Variants of Realizability for Propositional Formulas and the Logic of the Weak Law of Excluded Middle

Alexey V. Chernov[1], Dmitriy P. Skvortsov[2], Elena Z. Skvortsova[3], and Nikolai K. Vereshchagin[1]

[1] Dept. of Mathematical Logic and Theory of Algorithms, Moscow State University, Leninskie Gory, Moscow, 119992, Russia {chernov,ver}@mccme.ru
[2] All-Russian Institute of Technical and Scientific Information, ul. Usievicha 20a, Moscow, Russia skvortsov@viniti.ru
[3] All-Russian Multisubject School, Moscow State University, Leninskie Gory, Moscow, 119992, Russia

Abstract. It is unknown, whether the logic of propositional formulas that are realizable in the sense of Kleene has a finite or recursive axiomatization. In this paper another approach to realizability of propositional formulas is studied. This approach is based on the following informal idea: a formula is realizable if it has a "simple" realization for each substitution. More precisely, logical connectives are interpreted as operations on sets of natural numbers and a formula is interpreted as a combined operation; if some sets are substituted for variables, then elements of the result are called realizations. A realization (a natural number) is simple if it has low Kolmogorov complexity, and a formula is called realizable if it has at least one simple realization whatever sets are substituted. Similar definitions may be formulated in arithmetical terms. A few "realizabilities" of this kind are considered and it is proved that all of them give the same finitely axiomatizable logic, namely, the logic of the weak law of excluded middle.
Keywords: realizability; Kolmogorov complexity; superintuitionistic logics.

1 Introduction

1.1 Preliminary Notes

Kolmogorov in [5] proposed a constructive semantics for the propositional intuitionistic calculus, the so-called "calculus of problems". The main idea is the following. Let us fix a set of "elementary" problems and interpret the propositional connectives ($\vee$, $\wedge$, $\to$) as natural operations on this set ("to solve one of the problems", "to solve both problems", "to solve the second problem if any solution of the first problem is known"). Thus, substituting some problems for propositional variables in a formula, we get a combined problem. And if a formula is intuitionistically deducible, then the combined problem assigned to the formula has a common solution for all possible substitutions.

Kolmogorov did not define exactly what a "problem" is, he only gave some examples. Afterwards there were several attempts to construct a formal semantics for intuitionism based on Kolmogorov's ideas, for instance, Kleene realizability (see [4, §82]) and Medvedev's logic of finite problems (see [8–10]). However the intuitionistic propositional calculus turned out to be incomplete with respect to these interpretations. Moreover, the logic of finite problems has no finite axiomatization (see [7]), and it is unknown, whether it has a recursive axiomatization. For the logic of Kleene realizability both questions are open.

In this paper we consider a few new interpretations of the following kind. Let us fix some complexity measure on problems. We say that a formula is realizable if the complexity of the combined problem is bounded by some fixed function of the complexities of the substituted elementary problems. Changing the class of elementary problems, the complexity measure, and the bounding function, we can get various "realizabilities". We consider several definitions of this kind; they lead to the same set of realizable formulas.

1.2 Definitions and Results

Propositional formulas consist of variables p, q (with indices), the constant $\bot$ ("false") and the connectives $\vee$, $\wedge$, $\to$. The common abbreviations $(\Phi \leftrightarrow \Psi) \rightleftharpoons (\Phi \to \Psi) \wedge (\Psi \to \Phi)$, $\neg\Psi \rightleftharpoons (\Psi \to \bot)$, $\top \rightleftharpoons (\bot \to \bot)$ also will be used. *Positive* formulas are formulas that do not contain the constant $\bot$ (and the connective $\neg$). Propositional formulas will usually be denoted by capital Greek letters Φ, Ψ (and arithmetical formulas will be denoted by ϕ, ψ).

$\mathfrak{Int}$ denotes the intuitionistic propositional calculus (with *modus ponens* and substitution). A *superintuitionistic logic* is a set of propositional formulas that is closed under deduction in $\mathfrak{Int}$. We write $L \vdash \Phi$ if the formula Φ belongs to the logic L. If L is a logic and Γ is a set of formulas, then the least superintuitionistic logic containing the set $(L \cup \Gamma)$ is denoted by $(L + \Gamma)$. The set of all positive formulas of a logic L is called the *positive fragment* of L and is denoted by L_{Π}. We say that a logic L *has the intuitionistic positive fragment* if $L_{\Pi} = \mathfrak{Int}_{\Pi}$. In the sequel, we need the so-called Jankov logic (or the logic of the weak law of excluded middle); it is the superintuitionistic logic $\mathfrak{J} = \mathfrak{Int} + \{\neg p \vee \neg\neg p\}$, which was considered by Jankov in [3].

