$$M: \neg\neg \exists x\, \alpha(x, \overline{z}) \supset \exists x\, \alpha(x, \overline{z});$$

$$M_U: \neg\neg \exists x \in \mathrm{Un}\, \alpha(x, \overline{z}) \supset \exists x \in \mathrm{Un}\, \alpha(x, \overline{z});$$

where α is quantifier-free formula.

Later we prove constructivity (cf. §1 and corollaries 6.5(b),7.4(b)) of the principles ECT_U and M_U with respect to the theory HT_0. As for traditional variants of ECT and M, they will be shown to have a tight connection with the «P = NP?» problem. Thus, these principles imply existence of an algorithm, which given any compatible formula finds values of variables satisfying it. (See 3.1, 3.2, 6.10, 7.5, 7.6).

We call a binary word e to be *a search algorithm* if the following formula is true for it

$$\mathrm{SA}(e) \rightleftharpoons \forall x (\exists y . x[y] \supset \exists y (\{e\}(x) = y \ \wedge x[y]))$$

or the following $\forall\exists$-formula which is equivalent to the previous one

$$\forall x y \exists n \in \mathrm{Un} (x[y] \supset H(e * x, n) \wedge x[M(e * x, n)]).$$ is true for e.

Recall that $x[y]$ denotes the truth value of the Boolean formula x on the tuple y. The following two formulae assert the existence of a search algorithm and the existence of a short search algorithm:

$$\mathrm{SA} \rightleftharpoons \exists e.\, \mathrm{SA}(e)\,,$$

$$\mathrm{DSA} \rightleftharpoons \exists i \in \mathrm{Un}\,.\, \mathrm{SA}(B_i)\,.$$

Proposition 3.1. (a) $\mathrm{HT}_0 + \mathrm{EST} \vdash \mathrm{SA}$,

(b) $\mathrm{HT}_0 + \mathrm{EST}_U + M \vdash \mathrm{EST} \wedge \mathrm{SA}$.

In Corollary 5.3 (c) we prove that $\mathrm{HT}_0 + \mathrm{ECT} + \mathrm{M}_U \vdash \mathrm{M}$.

Proof. (a) The existence of the algorithm required follows from the next example of ECT:

$$\forall x\,(\exists y.x[y] \supset \exists y.x[y]\,) \supset \exists e\, \forall x(\exists y.x[y] \supset x[\{e\}\,(x)]\,)\,,$$

since its antecedent is a logical axiom $\varphi \supset \varphi$.

(b) By M, $\mathrm{ECT} = \mathrm{CT}(\chi\,,\varphi)$ is reduced to ECT_U by replacing the quantifiers $\exists$ in by $\neg\neg\exists$ in χ and then by $\neg\forall\neg$. Now apply (a).

Corollary 3.2. *Let a theory S in the language* T_0 *have the same* Π_2*-theorems as* T_σ *If S is constructive and has a form of* $\mathrm{HT}_0 + \mathrm{M} + \ldots$ *or S is* $\exists$*-constructive and has a form* $\mathrm{HT}_0 + \mathrm{SA} + \ldots$ *or* $\mathrm{HT}_0 + \mathrm{ECT} + \ldots$; *then* $\mathrm{P} = \mathrm{NP}$.

As we could see later (see 6.7) if $\mathrm{HT}_0 \subseteq S \subseteq \mathrm{HT}_0 + \mathrm{EST} + \mathrm{M}$; then the theory S has the same Π_2-theorems as T_σ

Proof. It is sufficient now to prove derivability of a Π_2-sentence $\mathrm{SA}(e_0)$ in the calculus S for a certain concrete binary word e_0 It implies derivability in T_σ, since it entails existence (in P) of a polynomial search algorithm e_0 which is equivalent to $\mathrm{P} = \mathrm{NP}$ because of 2.2

In the case of $\mathrm{S} = \mathrm{HT}_0 + M + \ldots$ one can, by the Markov principle, prove $\neg\forall y \neg x[y] \subset \exists y.x[y]$, which because of constructivity of S implies provability of $\neg\forall y\neg x[y] \supset x[\,\{e_0\}\,(x)]$ for a certain concrete e_0 and, hence, derivability of $\mathrm{SA}(e_0)$.

In the case of $\mathrm{S} = \mathrm{HT}_0 + \mathrm{SA} + \ldots$ or $= \mathrm{HT}_0 + \mathrm{ECT} + \ldots$, the derivability of $\mathrm{SA}(e_0)$ follows from 3.1 (a) and $\exists$-constructivity of S.

Proposition 3.3. $\mathrm{P} = \mathrm{NP}$ implies equivalence in HT_0 of principles M and M_U and also ECT and ECT_U.

Proof. If α is a quantifier-free formula, then

$$\exists x\, \alpha(x\,,\overline{z}\,) \leftrightarrow \exists n \in \mathrm{Un}\, \exists x < n\, \alpha(x\,,\overline{z}) \leftrightarrow \exists n \in \mathrm{Un}\, \alpha_0(n\,,\overline{z})$$

for some polynomially computable predicate α_0, which exists by $\mathrm{P} = \mathrm{NP}$. Thus, M and ECT are reduced to partial cases M_U and ECT_U.

In Corollaries 7.4(b) and 6.5(b) we shall prove constructivity of the theories HT_0, $\mathrm{HT}_0 + \mathrm{M}_U$, $\mathrm{HT}_0 + \mathrm{ECT}_U$ and $\mathrm{HT}_0 + \mathrm{ECT}_U + \mathrm{M}_U$. So 3.2 and 3.3 imply that each of the theories $\mathrm{HT}_0 + \mathrm{M}$, $\mathrm{HT}_0 + \mathrm{ECT}$, $\mathrm{HT}_0 + \mathrm{EST} + \mathrm{M}_U$ and $(=)\,\mathrm{HT}_0 + {} + \mathrm{ECT}_U + \mathrm{M} = \mathrm{HT}_0 + \mathrm{ECT} + \mathrm{M}$ is constructive if and only if $\mathrm{P} = \mathrm{NP}$. Moreover, the equality $\mathrm{P} = \mathrm{NP}$ is equivalent to provability of Π_2-sentence $\mathrm{SA}(e_0)$ for certain concrete search algorithm e_0 in any of the theories mentioned above (see the beginning of the proof of Corollary 3.2). Note, that this result seems to contradict the fact below (after Theorem 5.2) that there is constructed a rather concrete "search algorithm" ε is constructed which is optimal among all the search algorithms in P. The matter is that its optimality and the sentence $\mathrm{SA}(\varepsilon)$ itself one can prove only in the theory $\mathrm{HT}_0 + \mathrm{EXP}$ or $\mathrm{HT}_0 + \mathrm{DET}$ (the axiom DET is defined in § 4).

In § 5 we shall see that search algorithms are of more wide importance than it follows immediately from the definition, and also that they can transformed into a canonical form. This will be used to prove the basic results. But first we have to consider coding of binary words by the means of unary words.

§ 4. POLYNOMIALLY OPTIMAL CODING OF FINITE BINARY WORDS BY UNARY WORDS

As it was already noted above in the theories for which one can not prove the feasibility of the exponential, the binary words can not be enumerated by the means of the usual coding $x = B(i)$, because of exponential complexity and even partiality of the inverse function $i = B^{-1}(x)$ (if it is total). The words of the form B_i in these theories are very short and so they can not pretend to be even an approximation to the set of all binary words which are subsumed to be in these theory. Nevertheless, it is possible to find a coding of a rather wide set of binary words, which as we shall see later, may be assumed without contradiction to be the set of all binary words and this coding is nonexponential in a certain sense.

So we can take a coding $\{B_i\}$ instead of the coding B_i (=the result of the algorithm B_i if it is defined) . Binary words x of type $x = \{B_i\}$ will be called *constructive* or *simple*. Nonconstructive words (if they do exist) are natural to be called *random* or *complicated*. (see also subsection 1 of Appendix). It is not hard to prove that in HT_0 binary words, for example, are constructive.

Further on we consider the following axioms:

Axioms 4.1. $\mathrm{DET} \rightleftharpoons \forall x \exists i (x = \{B_i\})$,

$$\mathrm{DET}^{e} \rightleftharpoons \forall x \exists i (x = \{B_i\}(e)),$$

$$\mathrm{RDET} \rightleftharpoons \exists e\, \mathrm{DET}^{e}.$$

These axioms assert that all finite binary words are constructive or respectively constructive (with respect to some single binary word e).

Axioms SA and DSA are weaker forms of the axiom DET on constructivity of binary words (see § 5).

A shortcoming of $\{B_i\}$ is its partiality because the algorithm B_i can "get into a loop". So we consider the polynomial computable coding ξ_i for the class of constructive words which is defined by the unary coding of unary pairs $j = «i, n»$ (see § 2).

Definition 4.2. $\xi_{«i,n»} \rightleftharpoons M(B_i, n)$.

