On Feasible Numbers*

Vladimir Yu. Sazonov

Program Systems Institute of Russian Academy of Sciences,
Pereslavl-Zalessky, 152140, Russia.
e-mail: sazonov@logic.botik.yaroslavl.su

Abstract. A formal approach to *feasible numbers,* as well as to *middle* and *small* numbers, is introduced, based on ideas of Parikh (1971) and improving his formalization. The "vague" set F of feasible numbers intuitively satisfies the axioms $0 \in F$, $F+1 \subseteq F$ and $2^{1000} \notin F$, where the latter is stronger than a condition considered by Parikh, and seems to be treated rigorously here for the first time. Our technical considerations, though quite simple, have some unusual consequences. A discussion of methodological questions and of relevance to the foundations of mathematics and of computer science is an essential part of the paper.

1 Introduction

How to formalize the intuitive notion of *feasible numbers*? To see what feasible numbers are, let us start by counting: 0,1,2,3, and so on. At this point, A.S. Yesenin-Volpin (in his "Analysis of potential feasibility", 1959) asks: *"What does this 'and so on' mean?" "Up to what extent 'and so on'?"* And he answers: *"Up to exhaustion!"* Note that by cosmological constraints exhaustion must occur somewhat before, say, 2^{1000}, which is larger than the number of electrons in the universe! In a stricter sense, 2^{100} might also be viewed as non-feasible, but $2^{10} = 1024$ is surely feasible. The problem is that we cannot imagine any universally accepted border point between feasible and non-feasible numbers, seemingly precluding a systematic mathematical study of feasibility. Our aim here is to show that, quite to the contrary, feasibility is a notion that can be captured and analyzed by precise mathematical means.

> Nevertheless, according to quite a different approach a formal border point between "feasible" and "non-feasible" may be postulated to exist. We just *reject the abstraction of potential feasibility* in another way. We could postulate the existence of some *resource bounds* which always appear in practice and should not be neglected, as usually, but *explicitly taken into our consideration*, say, as parameters. This leads us to the idea of a finite row of natural numbers with the largest number (symbolizing the incidental resource bound), which may be denoted like zero as $\Box$. It proves that recursion theory relativized to such a finite row of

* Supported by Russian Basic Research Foundation (project 93-011-16016). This paper is an extended version of the abstract (Sazonov 1992).

> natural numbers is essentially the theory of polynomial-time computability (Sazonov 1980), (Gurevich 1983), (Immerman 1982), (Vardi 1982). Then we may consider the corresponding version of Peano Arithmetic in $\{0, 1, \ldots, \Box - 1, \Box\}$ with two constants 0 and $\Box$ and the ordinary induction schema, etc. (Sazonov 1980a, 1989). Moreover, it makes sense to fix the value of $\Box$ to be equal, say, to 8 (the case of the chess-board 8×8). However, in this paper we will treat the "negation" of the abstraction of potential feasibility somewhat differently, without postulating any maximal (feasible) natural number.

So, if we denote the "vague" or "fuzzy" set of feasible numbers as F then we should postulate that $0 \in F$, $F+1 \subseteq F$ and $2^{1000} \notin F$ according to our intuition. However, it seems that Traditional Mathematics (both classical and intuitionistic) does not allow considering such postulates as consistent ones. Also, the approach of A.S.Yesenin-Volpin (which is sometimes called "ultraintuitionism" or "ultrafinitism", "actualism" (Troelstra 1990)) being very suggestive, appears too informal.

Troelstra and van Dalen (1988) also wrote on feasibility notion the following. "Natural numbers are usually regarded as unproblematic from a constructive point of view; they correspond to very simple mental constructions: start thinking of an abstract unit, think of another unit distinct from the first one and consider the combination ("think them together"). The indefinite repetition of this process generates the collection N of natural numbers. It should be pointed out that already here an element of idealization enters. We regard 5, 1000 and $10^{10^{10}}$ as objects of "the same sort" though our mental picture in each of these cases is different: we can grasp "five" immediately as a collection of units, while on the other hand $10^{10^{10}}$ can only be handled *via* the notion of exponentiation; 1000 represent an intermediate case. Visualizing $10^{10^{10}}$ as a sequence of units is out of the question. Exponentiation as an always performable *operation* on the natural numbers involves a more abstract idea than is given with the generation of N. $< \ldots >$ There are considerable obstacles to overcome for a coherent and systematic development of ultra-finitism, and in our opinion no satisfactory development exists at present." (p.5–6.) "... certainly we have much less difficulty managing the idealized concept of the natural numbers, even though it is highly sophisticated one." (p.832.) "On the other hand, intuitionistically we do accept that "in principle" we can view $10^{10^{10}}$ as a sequence of units (i.e. we reject the ultrafinitist objection), and the authors are not sure that this is really less serious than the platonist extrapolation. At least it needs arguments." (p.851.) Also Borel (1947) mentioned that "the very large finite offers the same difficulties as the infinite".

Another informal consideration of feasibility notion was given in a popular lecture of A.N.Kolmogorov (1979) whose idea of *middle* and *small* numbers is formally developed in this paper.

A rigorous mathematical approach to feasibility was suggested by R.Parikh (1971) and developed further by other authors (V.P.Orevkov (1979), R.O.Gandy (1982), A.G.Dragalin (1985)). As Professor Gandy noted to the author, R.Parikh was the first who showed that feasibility indeed can be treated as mathematically coherent notion. However, the reason for writing the present paper is that his very interesting formalization of feasibility notion appears not to be completely adequate.

R.Parikh considered the ordinary Peano Arithmetic PA (in the language of primitive recursive functions) augmented with a new unary predicate F (which should not occur in the Induction Schema of PA!) and new axioms like the following:

$$0 \in F, \quad 1 \in F, \quad (x \in F \& y \in F \Rightarrow x + y \in F \& x \cdot y \in F \& \forall z \leq x (z \in F)),$$

and, most important,

$$2_{2^{1000}} \notin F.$$

Here it is defined by primitive recursion $2_0 := 1$ and $2_{k+1} := 2^{2_k}$ (and more generally, $2_0^x := x$, $2_{k+1}^x := 2^{2_k^x} = 2_k^{2^x}$; $2_k^x = 2^{\cdot^{\cdot^{2^x}}}$, k times "2"). So, $2_{2^{1000}}$ denotes a huge value of exponential tower of 2^{1000} number of stages. The resulting theory PA_F was proved in (Parikh 1971) to be practically (or feasibly) consistent in the sense that every formal proof of a contradiction in this theory should contain at least 2^{1000} symbols.

> More exactly, it follows from Parikh's theorems $2.2a$ and $2.2b$ (Parikh 1971) that in any tree-like Hilbert-style proof in PA_F of the contradiction $0 = 1$ the number of logical axioms $A(t) \Rightarrow \exists x A(x)$ containing F or their quantifier complexity or the number of new F-axioms involved should be $> 2^{990}$.

This metamathematical statement is proved in the ordinary mathematical manner (roughly speaking, in the framework of Zermelo-Frenkel set theory or the like) and is based on Hilbert and Ackermann's ϵ-symbol elimination technique. In fact, R.Parikh and other authors (using also the cut-elimination technique) are concerned rather with obtaining complexity estimates for some proof parameters. However, we prefer to stress on reasonable concrete values of these parameters. We believe that, e.g. 2^{990} or even 2^{100} are non-feasible numbers and 1000 is feasible one in some *absolute* sense. So, their feasibility/non-feasibility does not depend on any computer technology. (Otherwise the parametric approach would be indeed the most reasonable.) That is why we will often use "finite"/"infinite" instead of "feasible"/"non-feasible". We also call such numbers as 2^{1000} as "imaginary finite" or simply "imaginary" or even as "infinite".

The number $2_{2^{1000}}$ is too rough upper bound for feasible numbers and without essential changes of the above approach we cannot replace such upper bound in the last axiom of R.Parikh by 2^{1000} or even by 2_{1000} (where $2^{1000} \ll 2_{1000} \ll 2_{2^{1000}}$). In fact, we can argue (by using the material of the next section) that provability of $2_{1000} \in F$ is in some exact sense inevitable here. So, even the intuitively true axiom $2_{1000} \notin F$ would be *contradictory* in PA_F. This means that Parikh's upper bound $2_{2^{1000}}$ for feasible numbers was sufficiently exact for the concrete formalism he used. Simultaneously, this witnesses that his theory (together with its underlying logic) is not completely adequate as a theory of feasible numbers. It is rather a first satisfactory approximation.