A *problem* is an arbitrary set of natural numbers, a *solution* of the problem is any element of this set. We thus identify a problem with the set of its solutions encoded by natural numbers.

Let us define operations on problems corresponding to the logical connectives. To this end we fix some effective enumeration U of all partial computable functions from $\mathbb{N}$ to $\mathbb{N}$. We assume that U has the following property: for every computable partial function $V(e,x)$ there is a total computable function $f(e)$ such that $V(e,x) = U(f(e),x)$ for all e, x (this provides s-m-n-theorem). For brevity we write $e(x)$ instead of $U(e,x)$. As $e(x)$ specifies a computable function of x for any fixed e, we often say that e is a program for this function. Let us also fix an effective enumeration of all pairs $\langle x, y\rangle$ and of all sequences $\langle x_1, \ldots, x_k\rangle$.

Definition 1. *Let* $X, Y \subseteq \mathbb{N}$.

$$\begin{aligned} X \wedge Y &\rightleftharpoons \{\langle x, y\rangle \mid x \in X, y \in Y\};\\ X \vee Y &\rightleftharpoons \{\langle 0, x\rangle \mid x \in X\} \cup \{\langle 1, y\rangle \mid y \in Y\};\\ X \to Y &\rightleftharpoons \{e \in \mathbb{N} \mid \forall x \in X \quad e(x) \in Y\};\\ \bot &\rightleftharpoons \emptyset,\\ \neg X &\rightleftharpoons X \to \bot \rightleftharpoons X \to \emptyset. \end{aligned}$$

The set $\Phi(X_1, \ldots, X_n)$ is defined by induction for any formula $\Phi(X_1, \ldots, X_n)$ and for any sets $X_1, \ldots, X_n$. This set is said to be the result of substituting the sets $X_1, \ldots, X_n$ for the variables $p_1, \ldots, p_n$ in the formula Φ.

Now we define Kleene realizability for propositional formulas. It is convenient to do this using *a set of realizations of a closed arithmetical formula*. Suppose the formula ϕ is atomic, then the set $R(\phi)$ of its realizations is the set $\{0\}$ if the formula ϕ is true and $\emptyset$ otherwise. Let $R(\phi \circ \psi) \rightleftharpoons R(\phi) \circ R(\psi)$, where $\circ$ is $\vee$, $\wedge$ or $\to$; $R(\forall x \phi(x)) \rightleftharpoons \{e \mid \forall k \in \mathbb{N} \quad e(k) \in R(\phi(k))\}$, and $R(\exists x \phi(x)) \rightleftharpoons \{\langle a, k\rangle \mid a \in R(\phi(k))\}$. We say that a number e *realizes* a closed formula ϕ if $e \in R(\phi)$ (this definition is equivalent to the definition of realizability from [4, §82]); a number r realizes a formula $\phi(x_1, \ldots, x_n)$ with free variables if $r(\langle k_1, \ldots, k_n\rangle) \in R(\phi(k_1, \ldots, k_n))$ for all $k_1, \ldots, k_n \in \mathbb{N}$. An arithmetical formula is called *realizable* if it has a realization.

A propositional formula $\Phi(p_1, \ldots, p_n)$ is called *realizable* if the arithmetical formula $\Phi(\phi_1, \ldots, \phi_n)$ is realizable for all arithmetical formulas $\phi_1, \ldots, \phi_n$ (possibly with free variables). The set of all realizable propositional formulas will be denoted by $\mathfrak{R}$.

If for all closed arithmetical formulas $\phi_1, \ldots, \phi_n$ a realization of $\Phi(\phi_1, \ldots, \phi_n)$ can be found effectively, then Φ is called *effectively realizable*. If there is an r that realizes $\Phi(\phi_1, \ldots, \phi_n)$ for all closed $\phi_1, \ldots, \phi_n$ then Φ is called *constantly (or uniformly) realizable*. The set of effectively realizable formulas is denoted by $\mathfrak{R}_{\text{eff}}$ and the set of constantly realizable formulas is denoted by $\mathfrak{R}_{\text{const}}$.