More generally, define ξ_j^y for a tuple y of binary words.

Definition 4.3. $\xi^{\bar{y}}_{«i,n»} \rightleftharpoons M(B_i * \bar{y}, n)$.

One can easily reformulate the axioms DET and DET^{e} in HT_0 in terms of this coding by using 2.9 (with the empty list $\bar{x}$):

$$\xi_j^{\bar{y}} = \{B_{r(j)} * \bar{y}\} = \{B_{r(j)}\}(\bar{y}),$$

$$\mathrm{DET} \leftrightarrow \forall x\, \exists j\, (x = \xi_j),$$

$$\mathrm{DET}_c \leftrightarrow \forall x\, \exists j\, (x = \xi_j^c).$$

In [2] similar equivalences were adopted by definition. The following theorem partially implies constructivity of unary and short binary words. The class of constructive words is closed under PCF. Words which are constructive with respect to a constructive word are constructive too and $\mathrm{DET} \leftrightarrow \mathrm{DET}^{\varnothing}$. Thus (relatively) constructive words form a definable in T_0 interpretation of the quantifier-free theory T_0. It is a pity that it can not be proved for the theory T or T_0 + the bounded induction (see in this the connection [2] and particularly correction to [2] in [3,p.490]). The axiom DET (respectively RDET) is obviously valid in the same interpretation .

Theorem 4.4. *A sequence* $\xi_j^{\bar{x}}$, $j = \varnothing, 1, 11, 111, \ldots$ *is a polynomially optimal in the sense that the following facts are provable in the theory* HT_0 *(for a unary* $\bar{\imath}$*):*

(a) $p(\bar{\imath}) = \xi_{r(\bar{\imath})}$,

(b) $p(\bar{\imath},\bar{x}) = \xi^{\bar{x}}_{r(\bar{\imath},\bar{x})}$,

(c) $\{e\}(\bar{\imath},\bar{x}) \cong \xi^{e,\bar{x}}_{q(e,\bar{\imath},\bar{x},t(e,\bar{\imath},\bar{x}))}$;

here $t(e,\bar{\imath},\bar{x}) = \mu z \in \mathrm{Un}\, H(e * (\bar{\imath},\bar{x}),\bar{z})$; *and* p, q, r *are polynomially computable functions, and* p *is arbitrary;* r *depends on* p, *and* q *is an appropriate function.*

In such a way the polynomially optimal sequence $\xi_j^{\bar{x}}$ determines the "most rapid" up to polynomials exhaustive search of binary words´. It "catches up" with every other computable (partial) sequence $\{e\}(i,\bar{x})$, $i = \varnothing, 1, 11, 111$, if the corresponding time for computation of $t(e,i,\bar{x})$ is taken into account.

Proof. (b) evidently implies its subcase (a); (c) also follows from (b):

$$\{e\}(\bar{\imath},\bar{x}) \cong M(e * (\bar{\imath},\bar{x}),\ t(e,\bar{\imath},\bar{x})) \cong \xi^{e,\bar{x}}_{r(\bar{\imath},t(e,\bar{\imath},\bar{x}),e,\bar{x})}.$$

Thus we have to prove (b). At first let us prove (b) for a sequence $\tilde{\xi}_j^{\bar{x}}$ which is defined like $\xi_j^{\bar{x}}$ by the equality $\tilde{\xi}^{\bar{x}}_{«n,i,t»} = M(B_n * (i,\bar{x})\cdot, t)$. Let B_{n_0} be an arbitrary program for the computation of $p(i,\bar{x})$ and $t_0(i,\bar{x})$ is a (polynomial) time of work for this program when started with $i,\bar{x}$. Then

$$p(i,\bar{x}) = M(B_{n_0} * (i,\bar{x}), t_0(i,\bar{x})) = \tilde{\xi}^{\bar{x}}_{«n_0,i,t_0(i,\bar{x})»} = \tilde{\xi}^{\bar{x}}_{r(i,\bar{x})}.$$

(*Remark:* Regrettably the unary number n_0 of B_{n_0} can appear practically unattainable, in contrast to B_{n_0}. Nevertheless in the view of the traditional approach to finite, the number n_0 is "standard" and in such sense is also concrete.)

Thus the sequence $\tilde{\xi}_j^{\bar{x}}$ is polynomially optimal. Our sequence $\xi_j^{\bar{x}}$ is also such while (by 2.10 (c)) $\tilde{\xi}_j^{\bar{x}}$ is polynomially reducible to it:

$$\tilde{\xi}^{\bar{x}}_{«n,i,t»} = M((B_n * i) * \bar{x}), t) \overset{2.10(b)}{=} M(B_{v(n,i)} * \bar{x}, s(n,i,\bar{x},t)) = \xi^{\bar{x}}_{«v(n,i),s(n,i,\bar{x},t)»}. \square$$

It is also easy to produce a one-to-one (unary with the argument n) polynomially optimal sequence $\zeta_n^{\bar{x}} \rightleftharpoons$ IF $\xi_n^{\bar{x}} \notin \{\zeta_m^{\bar{x}} \mid m < n\}$ THEN $\xi_n^{\bar{x}}$ ELSE the first $B_j \notin$ $\notin \{\zeta_m^{\bar{x}} \mid m < n\}$. It is evident that here $j \leq n$ and for some PCF $s(n, \bar{x}) \leq n$ in P we have equality $\xi_{dn}^{\bar{x}} = \zeta_{s(n,\bar{x})}^{\bar{x}}$, from which the polynomial optimality of the different-valued sequence $\zeta_n^{\bar{x}}$ follows.

Proposition 4.5. $\mathrm{HT}_0 + \mathrm{EXP} \vdash \mathrm{DET}$, $P \models \mathrm{DET}$ (i.e. the feasibility of the exponential implies the possibility of optimal coding of all binary words via unary ones).

Proof follows from the equivalence $\mathrm{EXP} \leftrightarrow \forall x \exists i\, (x = B_i)$ and optimality of $\xi_i : B_i = \xi_{r(i)}$.

But the contrary conjecture is false:

Theorem 4.6. [2] EXP *can not be proved in the theory* $\mathrm{T}_0 + \mathrm{DET}$. *All provably-recursive functions from unary argument in* $\mathrm{T}_0 + \mathrm{DET}$ *are* PCFs.

Proof. Define $\nu(x)$ the PRF $\mu i \in \mathrm{Un}\, (x = \xi_i)$ taking unary values which are inverse to ξ_i. Thus $x \simeq \xi_{\nu(x)}$ and $\nu(\xi_i) \leq i$. The function $\alpha(i) \rightleftharpoons \nu(\xi_i)$ is evidently polynomially computable. Because of DET the function ν is everywhere defined. From the cardinality argument it is clear that this function has an exponential growth for some arguments and thus is not computable in a polynomial time. Nevertheless, every superposition $t(n)$ of signature functions and of the function ν from only one unary variable n gives PCF. Indeed, the function ν can be eliminated from $t(n)$ on the basis of polynomial optimality of ξ: $\nu(p(n)) = \nu(\xi_{r(n)}) = \alpha(r(n))$, where $p(n)$ is an arbitrary PCF. Hence as in Proposition 2.2 and Corollary 2.4 we use the Herbrand theorem to obtain the result needed □.

In contrast to Theorem 4.6 and Corollary 2.4 we have

Proposition 4.7 [2, p.574]. $\mathrm{T}_0 + \Delta\text{–Coll} + \mathrm{RDET} \vdash \mathrm{EXP}$.

Proof. $\Delta =$ Coll and DET give

$$\forall n \exists m \forall x \leq n \exists j < m\, (x = \xi_j^e).$$

But this leads to EXP, because in T_0 an (evidently true) implication

$$\forall x \leq n \exists j < m\, (x = \xi_j^e) \supset m \geq 2^{n+1} - 1$$

is deducible. Indeed , its contraposition follows from the quantifier-free formula

$$m < 2^{n+1} - 1 \supset \forall j < m\, (X^e(m) \neq \xi_j^e) \wedge (X^e(m) \leq n,$$

which holds in P, where $X^e(m) \rightleftharpoons B(\mu i \leq m \forall j < m\, (B_j \neq \xi_j^e))$ is a PCF from m and e.

Open Problem. Is it true that T_0+ a limited induction + $\mathrm{DET} \vdash \mathrm{EXP}$? (See also the correction to [2] in [3, p.490]).

For axioms RDET and DET^e which are weaker than DET (e is a new constant) it is possible to strengthen Theorem 4.6 in the following way.

Theorem 4.8. *Theories* $\mathrm{T}_0 + \mathrm{RDET}$ *and* $\mathrm{T}_0 + \mathrm{DET}^e$ *expand conservatively the theory* T_0 *relatively to* Π_2*-formulae not containing the constant* e.