This paper is devoted to perform some further step to overcome this difficulty. It consists in finding suitable restriction on the underlying predicate calculus considered as Logic of Mathematics and in arguing that this restriction (probably[2]) does not crucially destroy our ability to develop mathematical knowledge. Moreover, this allows to consider even the feasible number 1000 as infinite in a suitable sense (cf. Vopenka's notion of "witnessed universe" (Vopenka 1979)). This restriction on logic (in its strongest form) proves to be quite simple. Its main clause has been well known for a long time but was not considered immediately in connection with feasible numbers. It consists just in *rejecting the cut rule* or, equivalently, in *allowing only normal natural deductions* in developing Mathematics. The basic aim of this paper is to demonstrate the adequacy of such a restriction. We also suggest some other more liberal and still adequate restriction.

Note, that there is a more rough approach to feasibility which also was initiated by R. Parikh (1971). Here only $\exists n(2^n = \infty)$ may be postulated, rather than $2^{1000} = \infty$. There were many corresponding works on Bounded Arithmetic where exponentiation is not a provably total function. In addition to abovementioned (Sazonov 1980a, 1989) we refer to (Buss 1986), (Nelson 1986) and to more recent books (Hájek and Pudlák 1993) and (Krajíček 1995) for further details and the literature.

The complexity theorists know very well that there is an essential difference between, say, binary and unary notation systems for natural numbers. So, the (imaginary) number 2^{1000} in binary notation has a quite feasible form $100\ldots0$ (only thousand zeros), but its unary representation $111\ldots11$ is non-feasible, which corresponds to our intuition about this number. That is why we prefer (not for practical aims) unary notation system which also properly reflects the counting process. It is very good that we also have binary, decimal and other number systems which allows to considerably abbreviate "unary" numbers. But this does not mean that e.g. each (feasible in length) binary string like $100\ldots0$ denotes some (feasible) number. Nonetheless, the tradition is so strong that even in Bounded Arithmetic the abbreviations of natural numbers are identified with the numbers themselves. This theory is Arithmetic only by the form of its axioms. Actually it proves to be a theory of binary strings. On the other hand, Peano and Primitive Recursive Arithmetic completely neglect any such distinctions because they are too strong and rough for this.

2 Why Consider Feasible Numbers?

Let us first ask the counter-question: *Why consider non-feasible numbers*? It seems that there is no need in Mathematics and in Applied Mathematics to spe-

[2] Note, that we consider this paper as a reassuring experiment, a reasonable step, but not as a final truth.

cially introduce them. Rather, such unrealistic things as non-feasible numbers or non-measurable sets, or the possibility "to make two apples from one which have the same form" (due to the Choice Axiom in Set Theory) etc. are *undesirable side effects* of various formal techniques. We prove by the Mathematical Induction that function 2^x is total. However, the computational practice shows that it is actually partial ($2^{1000} = \infty$)! This is an interesting and actually well known (in Science and in every-day life) strange effect when we immediately *see* something as "black" but nevertheless *think* (for a technical convenience, by a habit or for some other reasons) that it is "white".

Another principle which is postulated in Mathematics and Logic, despite its "false" consequences, is the transitivity of implication. For example, we may argue that the implication is not transitive in some real situations such as the following one: if somebody is a baby today then he will be a baby one month later, but after one hundred months he will be surely not a baby. Hence, one hundred applications of the transitivity of implication fail in this case.

It seems that the reason for such approaches to develop Mathematics which contradict to our ground intuition and experience is in neglecting the corresponding "vague" notions "feasible"/"non-feasible", "big"/"small", etc. as non-mathematical ones. Also the resulting ordinary working apparatus proves to be still extreemly successful, sufficient and adequate in many *other* important respects. However, why should we consider these traditional approaches as the best or the unique possible ones?

Note that the ordinary Complexity Theory also deals with feasibility problems. Therefore, for completeness' sake this important comparatively-quantitative approach to algorithms theory might be deliberately concerned also with *feasible numbers* (not just only with *feasible computations* of functions and predicates defined both on feasible and non-feasible arguments). Kolmogorov's Complexity Theory of Finite objects seems was sufficiently close to this idea. Probably its highest success in the *traditional* framework was the reason that this theory did not turn to feasibility considerations in a rigorous mathematical way.

Moreover, by the author's opinion feasible numbers could be the proper notion to set into the foundation of (Applied) Mathematics. This is simply another way to introduce complexity theoretic approach in Mathematics by reconsidering the initial fundamental notions. It seems that this could give more smooth connection of Mathematics with real computers. Also this is a different and hopefully more natural approach to so called "fuzzy" Mathematics as well as to (Feasibly) Constructive Mathematics. As is well known, the Ordinary Constructivism allows transformation of existence proofs to *potential* constructions of corresponding "existing" objects. In contrast, Feasible Constructivism should guarantee just feasible constructions of feasible objects.[3]

[3] There are also other approaches to Feasible Constructivism or, more precisely, to *Polynomial Constructivism* (Cook 1975), (Cook and Urquhart 1993), (Buss 1986), (Sazonov 1989) which are concerned with extracting from constructive existence proofs the corresponding polynomial-time constructions of possibly non-feasible (in the proper sense) finite objects.

Let us illustrate this on the following quasi-practical example. Consider a variation of the chess game which differs from the ordinary one essentially by allowing for whites and blacks to make just two moves of the pieces at once instead of one move. Let also the overall number of moves is bounded, say, by 100. Then we may easily prove that whites have a strategy which allows them at least not to lose the game. Indeed, otherwise they can move a knight forth-and-back after which blacks prove to be at the symmetrical position! Intuitively, it is clear that this proof of the existence of a strategy for whites is highly non-constructive. (For the ordinary chess game we have no proof at all!) On the other hand, from the point of view of the traditional constructivism we may potentially find (by successive trials) the required strategy for whites which may be considered even as a (huge) finite object of a bounded size. We believe that a Feasible Number Theory is a reasonable framework which will give a precise sense to the notion of Feasible Constructivity. Only then we could hope to prove the plausible hypothesis that there exists no feasibly-constructive proof for (the variation of or for the original) chess game that whites, say, have a winning or non-losing strategy.

If, nevertheless, whites do have an intuitively feasibly constructive strategy in any reasonable rigorous sense then this could be guaranteed just by a proof in a Feasibly Constructive Theory. Not only the ordinary Constructivism, but even Polynomial Constructivism mentioned in the above footnote can do nothing in this situation. It probably could work if we generalize 8×8 chess-board to $n \times n$ for sufficiently *large* n. However, what about 8×8?

3 Formal Systems Revised

What is (a proof in) a formal or an axiomatic system? It is necessary here to give a right answer to this question. The ordinary explanation of this notion is rather rough for our aim to formalize feasible numbers. We define a formal system e.g. as a finite set of rules $A_1 \dots A_k / A_{k+1}$ where A_i are some syntactically well formed (schemes of) formulas. However, we may consider finite (instances of the schematic) formulas A_i and their sequences (which are formal proofs according to the rules) in three ways:

1. as some *real* or *feasible* strings of symbols which may appear on a sheet of paper or in a computer memory,
2. as some *abstract*, imaginary finite strings which are considered only as *potentially-feasible*[4], or
3. *inside some mathematical (meta-) theory* (such as PA or ZF via a Gödel numbering or the like).

In the first two cases our intended subject is some axiomatized branch of Mathematics described by the given formal system and developed, respectively,

[4] As usual, this term does *not* mean something which *could be made feasible* in our sense. It rather allows to *think* about too long non-feasible strings which are considered as finite only by some sufficiently formal reasons or by an idealization.

in a *strictly* formal or *potentially* formal way. In the third case we are actually considering Metamathematics of the formal system, so making more precise the second case. (However, it may be asked, which way we prove metameta...mathematical results? Let us interrupt this infinite regress!) Of course, all these aspects are explicitly or implicitly involved in everyday mathematical activity. But the most essential point of this paper is that we should *not* mix them.