Proof. We see first hat words of the form ξ_i^e, where i runs through unary words (and e is fixed), are forming an interpretation of the theory $\mathrm{T}_0 + \mathrm{DET}^e$ in the theory

T_0 (cf. the hint before Theorem 4.4). Thus, if $\mathrm{T}_0 + \mathrm{DET}^e \vdash \forall x \exists y \alpha(e, x, y)$ for quantifier-free α; then $\mathrm{T}_0 \vdash \forall i \exists j \alpha(e, \xi_i^e, \xi_j^e)$, where the constant e now plays the role of a variable. We get $\mathrm{T}_0 \vdash \forall x \exists y \alpha(x, x, y)$ from above and from the fact that every word x is evidently representable in the form $x = \xi_i^x$ for some i. Thus in particular the conservativeness relatively to the Π_2-formulae $\forall x \exists y \alpha(x, y)$ without constant e is proved. □

§ 5. GENERAL CANONICAL SEARCH ALGORITHMS

Let us look back at search algorithms. On the basis of the polynomially optimal exhaustive search $\xi_i^{(e)}$ of binary words one evidently can produce a (relatively) short search algorithm if the corresponding axiom on (relative) constructivity of all binary words holds. Thus in HT_0 we have implications

$$\begin{tikzcd}
 & & \mathrm{DSA} \arrow[dr] & \\
\mathrm{EXP} \arrow[r] & \mathrm{DET} \arrow[ur] \arrow[dr] & & \mathrm{SA} \\
 & & \mathrm{RDET} \arrow[ur] &
\end{tikzcd}$$

In particular from the implication RDET → SA and Theorem 4.8 we have

Theorem 5.1. *The theory* $\mathrm{T}_0 + \mathrm{SA}(e)$ *expands conservatively the theory* T_0 *relatively to* Π_2*-formulae (without* e*)* □

From this or from Theorem 4.6 and from the implication DET → SA we find underivability in T_0 of the lower exponential bound of the time of work for search algorithms (cf. [2] and also the exact form of the proposition on the lower valuation in Corollary 6.8).

Apart from the formula $x[y]$, which is involved in the definition of a search algorithm, we will be also interested in arbitrary quantifier-free formulae $\alpha(x, y)$ playing similar roles.

Theorem 5.2 (on canonical search algorithms). *For every quantifier-free formula* $\alpha(x, y)$ *the following formulae are deducible in* HT_0:

(a) $\exists j\, \mathrm{SA}(\xi_j^e) \wedge \exists y\, \alpha(x, y) \supset \exists i\, \alpha(x, \xi_i^{e,x})$,

(b) $\mathrm{DSA} \wedge \exists y\, \alpha(x, y) \supset \exists i\, \alpha(x, \xi_i^x)$,

(c) $\mathrm{DET} \wedge \exists y\, \alpha(x, y) \supset \exists i\, \alpha(x, \xi_i)$.

Note that, by Proposition 2.10 (a), $\mathrm{DSA} \leftrightarrow \exists j\, \mathrm{SA}(\xi_j)$.

The point (a) of Theorem 5.2 means that for every binary word e containing information on some search algorithm $e' = \xi_j^e$ for propositional formulae, one can produce a (unified in its essence) search algorithm for all quantifier-free formulae $\alpha(x, y)$, which is based on the exhaustive search $\xi_i^{e,x}, i = \varnothing, 1, 11, 111, \ldots,$; namely, the algorithm

$$\varepsilon_\alpha(e) \rightleftharpoons \Lambda x . \xi^{e,x}(\mu i \in \mathrm{Un}. \alpha(x, \xi_i^{e,x})) .$$

If this starting information e is a short one then in accordance with (a) or (b) a similar search algorithm ε (for $\alpha(x, y) \rightleftharpoons x[y]$) based on exhaustive search ξ_i^x will not depend on e. It is obvious that $\mathrm{DSA} \leftrightarrow \mathrm{SA}(\varepsilon)$. Moreover, the algorithm ε is *polynomially optimal* among all short search algorithms and even among all search algorithms of the form ξ_j in the following sense: for every satisfiable propositional formula x the time of computation $\{\varepsilon\}(x)$ can appear longer than that for $\{\xi_j\}(x)$ in no more than polynomial times, with such a polynomial, of course, being dependent on j. This assertion can be obtained through use of Theorem 4.4(c) and (b) with $e = \xi_j$. It is also possible at first to deduce in HT_0 the formula

$$\forall x j n \exists m\, (x[M(\xi_j * x, n)] \wedge H(\xi_j * x, n) \supset x[M(\varepsilon * x, m)] \wedge H(\varepsilon * x, m))$$

on the basis of the polynomial optimality of ξ and of definition of the algorithm ε and then to make use of Proposition 2.2. The existence of the polynomially optimal search algorithm (in the "standard" universe of finite objects) was asserted in [24], but without revealing of the very algorithm and also without determining of the optimal exhaustive search of binary words on which our search algorithms are based (were introduced in [2]). It is evident that the lexicographic exhaustive search is utterly ineffective as a search algorithm.

Proof of Theorem 5.2. (c) is evident and (b) follows from (a) and from the polynomial optimality of ξ. The proof of (a) is evidently reducible to the case of a bounded $\exists y$ quantifier, i.e. of the form $\exists y \le n$, where n is a new variable. Because of the well-known polynomial reducibility of the problem of finding of $y \le n$ such that $\alpha(x, y)$ is true to the problem of satisfiability of appropriate propositional formula (i.e., because of the to NP-completeness of the problem of satisfiability of propositional formulae, [4]); it is possible to rebuild (in a polynomial time) a given search algorithm $e' = \xi_i^e$ satisfying SA (e') into a search algorithm $s(e')$ for $\alpha(x, y)$:

$$\mathrm{HT}_0 \vdash \exists y \le n\, \alpha(x, y) \supset \exists y\, (y = \{s(e')\}(x) \wedge y \le n \wedge \alpha(x, y)).$$

But in accordance with Theorem 4.4 (c), (b) and the equality $e' = \xi_j^e$ we have

$$y = \{s(e')\}(x) \overset{(c)}{\cong} \xi^{s(e'), x}_{q(s(e'), x, t(s(e'), x))} \overset{(b)}{\cong} \xi^{e, x}_{r(j, e, x, t_1(j, e, x))}.$$

Thus y has the form $\xi_i^{e, x}$. The theorem is proved. □

Corollary 5.3. (a) $\mathrm{HT}_0 + \mathrm{SA} + \mathrm{ECT}_U \vdash \mathrm{ECT}$,

(b) $\mathrm{HT}_0 + \mathrm{SA} + \mathrm{M}_U \vdash \mathrm{M}$,

(c) $\mathrm{HT}_0 + \mathrm{ECT} + \mathrm{M}_U \vdash M$.

Proof. By Theorem 5.2(a) and Proposition 3.1(a), it follows from SA and ECT that formula of the form $\exists y\, \alpha(y, \bar{z})$ is equivalent to the formula $\exists i \in \mathrm{Un}\, \alpha(\xi_i^{e, z}, \bar{z})$ with unary $\exists$, where α is quantifier-free and e denotes the search algorithm whose existence is asserted by SA.

Using this scheme, we reduce ECT and M to ECT_U and M_U correspondingly. □

Let us define PRFs "inverse" to canonical search algorithms introduced in Theorem 5.2:

$$\nu(x) \rightleftharpoons \mu i \in \mathrm{Un}\, (x = \xi_i) \quad \text{(see the proof of Theorem 4.6)},$$

$$\nu^2(x, y) \rightleftharpoons \mu i \in \mathrm{Un}\, (x[y] \supset x[\xi_i^x]),$$

$$\nu^3(e,x,y) \rightleftharpoons \mu i \in \mathrm{Un}\,(x[y] \supset x[\xi_i^{e,x}]) .$$

Let us introduce the notation

$$\mathrm{SA}^e \rightleftharpoons \forall x y! \, \nu^3(e,x,y) \; (\leftrightarrow \forall x y\, (x[y] \supset \exists i\, x[\xi_i^{e,x}])) .$$

Because of Theorem 5.2 and the polynomial optimality of ξ we have

Proposition 5.4. *Following equivalencies are deducible in* HT_0 ,

$$\mathrm{SA}^e \leftrightarrow \exists j\, \mathrm{SA}\,(\xi_j^e) ,$$

$$\forall x y! \, \nu^2(x,y) \leftrightarrow \mathrm{DSA} ,$$

$$\forall x !\, \nu(x) \leftrightarrow \mathrm{DET} . \; \square$$

Notice that if some concrete search algorithm e_0 works (in P) in a polynomial time, i.e. if P=NP; then $\mathrm{T}_0 \vdash \mathrm{SA}(e_0) \wedge \mathrm{DSA}$ and thus by 5.4 $\mathrm{T}_0 \vdash \mathrm{SA}^{e_0} \wedge \forall x y! \, \nu^2(x,y)$ and by Proposition 2.2 functions $\nu^3(e_0,x,y)$ and $\nu^2(x,y)$ appear to be polynomially computable (in P). More exactly, we have

Proposition 5.5. *The existence in P of a concrete word e_0, for which the function $\nu^3(e_0,x,y)$ is polynomially computable, is equivalent to polynomial computability of the function $\nu^2(x,y)$; and is equivalent to* P = NP . □

Recall that the function $\nu(x)$ is certainly uncomputable in a polynomial time.

§ 6. KLEENE'S REALIZABILITY AND CONSTRUCTIVITY OF THEORIES CONTAINING ECT_U

Let us now define the Kleene realizability; i.e., let us put in correspondence to every formula φ another one $x \mathbf{r} \varphi$, all free variables of which are exactly those of the formula φ plus the variable x. Additionally we make it in such a manner that formula $x\mathbf{r}\varphi$ appears to be not only almost negative (as in [17, p.51]) but U-negative; i.e., it doesn't contain quantifiers $\exists$ on unary words only (this is needed for the proof of Proposition 6.1). Let, by induction,

$$x\mathbf{r}\varphi \rightleftharpoons \varphi \quad \text{if} \quad \varphi \text{ is an atomic formula,}$$

$$\langle x,y\rangle\, \mathbf{r}(\alpha \wedge \psi) \rightleftharpoons x\mathbf{r}\,\varphi \wedge y\mathbf{r}\psi ,$$

$$\langle x,y,z\rangle\, \mathbf{r}(\varphi \vee \psi) \rightleftharpoons (x=0 \supset y\mathbf{r}\varphi) \wedge (x \neq 0 \supset z\,\mathbf{r}\,\psi) ,$$

$$\langle x,y\rangle \mathbf{r}\, \exists y \psi(y) \rightleftharpoons x\mathbf{r}\psi(y) ,$$

$$x\mathbf{r}\,(\varphi \supset \psi) \rightleftharpoons \forall y\, (y\,\mathbf{r}\psi \supset \exists z \in \mathrm{Un}\, H(x*y,z)) \wedge \forall y z\, (y\,\mathbf{r}\,\varphi \wedge H(x*y,z) \supset M(x*y,z)\mathbf{r}\,\psi) ;$$

$$x\mathbf{r}\forall y\, \psi(y) \rightleftharpoons \forall y\, \exists z \in \mathrm{Un}\, H(x*y,z) \wedge \forall y z\, (H(x*y,z) \supset M(x*y,z)\mathbf{r}\psi(y)) .$$

Define also $\mathbf{r}\varphi \rightleftharpoons \exists x\,(x\,\mathbf{r}\,\varphi)$.

Proposition 6.1. *In the theory* HT_0 *the scheme* $\varphi \leftrightarrow \mathbf{r}\,\varphi$ *is deducible from the scheme* ECT_U.

It follows from Theorem 6.3(c) that these schemes are in fact equivalent.

Proof is by induction on the construction of φ. Let, for example, $\varphi \rightleftharpoons \psi \supset \eta$. Using the assumption of induction we get

$$(\psi \supset \eta) \leftrightarrow (\exists x\,(x\mathbf{r}\psi) \supset \exists y\,(y\mathbf{r}\eta)) \leftrightarrow \forall x\,(x\mathbf{r}\psi \supset \exists y\,(y\mathbf{r}\eta)).$$

From this and from ECT_U (taking into account that formula $x\mathbf{r}\psi$ is almost negative with unary $\exists$) it follows that

$$\exists e\,\forall x\,(x\mathbf{r}\psi \supset \exists y\,(\{e\}(x) = y \wedge y\mathbf{r}\eta))\,;$$

i.e., $\mathbf{r}\,(\psi \supset \eta)$. Conversely, let us show that $e\mathbf{r}\,(\psi \supset \eta)$ implies $\psi \supset \eta$; i.e., let us deduce η from $e\mathbf{r}(\psi \supset \eta)$ and ψ. By the inductive assumption we have $x\mathbf{r}\psi$ for some x. Then $\{e\}\,(x)\mathbf{r}\eta$ and again by assumption we get η. Notice that in the case $\varphi \rightleftharpoons \forall y\psi$ instead of ECT_U it is possible to use its particular case CT. □

In the absence of the formal Church thesis such a link of truthfulness of formulae with their realizability can be guarantied only for formulae of a special form. Let us define for every almost Harrop formula χ its *potential* realization - the PRT $\tau_e\,[\chi]$, where parameter e denotes a binary word containing information on some search algorithm: i.e., suppose SA^e to hold (see 5.4). Let inductively

$$\tau_e\,[\mathrm{atom}] \rightleftharpoons \varnothing\,;$$

$$\tau_e\,[\varphi \wedge \psi] \rightleftharpoons \,<\tau_e\,[\varphi]\,,\tau_e\,[\psi]>\,;$$

$$\tau_e\,[\alpha \vee \beta] \rightleftharpoons \,<\ \mathrm{IF}\ \alpha\ \ \mathrm{THEN}\ 0\ \mathrm{ELSE}\ 1,\ \tau_e\,[\alpha]\,,\tau_e\,[\beta]\ >\,;$$

$$\tau_e\,[\eta \supset \psi] \rightleftharpoons \Lambda x.\,\tau_e\,[\psi]\ (x\ \ \text{is a new variable});$$

$$\tau_e\,[\neg\,\eta] \rightleftharpoons \Lambda x.\,\varnothing\,;$$

$$\tau_e\,[\forall x\,\psi\,(x)] \rightleftharpoons \Lambda x.\,\tau_e\,[\psi(x)]\,;$$

$$\tau_e\,[\exists x \in \mathrm{Un}\,\alpha(x)] \rightleftharpoons \,<\varnothing\,,\mu x \in \mathrm{Un}\,\alpha\,(x)>\,;$$

$$\tau_e\,[\exists x\,\alpha\,(x\,,\bar{z}\,)] \rightleftharpoons \,<\varnothing\,,\xi^{e,\bar{z}}\,(\mu\,i \in \mathrm{Un}\,\alpha\,(\xi_i^{e,\bar{z}}\,,\bar{z}))>\,;$$

where $\varphi\,,\psi$ are almost Harrop; $\alpha\,,\beta$ are quantifier-free; η is an arbitrary formula. If the almost Harrop formula χ in fact is a Harrop one, then $\tau_e\,[\chi]$ is the signature term (which is everywhere defined and polynomially computable).

Lemma 6.2. *If $\chi\,(e)$ is almost Harrop and $\theta\,(e)$ is almost negative, then in the theory $\mathrm{HT}_0 + \mathrm{SA}^e$ following equivalencies are derivable:*

$$\mathbf{r}\chi \leftrightarrow\, !\,\tau_e\,[\chi] \wedge \tau_e\,[\chi]\,\mathbf{r}\,\chi\,,$$

$$\mathbf{r}\,\theta \leftrightarrow \theta \leftrightarrow\, !\,\tau_e\,[\theta] \wedge \tau_e\,[\theta]\,\mathbf{r}\,\theta\,.$$

In addition in the case of the U-negative formula θ and the U-Harrop formula χ the axiom SA^e is not used and ξ^e is not present in $\tau\,[\theta]$ and $\tau\,[\chi]$.

Proof . Let us proceed by induction on the construction of formulae χ and θ; Theorem 5.2 on canonical search algorithms is used in the case $\chi\,,\theta \rightleftharpoons \exists x\,\alpha$. In fact, for θ implications $\mathbf{r}\,\theta \supset \theta$ and $\theta \supset\, !\,\tau_e\,[\theta] \wedge \tau_e\,[\theta]\,\mathbf{r}\,\theta$ are to be proved. □

Now we can formulate and prove the main theorem on r-realizability.