Let us consider for example the following first order theory T (regarded eventually as a finite list of formal axiom schemes and rules) of some weak arithmetic of natural numbers (even with *no* Induction Axiom at all). Non-logical symbols of T are one-place function symbol s for the successor operation $s(x) = x+1$ and three-place predicate symbol R with the meaning $R(x,y,z) \Leftrightarrow x + 2^y = z$. There are only two special axioms in T recursively defining R:

$$T: \begin{cases} R(x,0,sx) & (x+2^0 = x+1) \quad \text{and} \\ R(x,y,z)\&R(z,y,v) \Rightarrow R(x,sy,v) & (x+2^{y+1} = (x+2^y)+2^y). \end{cases}$$

Note, that T does not prove that $x+2^y$ is a total function, i.e. formally

$$T \nvdash \forall xy \exists z R(x,y,z).$$

Define the following sequence of formulas. $E_0(x) := x = x$; $E_{i+1}(x) := \exists y \in E_i.R(0,x,y)$ $(:= \exists y(E_i(y)\&R(0,x,y)) \Leftrightarrow$ "2^x is defined and $\in E_i$"). Hence $E_i(x)$ means that the value of 2^x_i is defined. Also take $N_0(x) := x = x$ and $N_{i+1}(x) := \forall y \in N_i \exists z \in N_i R(y,x,z)$ $(\Leftrightarrow \forall y \in N_i(y+2^x \in N_i))$.

Theorem. $T \vdash E_{1000}(0)$ *(i.e.* $T \vdash$ *"2_{1000} is a finite number").*

Proof. (Essentially due to V.P.Orevkov (1979); cf. also R.Statman (1978, 1979).) We first infer $N_i(0)$, $i = 0,1,2,\ldots$, in T. For $i = 0,1$ this is trivial. The case $N_{i+2}(0)$ is equivalent to proving the formula $\forall y \in N_{i+1}(y+1 \in N_{i+1})$ or equivalently $\forall y[\forall x \in N_i(x+2^y \in N_i) \Rightarrow \forall x \in N_i(x+2^{y+1} \in N_i)]$. But the latter follows from the second axiom of T.

Then we can prove $N_i \subseteq E_i$ in T by induction on $i = 0,1,2,\ldots$. The case $i = 0$ is trivial. To prove $N_{i+1} \subseteq E_{i+1}$ we take any $y \in N_{i+1}$, i.e. any y such that (2^y is finite and) N_i is closed under addition of 2^y, and apply it to $0 \in N_i$. This gives $2^y = 0 + 2^y \in N_i \subseteq E_i$ and hence $y \in E_{i+1}$, as required.

It follows step-by-step that all $E_i(0), i = 0,1,2,\ldots,1000$, are provable in T. □

We claim that there is something wrong in the above proof (which, however, seems very nice in itself). Indeed, what and how have been proved here? First of all, Mathematics and Metamathematics were mixed strongly. Even in the formulation of the theorem the expression $E_{1000}(0)$ is not a formula of our language but only a short denotation for some legitimate but rather long formula. ($E_i(x)$ contains exactly $3+13i$ symbols).

However, this is not the main difficulty with this proof. Of course, $E_{1000}(0)$ could be eventually written explicitly (13003 symbols are not so many). Much worse is the case with the (recursive) abbreviation N_{1000} which cannot be eliminated in practice because the intended formula of the original language evidently should contain $> 2^{1000}$ symbols. So, this direct attempt to make the proof rigorous i.e. to eliminate the Abstraction of Potential Feasibility, Metamathematics and other informal and illegal means does not succeed.

The conclusion is that the formula (denoted by) $E_{1000}(0)$ was not feasibly proved in T. We only proved that, potentially or metamathematically, there exists an *imaginary finite* proof of the formula $E_{1000}(0)$ in T. We cannot be completely satisfied by this metaproof of proof existence because we strongly believe that the *genuine* mathematical proof should be sufficiently short to be really written e.g. in a book.

A reasonable way of eliminating "meta" from metaproofs consists in extending the underlying predicate logic *to legitimate some formalism for required abbreviations*. This is a way to replace intuitive and metamathematical means by formal mathematical ones which we will adopt here[5]. Therefore we consider (some) abbreviation mechanisms, in general, as strong mathematical (rather than logical) tools.

Mathematical principles, in contrast to logical ones (as we understand them here), may have some special consequences about objects under consideration (e.g. the existence of very large numbers etc.). The above Theorem and especially considerations below show that some kinds of abbreviations indeed may have such consequences[6].

Of course, we cannot give the most general exhaustive mechanism for abbreviations to be used in Mathematics. This seems quite analogous to our inability to give a complete formalization of arithmetic or set theory. But we may introduce some useful and concrete such mechanisms[7]. Also we would not try to find abbreviations as strong as possible. Just as we choose some axioms and reject others in developing some branches of Mathematics, we will prefer only those most adequate abbreviation mechanisms which do not prevent us from formalizing the subject under consideration.

Remember that our present subject is feasible numbers. And the above theorem shows that theory T *together with all abbreviation mechanisms* used in it (both explicitly mentioned above and, even more important, implicit ones) is *non-adequate* for this aim: it proves that 2_{1000} is finite (what means here 'feasi-

[5] Another idea to introduce E_i and N_i, $i = 1 \dots 1000$, immediately in the language of T and to consider their definitions as a new axioms of T seems not very appropriate. We must not change a *given* theory and its language depending on theorems to be proved. Let us play in a game with fixed rules!

[6] In fact, the abbreviations E_i and N_i in the above theorem prove to be not so crucial in this respect. We concentrated on them just to show the role of abbreviations in the general notion of formal proof. Yet more important for us is some other kind of abbreviations which were used in the above theorem *implicitly*. They are discussed below.

[7] Actually, in this paper we only mention such-and-such abbreviation mechanisms without introducing them rigorously. What we *will* do here, is putting a formal *veto* on some such mechanisms.

ble'). However, intuitively even $2^{1000} < 2_{1000}$ should be infinite! Note, that this consideration on theory T may be repeated for Parikh's formalization PA_F of feasible numbers mentioned in the Introduction above. I.e. there exists a feasibly long proof in PA_F (with some kind of abbreviations used, as above) of $2_{1000} \in F$. It follows that Parikh's upper bound $2_{2_{1000}} \notin F$ cannot be strengthened even to $2_{1000} \notin F$ without essential reconsidering the whole approach. Note that no general restriction on abbreviating means of PA_F was imposed in (Parikh 1971) (except those rather technical requirements on proofs which we mentioned in the Introduction).

Abbreviations may be applied not only to formulas, but also to proofs. For example, in the above theorem the proof of $N_{i+1} \subseteq E_{i+1}$ was described using *recursively* its subproof of $N_i \subseteq E_i$, and without this the resulting proof of $N_{1000} \subseteq E_{1000}$ should be rather long (instead of a proof occupying only a quarter of page).

However, *the most crucial abbreviations* widely used in Mathematics *deal with terms and objects* (in comparison with formulas and proofs as above). Let us consider e.g. the simplest term abbreviation $2 \cdot x := x + x$. Then we may denote the number 2^{1000} as $2 \cdot 2 \cdot 2 \cdot \ldots \cdot 2 \cdot 1$ (thousand times '2'). This denotation, being rather long, is nevertheless quite feasible. However, it is impossible to really denote (even in a computer memory) such extraordinarily large number using only 1 and $+$, because this requires 2^{1000} occurrences of 1's. This suggests that *abbreviation of terms is not an appropriate tool if we want to formalize feasible numbers* (and thereby to exclude 2^{1000} from this numbers).