Theorem 6.3. (a) *For each logical rule* $\varphi_1, \ldots, \varphi_n/\varphi$, $n \geq 0$ *of the theory* HT_0 *and* PRT*s* $t_1, \ldots, t_n$ *(possibly with new constants) one can construct* a PRT t *such that*

$$\mathrm{H\,T}_0 + \tilde{\forall} \bigwedge_{i=1}^{\nu} (!t_1 \wedge t_i \mathrm{r} \varphi_i) \vdash \; !t \wedge t\mathrm{r}\varphi ,$$

where $\tilde{\forall}$ *denotes the universal closure on all free variables.*

(b) *For all non-logical (quantifier-free) axioms* θ *of the theory* HT_0 *we have* $\mathrm{HT}_0 \vdash \tau[\theta]\,\mathrm{r}\theta$, *where* $\tau[\theta]$ *is a signature term.*

(c) *For each of examples* $\overline{\mathrm{ECT}}$, ECT_U, M *and* M_U *it is possible to construct corresponding realizing signature terms* $t(e), t_U, t_{\mathrm{M}}(e)$ *and* $t_{\mathrm{M}U}$ *such that*

$$\mathrm{HT}_0 \vdash t_U \mathrm{r}\, \overline{\mathrm{ECT}}_U ,$$

$$\mathrm{H\,T}_0 + \mathrm{SA}^{\epsilon} \vdash t(e)\, \mathrm{r}\, \overline{\mathrm{ECT}} ,$$

$$\mathrm{HT}_0 + \mathrm{ECT} \vdash \mathrm{r}\, \overline{\mathrm{ECT}} ,$$

$$\mathrm{HT}_0 + \mathrm{M}_U \vdash t_{\mathrm{M}U} \mathrm{r}\, \mathrm{M}_U ,$$

$$\mathrm{HT}_0 + \mathrm{SA}^{\epsilon} + \mathrm{M} \vdash t_{\mathrm{M}}(e)\, \mathrm{r}\, \mathrm{M} ,$$

$$\mathrm{HT}_0 + \mathrm{ECT}_U + \mathrm{M} \vdash \mathrm{r}\,\mathrm{M} \wedge \mathrm{r}\, \overline{\mathrm{ECT}}.$$

(d) *There exists* PRT $t_S(e)$ *such that* $\mathrm{HT}_0 + \mathrm{SA}^{\epsilon} \vdash \; !t_S(e) \wedge t_S(e)\, \mathrm{r}\, \mathrm{SA}^{\epsilon} \wedge \mathrm{r}\, \mathrm{SA}$.

Notice that from the formulation of the theorem one cannot prove existence of the PRT t such that $\mathrm{HT}_0 + \mathrm{SA} \vdash t\,\mathrm{r}\,\mathrm{SA}$ or $\mathrm{HT}_0 + \mathrm{ECT} \vdash t\mathrm{r}\mathrm{ECT}$.

Proof. (a) See, e.g., [17, p.5 4-55]. (b) follows from Lemma 6.2: $\mathrm{HT}_0 \vdash \theta \leftrightarrow \tau[\theta]\,\mathrm{r}\theta$.

(c) As a realizability of $\overline{\mathrm{ECT}}_U$ and $\overline{\mathrm{ECT}}$,

$$\forall x (\psi(x, \bar{z}) \supset \exists y \psi(x, y, \bar{z})) \supset \exists f \forall x (\psi(x, \bar{z}) \supset \exists n (H(f \bullet x, n) \wedge$$
$$\wedge\; \varphi(x, M(f \bullet x, n), \bar{z}))) ,$$

one can take the PRT $t \rightleftharpoons \Lambda \nu < R(\nu, \bar{z}), F(\nu, \bar{z}) >$, where

$$F(\nu, \bar{z}) \rightleftharpoons \Lambda x(\{\{\nu\}(x)\}(\tau((x, \bar{z})))_2, \quad \tau((x, \bar{z}) \rightleftharpoons \tau_e[\psi(x, \bar{z})]$$

is the potential realization from Lemma 6.2 (without participation of ξ and e in the case of $\overline{\mathrm{ECT}}_U$) of an almost Harrop formula ψ and

$$R(\nu, \bar{z}) \rightleftharpoons \Lambda xw. << 0, S(\nu, x, \bar{z}) >, N(\nu, x, \bar{z}) > \text{(}w\text{ is a new "fictitious" variable)}$$

$$S(\nu, x, \bar{z}) \rightleftharpoons (\{\{\nu\}(x)\}(\tau((x, \bar{z})))_1 \text{ and } N(\nu, x, \bar{z}) \rightleftharpoons \mu n \in \mathrm{Un}\,.\,H(F(\nu, \bar{z}) \bullet x, n).$$

Indeed, let us show that from

$$\nu\, \mathrm{r} \forall x(\psi(x) \supset \exists y \varphi(x, y)) \tag{1}$$

it follows

$$R(\nu, \bar{z})\mathrm{r} \forall (\psi(x, \bar{z}) \supset \exists n(H(F(\nu, \bar{z}) \bullet x, n) \wedge \varphi(x, M(F(\nu, \bar{z}) \bullet x, n), \bar{z})))$$

or, equivalently,

$$\forall xw(w\mathbf{r}\psi(x) \supset\ !N(v,x,\bar{x}) \wedge\ !S(v,x,\bar{x})\mathbf{r}\psi(x, M(F(v,\bar{x}) * x, N(v,x,\bar{x})), \bar{x})) . \tag{2}$$

In accordance with Lemma 6.2, $!\tau(x,\bar{x})\mathbf{r}\psi(x,\bar{x})$ follows from SA^{e} and $w\mathbf{r}\varphi(x,\bar{x})$ in the case of $\overline{\mathrm{ECT}}$. Thus by the assumption (1) we have $!\{\{v\}(x)\}\tau(x,\bar{x}))\mathbf{r}\,\exists y\varphi(x,y,\bar{x})$; i.e.,

$$!\{F(v,\bar{x})\}\,(x), \tag{3}$$

$$!S(v,x,\bar{x})\mathbf{r}\varphi(x, \{F(v,\bar{x})\}\,(x)) . \tag{4}$$

But (3) is equivalent to $!N(v,x,\bar{x})$ and from (4) and $\{F(v,\bar{x})\}\,(x) \cong M(F(v,\bar{x}) * x,$ $N(v,x,\bar{x}))$ we also obtain the second conjunctive member of the implication (2).

The statement $\mathrm{HT}_0 + \mathrm{ECT} + \mathbf{r}\overline{\mathrm{ECT}}$ now follows by Proposition 3.1(a).

As a realizability of the Markov principle $\{M, \neg\neg\exists x\,\alpha(x) \supset \exists x\alpha(x)$ and its special case M_U with $\alpha(x) \rightleftharpoons x \in \mathrm{Un} \wedge \alpha'(x)$ we can take the signature term $t_{\mathrm{M}}(e) \rightleftharpoons$ $\rightleftharpoons \Lambda y.\tau_e(\exists x\alpha(x))$. Indeed, $\neg\neg\exists x\alpha(x)$ follows from $y\mathbf{r}\neg\neg\exists x\alpha(x)$ in HT_0 and so we deduce $\exists x\alpha(x)$ using M or M_{U} correspondingly. Hence using Lemma 6.2 (and SA^{e} in the case of M_U) we get $!\tau_e[\exists x\alpha(x)] \wedge \tau_e[\exists x\,\alpha(x)]\,\mathbf{r}\,\exists x\alpha(x)$, as required.

The statement $\mathrm{HT}_0 + \mathrm{ECT}_{\mathrm{U}} + \mathrm{M} \vdash \mathbf{r}M \wedge \mathbf{r}\overline{\mathrm{ECT}}$ now follows from Proposition 3.1(b).

(d) As the formula SA^{x} is almost negative with unary $\exists$, we get $\mathrm{HT}_0 +$ $+ \mathrm{SA}^{x} \leftrightarrow\ !\tau[\mathrm{SA}^{x}]\mathbf{r}\mathrm{SA}^{x}$ by Lemma 6.2 and thus it is possible to put $t_s(e) \rightleftharpoons \tau[\mathrm{SA}^{e}]$.

Corollary 6.4. *If* $\mathrm{HT}_0 + \mathrm{SA}^{e} + \mathrm{M} + \mathrm{ECT} \vdash \varphi(e,\bar{x})$, *where e is a new constant, then for some* PRT $t(e,\bar{x})$ *we have*

$$\mathrm{HT}_0 + \mathrm{SA}^{e} + \mathrm{M} \vdash\ !t(e,\bar{x}) \wedge t(e,\bar{x})\mathbf{r}\varphi(e,\bar{x}).$$

Also if the first proof was produced in the theory $\mathrm{HT}_0\,(+\mathrm{M}_U) + \mathrm{ECT}_U$, *then the second one can be produced in* $\mathrm{HT}_0\,(+\mathrm{M}_{\mathrm{U}})$ *and the term* $t(e,\bar{x}) = t(\bar{x})$ *can be chosen to be a signature one* (by Proposition 2.2).

In accordance to Proposition 2.12 and definitions of ν^3 and SA^{e} at the end of §5 here one can take the term $t(e,\bar{x})$ to be a superposition of signature functions, of functions $\nu^3(e,x,y)$ from x and y and, the constant e; and also that $\mathrm{HT}_0 + \mathrm{SA}^{e} \vdash\ !t(e,\bar{x})$. In this sense and taking into account Corollary 6.5 and the definition of constructivity of the theory from §1, it is possible to state that the degree of constructivity for the theory $\mathrm{HT}_0 + \mathrm{SA}^{e} + \mathrm{ECT} + \mathrm{M}$ (and for some of its weakenings) is characterized by the computational complexity of the function $\nu^3(e,x,y)$ from x and y.

Corollary 6.5 (on constructivity). (a) *The theory*

$$\mathrm{HT}_0 + \mathrm{SA}^{e}(+\mathrm{M}) + \mathrm{ECT}_{\mathrm{U}}$$

is constructive. In fact if the implication $\chi(e,\bar{x}) \supset \exists y\varphi(e,\bar{x},y)$ *with the almost Harrop premise χ is deducible in it, then in this theory with* ECT *instead of* $\mathrm{ECT}_{\mathrm{U}}$ *the implication* $\chi(e,\bar{x}) \supset\ !t(e,\bar{x}) \wedge \varphi(e,\bar{x},t(e,\bar{x}))$ *also can be deduced for some* PRT $t(e,\bar{x})$. *If the premise χ is absent, then $t(e,\bar{x})$ is the superposition of signature functions, of function* $\nu^3(e,x,y)$ *and of constant e.*

(b) *The theory* $\mathrm{HT}_0 + \mathrm{ECT}_{\mathrm{U}}(+\mathrm{M}_U)$ *is constructive and even polynomially $\exists$-constructive* (see §1.)

Remark. Regrettably, e or, equivalently, SA^e cannot be omitted here.

Proof. (a) By Corollary 6.4 we get in $\mathrm{HT}_0 + \mathrm{SA}^e(+\mathrm{M})$ a proof of a formula of the form $w\mathrm{r}\chi(e,\bar{x}) \supset \mathrm{r}\varphi(e,\bar{x},\{\bar{t}(e,\bar{x})\}(w))$. Further, Lemma 6.2 provides the validity of $\mathrm{r}\chi(e,\bar{x}) \supset \mathrm{r}\varphi(e,\bar{x},\{t(e,\bar{x})\}(\tau_e[\chi(e,\bar{x})]))$. Hence if we put $t \rightleftharpoons \{\bar{t}\}(\tau_e[\chi])$ and use Proposition 6.1, then we get the result needed. In the absence of χ we have $\vdash\, !t$ and appeal Proposition 2.12.

(b) The statement follows from the proof of (a) when the second part of Corollary 6.4 is taken into account together with the U-Harrop form of the formula χ which is required in the definition of constructivity of a theory , and Lemma 6.2; as a result the axiom SA^e is not used (and $\bar{t}$ is a signature term) □.

Corollary 6.6. *The theory* $\mathrm{HT}_0 + \mathrm{SA}^e(+\mathrm{M}) + \mathrm{ECT}$ *expands conservatively the theory* $\mathrm{HT}_0 + \mathrm{SA}^e(+\mathrm{M})$ *relatively to almost negative formulae. Analogously the same holds for* $\mathrm{HT}_0(+\mathrm{M}_U) + \mathrm{ECT}_U$ *and U-negative formulae.*

Proof consists of the use of Corollary 6.4 (and Theorem 6.3) and Lemma 6.2. □

From this combined with Theorem 5.1 we have

Corollary 6.7. *the theory* $\mathrm{HT}_0 + \mathrm{ECT} + \mathrm{M}$ *conservatively expands theories* T_0 *and* HT_0 *relatively to* Π_2*-formulae. Hence its provably-recursive functions are exactly the polynomially computable functions.*

In particular in this theory EXP can not be proved, but SA can be, and the following takes place.. □

Corollary 6.8. *In the theory* $\mathrm{HT}_0 + \mathrm{ECT} + \mathrm{M}$ (as in T_0 [2]) *the statement on existence of a lower exponential bound for the time of work of an algorithm, i.e. the formula*

$$\mathrm{SA}(e) \supset \forall z \exists x > z \exists n (H(e \bullet x, n) \wedge \forall m < n \neg H(e \bullet x, m) \wedge \mathrm{exp}(x, n))$$

cannot be proved. □

From Theorem 6.3 (c) and Proposition 6.1 we also get

Corollary 6.9. $\mathrm{HT}_0 + \mathrm{ECT} \vdash \overline{\mathrm{ECT}}, \mathrm{HT}_0 + \mathrm{ECT}_U \vdash \overline{\mathrm{ECT}}_U$.

Theorem 6.10. *Constructivity of the theory* $\mathrm{HT}_0 + \mathrm{ECT}(+\mathrm{M})$ *is equivalent to its (polynomial)* $\exists$*-constructivity and is equivalent to the equality* P=NP.

Proof. We shall show that from $\exists$-constructivity of this theory follows P=NP from which, in turn, its (polynomial $\exists$)-constructivity follows. Indeed from $\exists$-constructivity of this theory and from Proposition 3.1 we obtain derivability of the formula $\mathrm{SA}(e^0)$ in it, or, equivalently, of the formula

$$\forall xy \exists n \in \mathrm{Un}\, (x[y] \supset H(e_0 \bullet x, n) \wedge x[\mathrm{M}(e_0 \bullet x, n)])$$

for some concrete search algorithm e_0. But in such a case by Corollary 6.7 and Proposition 2.2 the search algorithm e_0 works (in P) polynomial time which is known to imply P=NP.

Next P=NP ensures (polynomial $\exists$-) constructivity of the theory under consideration. The proof follows from Proposition 3.3 and Corollary 6.5(b).

§ 7. CONSTRUCTIVITY OF THEORIES WITHOUT ECT_U

In absence of the scheme ECT_U we can not use Proposition 6.1 on the derivability of equivalence $\varphi \leftrightarrow \mathrm{r}\varphi$ for the proof of constructivity of the theory in question (see Corollary 6.5). For this reason we somewhat modify the notion of realizability. Namely define formula $x\mathbf{q}\varphi$ (see [18, p.178]) by induction on the construction of φ similar to the definition of $x\mathbf{r}\varphi$, changing only three points:

$$<u\,,v\,,w>\mathbf{q}\,(\varphi\vee\psi)\rightleftharpoons[u=0\supset(v\mathbf{q}\,\varphi)\wedge\varphi]\wedge[u\neq 0\supset(w\mathbf{q}\,\varphi)\wedge\psi]\,,$$

$$<x\,,y>\mathbf{q}\,\exists y\varphi(y)\rightleftharpoons(x\mathbf{q}\,\varphi\,(y))\wedge\varphi\,(y)\,,$$

$$x\mathbf{q}\,(\varphi\supset\psi)\rightleftharpoons\forall y((y\mathbf{q}\,\varphi)\wedge\varphi\supset!\,\{x\}\,(y)\wedge\{x\}\,(y)\,\mathbf{q}\,\varphi)\,.$$

Now the formula $x\mathbf{q}\varphi$ in general is not almost negative.

Lemma 7.1. *Claims of Lemma 6.2 are completely fulfilled also for* q-*realizability with addition of* $\mathrm{HT}_0+\mathrm{SA}^e\vdash\chi\supset!\,\tau_e[\chi]\mathbf{q}\chi$ *(for an almost Harrop formula* χ *and without* SA^e *for an U-Harrop formula* χ*).* □

Theorem 7.2. *All claims of Theorem 6.3 apart from statements on realizability of schemes* ECT *and* ECT_U *are fulfilled also for* q *realizability with the same terms.*

In the proof of this theorem Lemma 7.1 is used only for Σ_1- and Π_2-formulae θ by the proof of q-realizability of M and SA^e. □

Corollary 7.3. *If* $\mathrm{HT}_0+\mathrm{SA}^e(+\mathrm{M})\vdash\varphi(e\,,\bar{x})$, *where* e *is a new constant, then* $!\,t\,(e\,,\bar{x})\mathbf{q}\,\varphi(e\,,\bar{x})$ *is derivable in the same theory for some superposition* t *of signature functions, the* PRF $\nu^3\,(e,z\,,y)$ *and the constants* e. *Also if the first deduction was produced in* $\mathrm{HT}_0\,(+\mathrm{M}_U)$, *then the second one is the same, and the term* t *can be taken to be a signature one in this case.* □

Corollary 7.4 (on constructivity).

(a) *If the implication* $\chi\,(e\,,\bar{x})\supset\exists y\varphi(e\,,\bar{x}\,,y)$ *with an almost Harrop premise is derivable in the theory* $\mathrm{HT}_0+\mathrm{SA}^e\,(+\mathrm{M})$, *then in the same theory is derivable the implication* $\chi(e,\bar{x})\supset!t(e,\bar{x})\wedge\varphi\,(e\,,\bar{x}\,,t\,(e\,,\bar{x}))$ *for some* PRT t *of form same to that in Corollary 6.5.*

(b) *Theories* HT_0 *and* $\mathrm{HT}_0+\mathrm{M}_U$ *are (polynomially* $\exists$*)-constructive.*

Proof. (a) On the basis of Corollary 7.3 we get a deduction in $\mathrm{HT}_0+\mathrm{SA}^e\,(+\mathrm{M})$ } of formulae of the form

$$w\mathbf{q}\chi\,(e,\bar{x})\wedge\chi\,(e,\bar{x})\supset\mathbf{q}\,\varphi\,(e\,,\bar{x}\,,\{\tilde{t}(e,\bar{x})\}\,(w))\wedge\varphi(e\,,\bar{x}\,,\,\{\tilde{t}\,(e\,,\bar{x})\,\}\,(w))\,.$$

Hence Lemma 7.1 gives the needed $\chi(e\,,\bar{x})\supset\varphi\,(e\,,\bar{x}\,,\{\tilde{t}(e\,,\bar{x})\}\,(\tau_e[\chi(e\,,\bar{x})]))$.