Note, that the ordinary formalizations of the predicate logic contain *implicitly* some kind of abbreviations of terms. In the case of the Natural Deduction Calculus (Prawitz 1965) we have the rules of introduction (I) and elimination (E) for each logical connective, for example for $\exists$:

$$\frac{A(t)}{\exists x A(x)}\ (\exists \mathrm{I}) \qquad \frac{\exists x A(x) \qquad \begin{array}{c}[A(x)]\\ \mathcal{D}\\ B\end{array}}{B}\ (\exists \mathrm{E})$$

where x is not free in B and in the open assumptions in $\mathcal{D}$, except $[A(x)]$, and quantification is understood up to proper renaming the quantified variable. So, the first rule *abbreviates* (possibly rather long[8]) *term t by the name x*. The second one *uses* the name x for some object satisfying A. If in a natural deduction some $\exists$-formula occurrence is both the conclusion of $\exists$I-rule and the main premise of $\exists$E-rule then x plays the role of an abbreviation of a term which is used in a deduction. We claim that these are such situations (likewise the abbreviation $2 \cdot x := x + x$) which give rise to non-feasible numbers and therefore they should be avoided. We will avoid analogous situations for other logical connectives as well: *introduced by an* I-*rule logical connective is not allowed to be eliminated by the corresponding* E-*rule*. The reason is that such subinference, for example,

[8] and even if not long, what about the iteration of such abbreviations?

$$\cfrac{\cfrac{A \quad B}{A\&B}\ (\&\mathrm{I})}{A}\ (\&\mathrm{E})$$

may lead to the above situation with existential quantification when the formula A is $\exists x\tilde{A}(x)$, its upper occurrence in the figure shown is the conclusion of some $\exists$I-rule and its lower occurrence is the main premise of $\exists$E-rule.

Slightly generalizing, this means that our restriction on proofs will consist in *allowing only normal natural deductions* (cf. the exact definition in (Prawitz 1965) and (Troelstra and van Dalen 1988)). In particular, this also means that we *can not freely use the general modus ponens rule* ($\Rightarrow$ E) with the corresponding rule ($\Rightarrow$ I)

$$\frac{A \quad A \Rightarrow B}{B}\ (\Rightarrow \mathrm{E}) \qquad \frac{\begin{array}{c}[A]\\ \vdots \\ B\end{array}}{A \Rightarrow B}\ (\Rightarrow \mathrm{I})$$

because the premise $A \Rightarrow B$ of the former could be introduced in the deduction by the latter so that the normality requirement fails (and again, as above, it may be considered the case when B is $\exists x\tilde{B}(x)$).

In this connection it is worth to remember an anticipating note in (Troelstra and van Dalen 1988): "The strictly finitist view also has its consequences for logic; the derivations of A and $A \Rightarrow B$ may still be within reach, but in order to apply modus ponens one might have to exceed the available natural numbers necessary for the length of the derivation of B." (p.29.)

Similarly, there is no guarantee that implication is transitive. This might seem very strange if we forget that our aim is to formalize such vague notion as feasible numbers or, say, Vopenka's notion of the *horizon* (Vopenka 1979) or the notion of *middle* or *intermediate numbers*. The latter notion could be considered as natural numbers counted before the horizon is "overcomed". Here $0, 1, 2, \ldots, 10, 11, \ldots$ are middle, 1000 and even 100 are definitely not middle (and lie "behind the horizon") and there is no maximal middle number. (Just look along a straight railway towards the horizon and count the pillars; see also the discussion in § 2 on non-transitivity of implication and § 4 below.)

Of course, every natural deduction can be (potentially!) normalized (Prawitz 1965). However, it is well known that this normalization (or cut elimination) process has *non-elementary lower (and upper) complexity bounds* (Orevkov 1979; Statman 1978, 1979). For example, consider the above proof of $E_{1000}(0)$ in the Natural Deduction form:

$$\cfrac{\begin{array}{c}\vdots\\ N_{1000}(0)\end{array} \quad \cfrac{\begin{array}{c}[N_{1000}(0)]\\ \vdots \\ E_{1000}(0)\end{array}}{N_{1000}(0) \Rightarrow E_{1000}(0)}\ (\Rightarrow \mathrm{I})}{E_{1000}(0)}\ (\Rightarrow \mathrm{E})$$

It is not normal[9] because the conclusion of ($\Rightarrow$ I)-rule is the main premise of ($\Rightarrow$ E)-rule. This proof cannot be normalized in practice. Indeed, every normal proof of the formula $E_{1000}(0)$ (which asserts the existence of the number 2_{1000}) will contain a term of the length $\geq 2_{1000}$ essentially due to the following form of

Herbrand's metatheorem. *Every normal classical deduction of $\exists$-formula $\exists\bar{z}C\bar{z}$ or $\neg\neg\exists$-formula $\neg\neg\exists\bar{z}C\bar{z}$ (possibly without $\exists$) from $\forall$- and $\neg\exists$-formulas of the kind $\forall\bar{x}A\bar{x}$ and $\neg\exists\bar{y}B\bar{y}$ can be reconstructed into quantifier-free normal deduction of some finite disjunction $\vee_i C\bar{t}_i$ from the formulas of the kind, respectively, $A\bar{t}$ and $\neg B\bar{s}$, and conversely. Moreover (*and most crucial*), in both directions the new deduction will contain only those terms which were occurring in the initial one.* □

Nevertheless, using abbreviations is extremely important tool of Mathematics. Therefore, it would be not very reasonable to reject all of them. That is why we summarize our *special requirements on mathematical proofs* by the following three rather informal clauses (except the clause 2):

1. **Arbitrary explicitly fixed abbreviation mechanisms for formulas and proofs, but not for terms are allowed.**
2. **Only normal proofs are allowed.**
3. **The number of symbols in a proof should be (intuitively) feasible.**

Of course, these requirements could be formulated more rigorously and also in a more strong or, on the contrary, in a more weak form. For example, in 3) 'feasible' could be strengthened by 'middle' or something such, because the genuine mathematical proofs should be *clear* and hence not only feasible, but also rather short.[10] However, it will be quite sufficient for the current aims and for simplicity sake to weaken our requirements as follows:

ONLY NORMAL PROOFS WITH FEASIBLE TERM SIZE ARE ALLOWED

Here *term size* of a proof is defined as the maximum of the number of symbols in each term occurrence in the proof. No restriction is imposed on the number of term occurrences and on the length of proofs and formulas in this final requirement. So, proofs and formulas, except terms, may be treated abstractly, as potentially feasible. This considerably simplifies the matter, and the resulting requirement on proofs naturally corresponds to the above three clauses. However, we believe that the ideal approach should be based on those clauses, probably with the technical rather strong restriction 2) replaced by some more liberal and hopefully more convenient one; cf. also § 5 below.

[9] and, in fact, uses abbreviations of terms via quantifier rules here not shown

[10] There are many examples when rather complicated mathematical proofs became very transparent and rather short after suitable reconsidering the presentation of the whole theory. After all, the main idea of any mathematically interesting proof is usually sufficiently simple.

Instead of the natural deduction we could formalize mathematical proofs by Gentzen's sequent calculus. In this case *the normal proofs may be equivalently replaced by cut-free ones*. However, we prefer natural deduction just because it is "natural" and our aim is, after all, to develop *Feasible Mathematics* with as minimum as possible extra technical efforts (which, however, are inevitable) connected with choosing any unnatural formalism for a real deducing theorems.

Let $\Gamma \vdash_f^n A$ mean that there exists some (possibly imaginary) *normal* classical first-order *natural deduction* (or *cut-free sequent deduction*) of A from Γ with intuitively *feasible term size*. To assert $\Gamma \vdash_f^n A$, it is sufficient to be able to really write down each term occurrence in the corresponding proof or even to be surely convinced that such a proof with short terms exists. $\Gamma \nvdash_f^n A$ will mean that there exists no such proof. We may be quite sure about this if, for example, we have some traditional meta-proof (in ZF or the like) that there is no required proof of the term size less than 2^{1000}. As an additional technical convention we will consider *the negation sign* $\neg$ *as definable one*:

$$\neg A := (A \Rightarrow \bot),$$

where $\bot$ is the primitive logical symbol denoting falsity with the ordinary *reductio ad absurdum* rule of inference (Prawitz 1965): $[\neg A] \ldots \bot / A$. In particular, we have the inference rule: $\bot$/everything. We will see below that this convention about negation plays an essential role in the consistency of a theory of feasible numbers FEAS defined in the next section.

It might be thought that the above notion of nf-proof is too vague due to the involved intuitive notion of feasible terms. However, the implicit use of the abstraction of potential feasibility of proofs in the ordinary approach to the notion of proof seems much more unclear. We believe that the only way of rigorous formalization of Mathematics is through feasible proofs (in various formal systems). On the contrary, the *potentially* feasible proofs in the *full* generality of this notion (if it has any sense at all) hardly can be considered as a genuine formal, i.e. mathematical one due to the "infinite regress" implicit in this notion.

> Note, that we are speaking here only about the formal and routine nature of mathematical proofs. How these proofs and corresponding formal systems are created is quite different question. Of course, this is usually extremely informal process. Nevertheless, any mathematical result should be presented in a sufficiently formal way. It is very important that the ordinary, not completely formal proofs in Mathematics usually can be transformed into feasibly formal ones (as the above proof of $E_{1000}(0)$) via explicating the necessary abbreviating mechanisms. The author's opinion is that it is this reason why any particular not very formal mathematical proof is actually considered by mathematical community as genuine mathematical one.

The reader might probably consider as a rather artificial the above normality requirement of proofs (taken simultaneously with the requirement on feasibility of term size). This also seems too strong restriction to the author himself. However note, that our aim was to find first *any* reasonable restriction which allows to formalize feasibility sufficiently adequately. On the other hand, we will present in § 5 some more liberal restriction on the predicate calculus which represents more directly our main idea that only terms must not be abbreviated. There may be also some other approaches and variations.

4 A Basic Theory of Feasible Numbers

The following theory, FEAS, is a point of departure for formalizing feasible numbers. The theory's non-logical symbols are $0, 1, +, \lfloor \log_2 \ldots \rfloor$ and $\leq$. Let FEAS_0 denote a collection of closed universal formulas (with terms of intuitively feasible length) which are feasibly true in an intuitive sense, such as $\forall x(x \neq x + 1 \neq 0)$, $\forall x \forall y \neq 0(x \leq \log_2 y \Rightarrow x + 1 \leq \log_2(y + y))$, $\log_2 1 = 0$ and, for definiteness, $\log_2 0 = 0$, i.e., several *ordinary* axioms. We will assume that this collection contains the feasibly true universal formulas that we need. Now define FEAS to be FEAS_0 extended with the *Main Axiom*

$$\forall y(\log_2 \log_2 y < \mathbf{10}),$$

that is, $2^{2^{10}} = 2^{1024} = \infty$; this too is a universal formula, and is intuitively *true for feasible numbers* (in a new natural sense respecting the old one). Those in doubt may wish to check this on a computer for various feasible y's represented in unary notation.

Now we assert the following facts about FEAS.

Fact 1. $\mathsf{FEAS} \nvdash^n_f \perp$.

This assertion holds because any normal proof of $\perp$ in FEAS involves a term which is too long to be physically written down or stored, namely, we have

Metatheorem for FEAS. *Every normal proof of $\perp$ in FEAS contains a term with $\geq 2^{1024}$ symbols.*

Proof. By Herbrand's Theorem, in the form presented in § 3, each universal axiom of FEAS that occurs in a normal proof of $\perp$ can by replaced by closed instances thereof. The value of each closed term in the language of FEAS is bounded by its size. Substitution instances of axioms, including the Main Axiom, would be true in the standard sense if all substituted terms were of length $<$ 2^{1024}. Therefore, true (in the standard sense) axioms would imply $\perp$, which is impossible. □

Another important corollary of Herbrand's Theorem is:

Fact 2. *The theory FEAS is a conservative extension of FEAS_0 with respect to closed quantifier-free and $(\neg\neg)\exists$-formulas. In fact, if a $(\neg\neg\exists)$-sentence has a proof in FEAS of term size $< 2^{1024}$, then it has a proof in FEAS_0 of the same term size.* □

This means that the two theories prove the same theorems about the terminaton of computations, that is, the kind of existential statements that is of greatest value in applications. Theorems of other forms, such as the Main Axiom $\forall y(\log_2 \log_2 y < \mathbf{10})$, are aimed at providing a reasonable abstract context for computations and algorithms (as in Hilbert's Program). Nonethelss, we have

Fact 3. $\mathsf{FEAS} + \forall x(f(x) = x + x) \vdash_f^n \bot$, *where f is a new function symbol for multiplication by two.* $\square$

Thus the practically consistent theory FEAS becomes inconsistent once a name for the doubling function is introduced. This example have been discussed in § 3 above. Note that term size of the proof in Fact 3 is ~ 1000 symbols. The details are left to the reader.

Let us define $M(x) :=$ "x is a *middle* (or *intermediate*) *number*" $:= \exists y \neq 0(x \leq \log_2 y)$ (here $y \neq 0$ is an inessential technical restriction to simplify one formal proof below) and $S(x) :=$ "x is a *small number*" $:= \exists y(x \leq \log_2 \log_2 y)$. Then, we have

Fact 4. $\mathsf{FEAS} \vdash_f^n S(\mathbf{0}),\ \neg S(\mathbf{10}),\ \exists x(S(x) \& \neg S(x+1)),\ M(\mathbf{0}),\ \neg M(\mathbf{1024}),$ $\forall x(M(x) \Rightarrow M(x+1)),\ \forall x \leq y(S(y) \Rightarrow S(x)),\ \forall x \leq y(M(y) \Rightarrow M(x))$ *and* $\forall x(S(x) \Rightarrow M(x))$.

Note that provability of $M(\mathbf{0}), \neg M(\mathbf{1024})$ and $\forall x(M(x) \Rightarrow M(x+1))$ gives no contradiction here. Indeed, the reader may see that the corresponding deduction

$$M(\mathbf{0}),\ M(\mathbf{0}) \Rightarrow M(\mathbf{1}),\ M(\mathbf{1}),\ M(\mathbf{1}) \Rightarrow M(\mathbf{2}),\ M(\mathbf{2}),\ \ldots,\ M(\mathbf{1024})$$

by multiple application of modus ponens rule is not normal one because $M(x) \Rightarrow M(x+1)$ is actually deduced by introduction of implication rule (see the proof below), so modus ponens is not allowed. Of course, we could try to normalize successive subinferences of $M(\mathbf{1})$, $M(\mathbf{2})$, etc. by hand or by computer. However, this enterprise will be successful only for some initial part of this sequence. Surely, even $M(\mathbf{50})$ will be never "normally" proved (with any abbreviations for formulas and proofs but not for terms).

Proof of Fact 4. The cases of $S(\mathbf{0})$ and $M(\mathbf{0})$ are trivial. $\neg S(\mathbf{10})$ and $\neg M(\mathbf{1024})$ easily follow from the axiom $\forall y(\log_2 \log_2 y < \mathbf{10})$. The proof of $\forall x(M(x) \Rightarrow M(x+1))$ uses the axiom on $\log_2$ by inferring first $M(x+1)$ from $M(x)$:

$$\dfrac{M(x) := \exists y \neq \mathbf{0}(x \leq \log_2 y) \quad \dfrac{\dfrac{\dfrac{[y \neq \mathbf{0} \& x \leq \log_2 y] \quad y \neq \mathbf{0} \& x \leq \log_2 y \Rightarrow x + 1 \leq \log_2(y+y)}{y + y \neq \mathbf{0} \& x + 1 \leq \log_2(y+y)}}{M(x+1) := \exists z \neq \mathbf{0}(x + 1 \leq \log_2 z)}}{}}{M(x+1)}\ .$$

Then $\forall x(M(x) \Rightarrow M(x+1))$ follows by introduction of implication and universal quantification.