(b) The proof is similar to (b) from Corollary 6.5.

Theorems 7.5 and 7.6 below show that the problem on (polynomial $\exists$)-constructivity of the theory $\mathrm{HT}_0+\mathrm{M}$ has a solution which is, however, somewhat different to that , for example, for the theory $\mathrm{HT}_0+\mathrm{ECT}_U+\mathrm{M}=\mathrm{HT}_0+\mathrm{ECT}+\mathrm{M}$; constructivity properties of the last theory are equivalent to that of its $\exists$-constructivity (and also to P=NP; see Theorem 6.10).

Theorem 7.5. *Constructivity of the theory* HT_0+M *is equivalent to the equality* P=NP.

Proof. From the constructivity of the theory HT_0+M which contains a special case of the Markov principle $\neg\forall y\neg x\,[y]\supset\exists y.x\,[y]$ follows the derivability in the same theory and hence in the theory T_0 of the formula of the form $x[y]\supset!\,t(x)\wedge x[t(x)]$, where the PRT $t(x)$ is dependable only on the variable x. By Proposition 2.2 the time of computation of the value $t(x)$ can be assumed to be polynomial. This trivially leads to P=NP.

Conversely, from equality P=NP by Proposition 3.3 it follows that the principle M is reducible to the principle M_U, and so by Corollary 7.4(b) we get the constructivity of $HT_0 + M$

Theorem 7.6. *The theory* $HT_0 + M$ *is polynomially* $\exists$*-constructive.*

Let us first formulate a natural generalization of the theorem on *elimination* of cuts [2,22] , the proof of which coincides in many points with the proof of its ordinary ungeneralized variant (see [25] for example); instead of LK- or LJ-proofs containing the single cut one should consider regular [25] proofs containing a unique "bad" cut; also to the block 2.1.2 from the proof in [25] an non-trivial case of the cut J_2 is added). (Notice that in the author's review [26] of [22] (but not in [2,22]) a false (too strong) formulation of the generalized theorem on cuts elimination is provided.)

Theorem 7.7. *From every proof in the Gentzen propositional calculi* LK *or* LJ *enriched by some collection of initial sequences (apart from ordinary ones of the form* $\varphi \to \varphi$*) closed under operations of substitution of terms instead of variables, it is possible to eliminate all cuts except for possibly cuts on formulae encountered in new initial sequences. The proof constructed can be considered as a regular one.*

Proof of Theorem 7.6. In accordance to the generalized theorem on the elimination of cuts every proof in the theory $HT_0 + M$ based on the intuitionistic propositional calculus LJ [25], where M is presented in sequential form $\neg\neg\exists x\alpha \to \exists x\alpha$, can be reconstructed into the proof without "bad" cuts; i.e., with cuts only on formulae of the form α , $\exists x\alpha$ or $\neg\neg\exists x\alpha$ with a quantifier-free α. Thus let us suppose that the sequence $\Gamma \to \exists y\varphi(y)$ is derivable in $HT_0 + M$ without use of bad cuts, where the list Γ consists of formulae α , $\exists x\alpha$ or $\neg\neg\exists x\alpha$ with a quantifier-free α . We shall use induction on proof to show that then the sequence of the form $\Gamma' \to \varphi(t)$ is also derivable, where t is a signature term and Γ' is constructed from Γ by elimination of all quantifiers $\exists$ and $\neg\neg\exists$. (Thus the list Γ' consists of quantifier-free formulae only).

If $\Gamma \to \exists y\varphi(y)$ is an initial sequence , i.e. a special case of the Markov principle $\neg\neg\exists y\varphi \to \exists y\varphi$ (with a quantifier-free φ), then we can take y for t by trivial derivability of the sequence $\varphi \to \varphi$. Otherwise, $\Gamma \to \exists y\varphi(y)$ is obtained by one of the following rules

$(\to\exists)$ $$\frac{\Gamma \to \varphi(t)}{\Gamma \to \exists y\varphi(y)} .$$

Here the sequence required is $\Gamma' \to \varphi(t)$. It is proved (using a cut) from the premise and from trivial sequences of the form $\alpha(x) \to \exists x\alpha(x)$, $\alpha(x) \to \neg\neg\exists x\alpha(x)$ conclusions of which are in Γ

(right weakening) $$\frac{\Gamma \to}{|\Gamma \to \exists y\varphi(y)} .$$

In this case (as well as in the case $(\to\exists)$) the sequence $\Gamma' \to$ is derivable just as in the previous case and so is the sequence $\Gamma' \to \varphi(t)$; for arbitrary t

(cut) $$\frac{\Pi \to (\neg\neg)\exists x\alpha(x)(\neg\neg)\exists x\alpha(x) , \Delta \to \exists y\varphi(y)}{\Pi, \Delta \to \exists y\varphi(y)} .$$

Here $\Gamma = \Pi , \Delta$ and by the inductive assumption we can suppose that $\alpha(x)$, $\Delta' \to \varphi(r(x))$ is derivable for some term $r(x)$. As the theory $HT_0 + M$ forms the fragment of the classical theory (namely of T_0) and the sequence $\Pi' \to \exists x\alpha(x)$, with quantifier-free formulae Π' , α is classically derivable in it, we can use the Herbrand theorem to justify the derivability of the sequence $\Pi' \to \alpha(s_1) \vee \ldots \vee \alpha(s_k)$ and thus of the sequence $\Pi' \to \alpha(s)$ for some terms $s_1 , \ldots , s_k , s$. Hence with the help of a cut on $\alpha(s)$ and substituting

s instead of x into the sequence $\alpha(x), \Delta' \to \varphi(r(x))$ being derived, we get the proof of the sequence $\Pi', \Delta' \to \varphi(r(s))$ and put $t = r(s)$.

$$(\exists \to) \qquad \frac{\alpha(x), \Gamma \to \exists y\varphi(y)}{\exists x\alpha(x), \Gamma \to \exists y\varphi(y)}.$$

In this case the proof of the sequence $\alpha(x), \Gamma' \to \varphi(t)$, which exists by the inductive assumption, is the one needed.

$$(\supset \to) \qquad \frac{\Gamma_1 \to \alpha_1 \alpha_2, \Gamma_2 \to \exists y\varphi(y)}{\alpha_1 \supset \alpha_2, \Gamma_1, \Gamma_2 \to \exists y\varphi(y)}.$$

Here the term t, which exists by inductive assumption for the right premise, also suits the conclusion and the proof of the sequence $\alpha_1 \supset \alpha_2, \Gamma'_1, \Gamma'_2 \to \varphi(t)$ is constructed from proofs $\Gamma'_1 \to \alpha_1$ and $\alpha_2, \Gamma'_2 \to \varphi(t)$ by use of the same rule ($\supset \to$).

$$(\wedge \to) \qquad \frac{\alpha_1, \Gamma \to \exists y\varphi(y)}{\alpha_1 \wedge \alpha_2, \Gamma \to \exists y\varphi(y)}.$$

This is similar to the above.

$$(\vee \to) \qquad \frac{\alpha_1, \Gamma \to \exists y\varphi(y)\, \alpha_2, \Gamma \to \exists y\varphi(y)}{\alpha_1 \vee \alpha_2, \Gamma \to \exists y\varphi(y)}.$$

By the inductive assumption there exist corresponding terms t_1 and t_2 for upper sequences. As both α_1 and α_2 are quantifier-free here, we can take the term IF α_1 THEN t_1 ELSE t_2 for t. Remaining cases of transposition and reduction weakening rules are even simpler.

§ 8. APPENDIX

1. Connection with the Kolmogorov complexity theory

The partition of finite objects into constructive and non-constructive and simple and complex ones which is considered in this article was introduced in [2] on the basis of the polynomially optimal unary coding ξ_i. It was shown above that we are led to such a partition by the partially recursive coding $\{B_i\}$. Such definitions are connected with the notion of the Kolmogorov complexity of finite objects in the following way.

At first notice that we define the PRF $\{x\}$ in such a way that it should be (Kolmogorov) additively optimal. This means that every other partially recursive coding $\{e\}(x)$ is reducible to the given coding $\{x\}$ with the code length growth for x of no more then on (additive) constant: $\{e\}(x) \cong \{e * x\}$, where $|e * x| \le |x| + \mathrm{const}_e$, $(= |x| + 2|e|)$.

We call a binary word y *Kolmogorov simple*, if it has a description x by an additively optimal algorithm which is substantially shorter than that for the word y itself; i.e., $y = \{x\}$ and $|x| << |y|$ using a kind of informal notation. Notice that in the framework of traditional perception of finite such definition is not rigorous and it is not clear how it could be improved to be independent from the slight variations of additively optimal coding and so on , while still really partitioning sets of binary words into two classes. Of course, the Kolmogorov approach is somewhat different, mathematically correct and "machine-independent". But it is based on the transition to infinity, i.e. on asymptotic terms.

In the case of the exponential-free mathematics (e.g., in theories $\mathrm{T}_0, \mathrm{T}, \mathrm{HT}_0$, and so on) it appears possible to make this very definition more precise . For example, constructive words of the form ξ_i or $\{B_i\}$ can be characterized in a natural way as *Kolmogorov logarithmically simple* because lengths of codes B_i of such words (in additively optimal coding) are logarithms from all possible lengths in "exponential-free universe" of finite objects. It is also possible to define the Kolmogorov simplicity of the word y in another sense if it has a code $x, y = \{x\}$ such that the integral part of the fraction $|y| / |x|$ is a long unary word; i.e., doesn't have a form $|B_i|$. Notice that here definitions have precise (and non-degenerate) meaning while in our theories words of the form $|B_i|$ are generally not all possible unary words.

2. Proof of Proposition 2.1(b)

At first the linear induction is derived from the lexicographical one as from $\forall x(\varphi(|x|) \supset \varphi(|x1|))$ it follows $\forall x(\varphi(|x|) \supset \varphi(|x'|))$ by the quantifier-free axiom $|x'| = |x| \vee |x'| = |x1|$ and the rule of the excluded middle for quantifier- free formulae. Conversely; the lexicographical induction is derived from the linear one in the quantifier-free case as in the proof of Proposition 2.1(a). In the case of the limited induction formula let us represent the lexicographical induction in the form

$$\forall x(\varphi(x) \supset \varphi(x')) \supset \forall m \forall n \le m \forall x, y \le 1^m (|y| = m - n \wedge |x| = n \wedge \varphi(y0^n) \supset \varphi(yx)),$$

where φ is a limited formula and variables m, n run through unary words (notice that the inequality $y \le 1^m$ is trivially equivalent to $|y| \le m$). Let us derive the conclusion of the implication from the premise with the help of the limited induction on the unary argument n. The case $n = \varnothing$ is trivial. Let us prove the inductive step from n to $n+1$. Let $|y| = m - n - 1$, $|x| = n + 1$, $\varphi(y00^n)$. We need to show that $\varphi(yv)$ holds for each word v of the length $n+1$.

By the inductive assumption for each z of the length n we have $\varphi(y0z)$ and $\varphi(y01^n)$ in particular. Passing to the lexicographically next word, we get $\varphi(y10^n)$. Again by the inductive assumption, we have $\varphi(y1z)$ for each z of the length n. Thus we have proved that for each $v(= 0z$ or $= 1z$ of the length $n+1$ we have $\varphi(yv)$. Q.E.D.

One can see that in this proof we have used only finite number of axiom schemes of the theory HT_φ. When the appropriate finite basis for polynomially computable functions and predicates and finite number of corresponding quantifier-free axioms of the theory HT_φ (which are defining inductively basic functions and predicates) are chosen, such schemes follow from one scheme of the limited linear induction.

3. On realizability of bounded ~~limited~~ induction

Regrettably, one can not strengthen basic results of this paper (for example, on underivability of the lower exponential bound for search algorithms) substituting HT_0 for HT_φ − a limited induction, for example, in the form of

$$\varphi(\varnothing) \wedge \forall i(\varphi(i) \supset \varphi(i+1)) \supset \forall i \varphi(i),$$

where φ contains only limited quantifiers and i is a variable on unary words (natural numbers). For this purpose, one should have constructed a realization e_φ of this scheme and prove that e_φ is indeed a realization using only limited induction. The only thing that could be done is to take an ordinary realization of a total induction scheme as e, i.e., with a fully arbitrary induction formula φ. Such realization e is independent of φ and is defined by the system of equations

$$\{\{e\}(<x, y>)\}(0) \simeq x,$$

$$\{\{e\}(<x,y>)\}(i+1) \cong \{\{y\}(i)\}(\{\{e\}(<x,y>)\}(i)),$$

i.e. essentially with the help of *primitive recursion*. To assure that e will really be a realization one should prove that the operator e on realizations

$$\{\{e\}(<x,y>)\}(i+1) \cong \{\{y\}(i)\}(\{\{e\}(<x,y>)\}(i)$$

and y gives everywhere defined function on i. This, however, can be done only for theories in which the primitive recursion operator is legitimate and thus the exponential, the iteration of exponential, and other similar primitive-recursive functions are feasible.

References

1. SAZONOV V. Yu. (1987) The equivalence of polynomial constructivity of the Markov principle to equality P=NP. *19th All-Union Algebraic Conference, Lvov, (Thesis),* part 2, 250-251 (Russian).

2.* SAZONOV V. Yu. (1980) A logical approach to the problem "P=NP?" *Math. Found. of Computer Sci.: Proc / 9th Symp. Rydzyna, Poland* . Berlin etc., Springer, 562-575 (Lecture Notes in Computer Sci.; 88).

3. SAZONOV V. Yu. (1981) On existence of complete predicate calculus in metamathematics without exponentiation *Math. Found. of Computer Sci.: Proc / 10th Symp. Strbske Pleso, Czechoslovakia.* . Berlin a.o., Springer, 483-490 (Lecture Notes in Computer Sci., 118).

4. HARY M., JONSON D. (1979) *Computers and Interactability. A Guide to the Theory of NP-Completeness.* San Fransisco.

5. BUSS S.R. (1986) *Bounded Arithmetic.* Bibliopolis (Studies in Proof Theory. Lecture Notes).

6. NELSON E. (1986) *Predicative Arithmetic.* Princeton, New Jersey: Princeton University Press, (Mathematical Notices, 32.)

7. SAZONOV V. Yu. (1980) Polynomial computability and recursivity in finite domains *Electronische Informationsverarbeitung und Kybernetik,* v.16, N7, 319-323.

8. SAZONOV V. Yu. (1985) Bounded set theory and polynomial computability. *All-Union conference on Applied Logic,* Novosibirsk, Oct. Thesis, 188-191 (Russian).

9. SAZONOV V. Yu. (1987) Bounded set theory, polynomial complexity and Δ-programming. (Computational Systems) *Applied Aspects of Mathematical Logic,* Novosibirsk, v.122, 10-131. (Russian)

10. GUREVICH Y. (1983) Algebras of feasible functions. *Proc. 24th IEEE Conf. on Found. of Computer Sci.* Tucson. 210-214.

11. MOSTOWSKI A. (1956) Concerning a problem of H.Sholz. *Z. math. Log. und Grundl. Math.*., N3, 210-214.

12. LIVCHACK A. B. (1982) The language of polynomial inquiries. *Computer - aided Computation and Optimization of Heat Technics.* Sverdlovsk. 41. (Russian)

13. IMMERMAN N. (1982) Relational queries computable in polynomial time. *14th ACM Symp. on Theory of Computing,* San-Francisco. 147-152.

14. VARDI M. (1982) Complexity of relational query languages. *Ibid.* 137-146.

[*] An important correction for this paper is given in [3, p.490].

15. FAGIN R. (1974) Generalized first order spectra and polynomial time recognizable sets. *Complexity of Computations. SIAM-AMS Proc.*, N7, 43-73.
16. MYCIELSKI J. (1981) Analysis without actual infinity *J.Symbol. Log.*, v.46, 625 - 633.
17. DRAGALIN A. G. (1979) Mathematical Intuitionism. *Introduction to the Proof Theory.* Moscow, Nauka, (Russian).
18. TROELSTRA A. S. (1977) Aspects of constructive mathematics. *In: Handbook of Mathematical Logic,* North-Holland, Amsterdam.
19. GÖDEL K. (1958) Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes. Princeton. *Dialectica,* v.12, N3/4, 280-207.
20. HOWARD W. A. (1980) The formulae-as-types notion of construction. *To H.B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism.* London: Acad. Press, 479-490.
21. BERMAN P. Review on [2] *Math. Reviews* 83j: 68055.
22. SAZONOV V. Yu. The collection principle and existence quantifier. *Logical-Mathematical Problems of MOS (Computational Systems).* Novosibirsk v.107 (Russian).
23. PARIKH R. (1971) Existence and feasibility in arithmetic *J. Symbol. Log.*, v.36, 494 -508.
24. LEVIN L. A. (1973) Universal problems of exhaustive search. *Problems of Information Transfer,* v.9, N3, 115-116 (Russian).
25. TAKEUTI G. (1975) *Proof Theory.* North-Holland, Amsterdam - London.
26. SAZONOV V. Yu. Author's review of [22]. - *Zbl. Math.* 605, 03022.
27. ZVONKIN A. K., LEVIN L. A. (1970) Complexity of finite objects and foundation of notions of information and probability by means of algorithm theory. *Uspekhi Mat. Nauk,* v.25, N6, 85-127 (Russian).

Translated by A.S.Morozov and A.A.Maltsev