Other cases are also easy except that of $\exists x(S(x)\&\neg S(x+1))$. To prove this we first write down the following natural deduction for several feasible numerals $\mathbf{n} = 0+1+1+\ldots+1$

$$\dfrac{[\neg\exists x(S(x)\&\neg S(x+1))]^4 \quad \dfrac{S(\mathbf{n}) \quad [\neg S(\mathbf{n+1})]^1}{\exists x(S(x)\&\neg S(x+1))}}{\dfrac{\bot}{S(\mathbf{n+1})}\;1}\;.$$

Using successively these inferences for $\mathbf{n} = \mathbf{0}, \mathbf{1}, \ldots, \mathbf{8}$, together with the evident proof of $S(\mathbf{0})$, and the natural deduction

$$\dfrac{\dfrac{\begin{matrix}\vdots\\ S(\mathbf{9})\end{matrix} \quad \dfrac{\dfrac{[S(\mathbf{10})]^3 \quad \dfrac{[\mathbf{10}\le \log_2\log_2 y]^2 \quad \dfrac{\forall y(\log_2\log_2 y < \mathbf{10})}{\log_2\log_2 y < \mathbf{10}}}{\bot}}{\bot}\;2}{\neg S(\mathbf{10})}\;3}{\exists x(S(x)\&\neg S(x+1))} \qquad [\neg\exists x(S(x)\&\neg S(x+1))]^4}{\dfrac{\bot}{\exists x(S(x)\&\neg S(x+1))}\;4}$$

we obtain the required normal proof with feasible term size. $\square$

Analogously, $\mathsf{FEAS} \vdash_f^n \exists x \in S \forall y \in S(y \le x)$. Note, that we can prove $\mathbf{0} \in S, \mathbf{1} \in S, \ldots, \mathbf{4} \in S$ where e.g. the last statement means that $2^{2^4} = 2^{16} < 10^5$ is a finite number. Much more difficult (if possible at all) it is to prove $\mathbf{5} \in S$ because $2^{2^5} = 2^{32} \sim 10^{10}$ is extremely large number. But $\mathbf{7}$ and even $\mathbf{6}$ are surely not in S because $2^{2^7} = 2^{128}$ and $2^{2^6} = 2^{64} = 16^{16} > 10^{16}$ are intuitively non-feasible (however less than 2^{1024}). It follows that intuitively the largest number in S is something like $\mathbf{4}$, or $\mathbf{5}$ and that $2^4 = 16 \in M$ but $2^6 = 64 \notin M$. These considerations also show that we could strengthen the main axiom of theory FEAS as $\forall y(\log_2\log_2 y < \mathbf{6})$ or even as $\forall y(\log_2\log_2 y < \mathbf{5})$. Such or other strong versions of feasibility axiom may depend on computer technology available today. However, we believe that the truth value (or, better to say, the role) of original feasibility axiom $\forall y(\log_2\log_2 y < \mathbf{10})$ does not depend on any technology.

We see that S and M have somewhat different properties. But the following fact shows that the story is much more intriguing. Simultaneously with the formula $\forall x(M(x) \Rightarrow M(x+1))$ we also have provable its negation:

Fact 5. $\mathsf{FEAS} \vdash_f^n \neg\forall x(M(x) \Rightarrow M(x+1))$.

Proof. The following deduction of $\bot$ in the theory $\mathsf{FEAS} + \forall x(M(x) \Rightarrow M(x+1))$ is normal (despite many applications of modus ponens which are evidently allowed for partial cases of the *hypothesis* $M(x) \Rightarrow M(x+1)$):

> $\{M(\mathbf{0}), (M(\mathbf{0}) \Rightarrow M(\mathbf{1})), M(\mathbf{1}), \ldots, M(\mathbf{1023}), (M(\mathbf{1023}) \Rightarrow M(\mathbf{1024})),$ $M(\mathbf{1024}) := \exists y(\mathbf{1024} \le \log_2 y)$, so, let $\mathbf{1024} \le \log_2 y$, but this contradicts to the axiom $\forall y(\log_2\log_2 y < \mathbf{10})$, i.e. $\bot$ is proved$\}$.

Hence, the rule ($\Rightarrow$ I) gives $\mathsf{FEAS} \vdash_f^n \neg\forall x(M(x) \Rightarrow M(x+1))$. □

We see that Facts 4 and 5 give $\mathsf{FEAS} \vdash_f^n A$ and $\mathsf{FEAS} \vdash_f^n \neg A$, for $A := \forall x(M(x) \Rightarrow M(x+1))$. But *this is not a contradiction* (cf. Fact 1). It follows only that the rule $A, \neg A/\bot$ is not always admissible, as well as the more general modus ponens (or cut) rule $A, A \Rightarrow B/B$ (because $\neg A$ is $A \Rightarrow \bot$). So, we should reconsider the question:

What is a Contradiction?

We adopt here the reasonable convention that a theory may be considered contradictory only if it is *trivial*, e.g. if all its well formed formulas (of feasible term size) are provable in our sense. Of course, FEAS is not such one. Nevertheless, the above unusual peculiarity of FEAS properly reflects the *contradictory nature* of such fuzzy notions as feasible and middle natural numbers. It is intuitively plausible that there exists no maximal middle number (e.g. the last month of our childhood) and, on the contrary, it is very strange to think that before 1000 there exists an "infinite" increasing sequence of natural numbers.

> The reader may remember also the related example of a picture on a computer display which looks simultaneously as *continuous and discrete*, and the reason for that is evidently just our mind, not an optical effect. The same holds for the physical continuum, because real numbers used in Physics have about 30 decimal digits after the point or, equivalently, about 100 (the intuitively non-middle number) of binary digits. So, there is the possibility to formalize real numbers as *infinite* sequences of binary digits so that each digit after the point will have the number *less* than 100 (or 1000). And the resulting continuum will be both continuous and discrete. Probably these finitary/infinitary ways of arguing could have some interesting effects if used simultaneously or mixed in one and the same proof. Also physical elementary particles which are considered both as particles and as waves may have some releavance to feasible numbers.

5 A More Liberal Approach

Let NK denote the classical calculus of natural deduction in the form of (Prawitz 1965). We will define below another restricted version NK^0 of the calculus NK whose inferences *do not use term abbreviations* in some more natural and not so restrictive sense than it was considered above. Deducibility in these calculi will be denoted, respectively, as $\Gamma \vdash^0 A$ and $\Gamma \vdash A$ where $\Gamma \vdash^0 A$ evidently must imply $\Gamma \vdash A$. The converse implication '$\Gamma \vdash A$ implies $\Gamma \vdash^0 A$' also will hold (classically), however, $\vdash^0$-deduction could be of too large size than the initial $\vdash$-deduction. Especially crucial for us is a possible lengthening the size of the participating terms due to using their abbreviations in the initial deduction.

Let, as above, the subscript 'f' denote deducibility with a (real) feasible size of participating terms. Then we will have trivially

$$\Gamma \vdash^0_f A \quad \text{implies} \quad \Gamma \vdash_f A$$

where the converse implication will *not always* hold. In particular, some theory T may be inconsistent in the sense of $\vdash_f$ ($T \vdash_f \bot$), but not in the sense of $\vdash^0_f$ ($T \nvdash^0_f \bot$).

On the other hand,

$$\Gamma \vdash (\vdash^0)\ A \quad \text{iff} \quad \Gamma \vdash^n A,$$

where 'n' symbolizes, as above, the *normality* property of natural deduction. The 'if' case holds because $\vdash^0$ will be defined to generalize $\vdash^n$. The 'only if' case may give rise to a considerable increasing the whole size of the deduction, *except* for the term size, as we will see below:

$$\Gamma \vdash^0_f A \quad \text{iff} \quad \Gamma \vdash^n_f A. \tag{1}$$

This is the reason why we could freely use more liberal notion of deducibility $\vdash^0_f$ instead of $\vdash^n_f$ for formalizing any feasibility theory, like FEAS. The calculus NK^0 or its ramified version NK' defined below may be more comfortable to work with than normalized NK.

To define NK^0 let us consider an auxiliary calculus NK' (with the corresponding deducibility relation $\vdash'$) obtained from NK by extending the first-order language of NK by a *weak* quantifiers $\forall'$ and $\exists'$ and by replacing NK-rules of *introduction* for $\forall$ and $\exists$ and also the *classical* NK-rule $(\bot_\mathrm{C})$ for the falsity by the following rules

$$\frac{A(t)}{\exists' x A(x)}\ (\exists'\mathrm{I}) \qquad \frac{A(x)}{\forall' x A(x)}\ (\forall'\mathrm{I}) \qquad \frac{\begin{array}{c}[\neg A]\\ \vdots \\ \bot\end{array}}{A}\ (\bot'_\mathrm{C})$$

where in the rule $(\bot'_\mathrm{C})$ the formula A has not the form $\forall x B(x)$ or $\exists x B(x)$ (but, e.g., may have the form $\forall' x B(x)$ or $\exists' x B(x)$). In particular, quantifier *elimination rules* may be applied only to *strong* quantifiers $\forall$ and $\exists$

$$\frac{\exists x A(x) \qquad \begin{array}{c}[A(x)]\\ \vdots \\ B\end{array}}{B}\ (\exists\mathrm{E}) \qquad \frac{\forall x A(x)}{A(t)}\ (\forall\mathrm{E}).$$

If $\mathcal{D}$ is an inference in the resulting calculus NK' then $\mathcal{D}^0$ denotes the result of the replacement of all occurrences $\forall' x B(x)$ and $\exists' x B(x)$, respectively, by $\forall x B(x)$ and $\exists x B(x)$. Then we define NK^0-deductions as deductions of the form $\mathcal{D}^0$ where $\mathcal{D}$ is any deduction in NK'. We introduce analogously the denotations A^0 and Γ^0 for arbitrary formula A and list of formulas Γ in the extended language.

Note, that $\mathcal{D} : \Gamma \vdash' A$ implies $\mathcal{D}^0 : \Gamma^0 \vdash^0 A^0$. We also have that $\mathcal{D} : \Gamma \vdash^0 A$ iff $\mathcal{D}' : \Gamma' \vdash' A'$ for some $\mathcal{D}'$ such that $(\mathcal{D}')^0 = \mathcal{D}$, $(\Gamma')^0 = \Gamma$ and $(A')^0 = A$.

The calculus NK^0 explicates (via NK') the requirement that no quantifier introduced will be eliminated in a $\mathsf{NK}^0(\mathsf{NK}')$-derivation. Therefore, no (using of) term abbreviations are allowed in NK^0 and this is achieved with much more weak restriction than normality. However, we have the following connection with the approach presented before this section.

Detour-conversions (Troelstra and van Dalen 1988) (except for $\forall$- and $\exists$-*conversions* which are impossible here due to our splitting the quantifiers according to their I- and E-rules), $\bot_C$-*conversions*[11], *permutation conversions* and *immediate simplifications* are applicable to NK'-derivations as to NK-derivations. Moreover, no new terms will be introduced in the derivations during this process. It follows that (without using quantifier conversions) we may (potentially) normalize each NK'-derivation, as for the case of NK, however, evidently without introducing new terms and therefore with preserving the term size of the given NK'-derivation. This gives the one half of the above mentioned equivalence (1). The other half follows from a more general result that not only quantifiers, but also all logical connectives in a normal natural deduction may be split into the weak and strong ones according to their participating in the rules of the deduction. We postpone the corresponding detailed considerations to some other paper.

In the case of NK^0_f we have no usual semantics for logical connectives, e.g., for the implication $\Rightarrow$. So, modus ponens is again not always applied to $\Rightarrow$. The case of NK'_f seems better for the propositional connectives (no restrictions on the corresponding rules!). However the intuitive understanding the quantifiers requires some comments.

So, given a proof $\mathcal{D}(x)$ of $A(x)$ for an arbitrary x, i.e. essentially a proof of $\forall' x A(x)$, it may be problematic to obtain a proof of $A(t)$ for any term t of feasible size. The usual substitution $\mathcal{D}(t)$ works badly because t may have several occurrences in $\mathcal{D}(t)$ (or in some other term of $\mathcal{D}(t)$). One separate such substitution may be sufficiently harmless, and this could be considered as a justification of the missing in NK' rule ($\forall'$E). This makes corresponding strong and weak quantifiers $\forall$ and $\forall'$ "almost" the same. (Evidently, $\forall x A(x) \Rightarrow \forall' x A(x)$ and the converse implication was discussed just now as "almost" true.) However, doing this repeatedly may result in trying to consider deductions with terms of non-feasible size.

Analogous consideration is applicable to $\exists$ and $\exists'$ (as well as for the possible analogous splitting of implication or disjunction).

6 Further Possible Developments

To make the theory of feasible numbers more appropriate to applications in Computer Science it should be reformulated for more rich data types than nat-

[11] to be defined appropriately; in (Prawitz 1965) and (Troelstra and van Dalen 1988) there is no corresponding definition.

ural numbers, for example, for finite strings in some finite, e.g. binary alphabet or for hereditarily finite sets. Also intuitionistic as well as higher-order versions of theories discussed could be considered. A good mathematical theory should be sufficiently rich to describe a computability notion adequately. For example, in Bounded Set Theory (Sazonov 1987) provably recursive operations over HF-sets coincide with polynomial-time computable ones. Feasible Set Theory, if any, probably should have some features of BST and of Alternative Set Theory of P.Vopenka (1979).

In the case of strings, (feasible) natural numbers are identified with unary strings (those in one-letter-alphabet). Then, the addition operation "+" is generalized to the concatenation of feasible binary strings. Some other useful operations over strings may be introduced, as well, with the requirement: *The value of any* (intuitively) *feasible closed term should be a feasible string.*

Then binary strings of the length 1000 (or 100 or even 64, because intuitively $64 \notin M$) may be naturally considered as *real numbers* (in binary notation) between $0.000\ldots$ and $1.000\ldots = 0.111\ldots$. They are naturally factorised modulo equivalence relation of *approximate equality*

$$x \approx y := \forall i \in M(x_i = y_i) \vee \text{two symmetric disjuncts of the kind}$$

$$\exists j \in M[\forall i < j(x_i = y_i) \& x_j = 0 \& y_j = 1 \& \forall i \in M(i > j \Rightarrow x_i = 1 \& y_i = 0)]$$

where x_i denotes the i-th digit of string x. We may try to develop Mathematical Analysis (e.g. to prove that $\sin' x \approx \cos x$, etc). The advantage of such a kind of Nonstandard Analysis would be corresponding "smooth" computability theory with real numbers containing only bounded (or even suitably fixed, e.g. 100) number of binary digits. Note, that, in contrast to the ordinary Robinson's approach, "nonstandard" methods seem inevitable in developing Feasible Mathematical Analysis.

The "set" of feasible numbers F may be naturally considered as a proper initial part of the set P of *polynomial numbers* (and strings) which is closed not only under addition "+" but also under multiplication "$\cdot$". It follows that $2^{1000} \in P \backslash F$, because $2^{1000} = 2 \cdot 2 \cdot 2 \cdot \ldots \cdot 2$ and the right-hand side is now a legal term of feasible length. However, $2^{2^{1000}} \notin P$ because there is no feasible term in the language $0, 1, +, \cdot$ which denotes this "imaginary" number.

The corresponding theory POL of polynomial numbers *and* finite strings of polynomial length may be formulated (like FEAS) as POL_0 + the axiom

$$\forall y \in P(\log_2 \log_2 \log_2 y < \mathbf{10})$$

which means that $2^{2^{1024}} = \infty$. Here POL_0 denotes sufficiently reach list of closed $\forall$-formulas which are "true" over the "ordinary" finite binary strings. The language of POL and POL_0 consists of some finite list of symbols for functions over finite binary strings which are sufficient to express by terms all polynomial-time computable functions (cf. Sazonov 1980a, 1989). Moreover, it is required that this language does not contain the number function x^2. More exactly, we only have the multiplication $x \cdot y$ and, in particular, $x \cdot x$, where the abbreviation x^2

for the latter is not allowed and the corresponding one-place function symbol does not exist in the language. Otherwise, we could feasibly denote the (imaginary) number $2^{2^{1024}}$ as $(\ldots((2^2)^2)^2\ldots)^2$ and prove its finiteness and therefore infer the contradiction in POL.

We may define in POL feasible numbers by the predicate $F(x) := P(x) \& \exists y \in P(x \le \log_2 y)$. Then middle and small numbers should be redefined, respectively, as $M(x) := P(x) \& \exists y \in P(x \le \log_2 \log_2 y)$ and $S(x) := P(x) \& \exists y \in P(x \le \log_2 \log_2 \log_2 y)$. (Cf. the definition of the predicates E_i in § 3.)

As in weak theories, say, of (Sazonov 1980a, 1989), the quantifier-free induction scheme is provable in POL. Also partial recursive functions via Turing computability can be described, as well as universal Turing machine, *s-m-n* theorem and recursion theorem (Sazonov 1980a, 1989). In particular, exponentiation 2^x is a *partial recursive function* here. It is undefined for $x =$ non-feasible polynomial number 2^{1024}, but its value on feasible number $x = 1024$ is defined and non-feasible. Then provably recursive functions of POL (i.e. those partial recursive functions whose totality can be proved in POL) are just polynomial-time computable ones (over polynomial binary strings).

Note, that theory FEAS, even if suitably extended from numbers to strings, seems not very appropriate to develop Turing computability. Indeed, multiplication missing in FEAS is necessary to estimate the time of simulating any Turing machine by an *universal* one and to prove this. Nevertheless we may try to define suitably the notion of partial recursive functions with the help of some other model of computation in such a theory. Then corresponding provably recursive functions could be naturally called *linear-time* or *feasibly computable*. Generally, such a way of arguing may be considered as a method to estimate "naturalness" of various notions of computability and complexity theory.

The discussion in § 3 shows that quantification (= term abbreviation) rules in non-normal proofs give rise to non-feasible (or to non-polynomial, etc.) numbers. However, if we know that the value of a (possibly very complicated) term is bounded by the value of some other term which will be never abbreviated in a proof, then the first term may be freely abbreviated without any such undesirable non-feasibility effect. Hence, the *normality requirement on proofs may be somewhat weakened as*:

> **Formula occurrences in a proof where normality fails (or cut formulas) must contain only bounded quantifiers. Additionally, Bounded Induction Axiom may be allowed.**

Here also something interesting may appear. Such abbreviations for finite binary strings of a bounded length, may give rise to not lengthy but very *complex strings* (cf. the notion of Kolmogorov's complexity of strings and the notion of constructive/non-constructive finite strings (Sazonov 1980a, 1989)). But we might want to consider only *simple* (i.e. not complex) *binary strings*, as it was above with feasible and polynomial numbers. So, we should choose which notion of binary string we are interested in and respectively decide whether the above kind of abbreviations for terms with bounded values is allowed or not.

It is very desirable to develop corresponding *informal* style of "Feasible Mathematics Thinking" like "Model-Theoretic Thinking" of classical mathematics which allows to prove theorems sufficiently rigorously, but without using formalized predicate calculus. For this aim we could begin with considering more and more liberal and convenient formalizations of corresponding logic as it was attempted above. After all, a good formalizm is such one which we use without too strong effort.

Note, that Gödel's argument on non-provability in arithmetic of its consistency does not work for formalisms (like FEAS) *without* modus ponens rule. Therefore, it is interesting to see what exactly will take place in our case.

The author sees no unsurmountable obstacle to proceed in these directions with all necessary technical details. However such a work evidently must be a heavy one because any restrictions on logic and on arithmetic require some more attention and ingenuity than usually.

7 Acknowledgements

The author is very thankful to N.V.Beljakin for numerous friendly and stimulating discussions on feasible numbers and foundational problems and to D.Leivant for the strong support, encouragement and for the polishing the English language of some parts of the paper.

References

1. Buss, S.R. (1986) *Bounded Arithmetic*, Bibliopolis, Napoli, 1986.
2. Buss, S.R. (1986) The polynomial hierarchy and intuitionistic bounded arithmetic, in: Structure in Complexity Theory, Lecture Notes in Computer Science **223** (Springer, Berlin) 125–143.
3. Cook, S.A. (1975) Feasibly constructive proofs and the propositional calculus, in: Proceedings 7th ACM Symposium on the Theory of Computation, 83–97.
4. Cook, S.A. and Urquhart, A. (1993) Functional interpretations of feasibly constructive arithmetic, Annals of Pure and Applied Logic **63**, 103–200.
5. Dragalin, A.G. (1985) Correctness of inconsistent theories with notions of feasibility, in: *Lecture Notes in Computer Science*, **208**, Springer-Verlag, 58–79.
6. Gandy, R.O. (1982) Limitations to mathematical knowledge, in: D. van Dalen, D.Laskar, J. Smiley eds., *Logic Colloquium'80*, North-Holland, Amsterdam, 129–146.
7. Gurevich, Y. (1983) Algebras of feasible functions, in: FOCS'83, pp.210–214.
8. Hájek, P., and Pudlák, P. (1993) Metamathematics of First-order Arithmetic, *Perspectives of Mathematical Logic*, 460 pp. Springer-Verlag.
9. Immerman, N. (1982) Relational queries computable in polynomial time, in: 14th STOC, pp. 147–152.
10. Kolmogorov, A.N.(1979) Automata and life (in Russian), *Kibernetika – neogranichennye vozmozhnosti i vozmozhnye ogranichenija. Itogi razvitija.* Moskwa, Nauka, 10–29.
11. Krajíček, J., (1995) Bounded Arithmetic, Propositional Logic and Complexity Theory, to appear in Cambridge University Press.

12. Nelson, E. (1986) *Predicative arithmetic*, Princeton University Press, Princeton, New Jersey.
13. Orevkov, V.P. (1979) The lower bounds of complexity the deductions increasing after cut elimination. In: *Zapiski nauchnych seminarov LOMI AN SSSR*, **88**, 137–162. (In Russian)
14. Parikh, R. (1971) Existence and feasibility in arithmetic, *JSL*, **36**, (3), 494–508.
15. Prawitz, D. (1965) *Natural Deduction*, Stockholm.
16. Sazonov, V.Yu. (1980) Polynomial computability and recursivity in finite domains. *Elektronische Informationsverarbeitung und Kybernetik*, **16**, (7), 319–323.
17. Sazonov, V.Yu. (1980a) A logical approach to the problem "$P = NP$?", in: *Lecture Notes in Computer Science*, **88**, Springer, New York, 562–575. (An important correction to this paper is given in [*Lecture Notes in Computer Science*, **118**, Springer, New York,1981, p.490.])
18. Sazonov, V.Yu. (1987) Bounded set theory and polynomial computability, FCT'87, *Lecture Notes in Computer Science*, **278**, p.391–397.
19. Sazonov, V.Yu. (1989) An equivalence between polynomial constructivity of Markov's principle and the equality $P = NP$ (in Russian), in: *Trudy instituta matematiki, Sibirskoje otdelenie akademii nauk SSSR, "Matematicheskaja logika i algoritmicheskije problemy",* Novosibirsk, "Nauka", Sibirskoje otdelenije, 138–165. (See also shorter English version with the same title in P.Petkov ed., *Mathematical Logic*, Proceedings of the Heyting's conference, sept., 1988, Varna, Plenum Press, New York, 1990, 351–360.).
20. Sazonov, V.Yu. (1992) On feasible numbers, Abstracts of papers of European Summer Meeting of the Association for Symbolic Logic, Logic Colloquium'89, Berlin, *JSL*, **57** (1) 331.
21. Statman, R. (1978) Bounds for proof-search and speed-up of the predicate calculus. *Ann. Math. Logic.*, **15** (3), 225–287.
22. Statman, R. (1979) Lower bounds on Herbrand's theorem, *Proc. of the AMS*, **75** (1).
23. Troelstra, A.S. (1990) Remarks on intuitionism and the philosophy of mathematics (revised version), *ITLI Prepublication Series* X-90-01, University of Amsterdam, 18 pp.
24. Troelstra, A.S. and van Dalen, D. (1988) Constructivism in Mathematics. An introduction, Vol. I, II, North-Holland, Amsterdam.
25. Vardi, M.Y. (1982) The complexity of relational query languages, STOC'82, pp.137–146.
26. Vopenka, P. (1979) *Mathematics in the Alternative Set Theory*, Leipzig.
27. Yesenin-Volpin, A.S., (1959) Analysis of the potential feasibility, in: *Logicheskije issledovanija*, Moskwa, AN SSSR, 218–262. (In Russian).

This article was processed using the LaTeX macro package with LLNCS style