It is easy to see that $\mathfrak{R}$, $\mathfrak{R}_{\text{eff}}$, $\mathfrak{R}_{\text{const}}$ are superintuitionistic logics (it follows from Nelson's theorem in [4]). Obviously, $\mathfrak{R}_{\text{const}} \subseteq \mathfrak{R}_{\text{eff}} \subseteq \mathfrak{R}$. In [13] Rose showed that $\mathfrak{R}_{\text{const}} \neq \mathfrak{Int}$. The natural question is whether these logics can be described axiomatically (with a finite or enumerable set of axioms). Unfortunately, the answer is unknown. But an interesting property was discovered by Medvedev in [9] (Medvedev's original proof contains an error; in [11] Plisko gave a correct proof).

Theorem 1 (Medvedev, 1963; Plisko, 1973). *The logics* $\mathfrak{R}$, $\mathfrak{R}_{\text{eff}}$, $\mathfrak{R}_{\text{const}}$ *have the intuitionistic positive fragment.*

All the new notions of realizability defined in this paper will have the following form: we say $\Phi(p_1, \ldots, p_n)$ is realizable if the complexity of the set $\Phi(A_1, \ldots, A_n)$ is related somehow to that of the sets $A_1, \ldots, A_m$. Depending on the class of sets $A_1, \ldots, A_m$ allowed for substitution and on the complexity measure in question we obtain several versions.

In the first bunch of new realizabilities, substituted sets are arithmetical ones and complexity of A is measured by the level of A in the arithmetical hierarchy. Let us reformulate Kleene's first realizability in this vein. We say that a family of sets $A(k) \subset \mathbb{N}$, $k \in \mathbb{N}$, is *arithmetical* if there is an arithmetical formula $\phi(x, y)$ such that $A(k) = \{m \mid \phi(m, k)\}$.

Proposition 1. *A propositional formula $\Phi(p_1, \ldots, p_n)$ is realizable iff for arbitrary arithmetical families of sets $A_1(x), \ldots, A_n(x)$ there exists a number r (a realization) such that $r(k) \in \Phi(A_1(k), \ldots, A_n(k))$ for any $k \in \mathbb{N}$.*

Let us present the weakest[1] non-trivial definition of this kind.

Definition 2. *A propositional formula $\Phi(p_1, \ldots, p_n)$ is* weakly realizable *(belongs to the set $\mathfrak{R}_{\mathrm{w}}$) if for some $i > 0$ and for arbitrary arithmetical families $A_1(x), \ldots, A_n(x)$ there is an arithmetical family $B(x)$ such that $B(x)$ (more formally, an arithmetical formula that specifies $B(x)$) belongs to the class Σ_i of the arithmetical hierarchy and for all $k \in \mathbb{N}$ the set $B(k)$ is finite and intersects with $\Phi(A_1(k), \ldots, A_n(k))$.*

The crucial difference of this definition with Kleene's is that we do not require $B(k)$ to be a singleton. Note that any realizable formula is weakly realizable: we take $i = 1$ and $B(k)$ consisting of a single element for any k. The strongest non-trivial definition of this kind is as follows.

Definition 3. *A propositional formula $\Phi(p_1, \ldots, p_n)$ belongs to the set $\mathfrak{R}_{O(1)}$ if there is a number C such that for any arithmetical sets $A_1, \ldots, A_n$ there exists a natural number $r \leq C$ such that $r \in \Phi(A_1, \ldots, A_n)$.*

Note that the definition of $\mathfrak{R}_{O(1)}$ is similar to that of $\mathfrak{R}_{\mathrm{const}}$. There are other options to define realizabilities of this kind, but the corresponding logics are intermediate between $\mathfrak{R}_{O(1)}$ and $\mathfrak{R}_{\mathrm{w}}$, and we shall prove that $\mathfrak{R}_{O(1)}$ and $\mathfrak{R}_{\mathrm{w}}$ are equal.

The definitions immediately imply that $\mathfrak{R}_{\mathrm{w}}$ and $\mathfrak{R}_{O(1)}$ are superintuitionistic logics, $\mathfrak{R} \subseteq \mathfrak{R}_{\mathrm{w}}$, $\mathfrak{R}_{\mathrm{const}} \subseteq \mathfrak{R}_{O(1)}$, and $\mathfrak{R}_{O(1)} \subseteq \mathfrak{R}_{\mathrm{w}}$.

Theorem 2. $\mathfrak{R}_{\mathrm{w}} = \mathfrak{R}_{O(1)} = \mathfrak{J}$.

The second approach was proposed by A. Shen (see [14]). First, we will substitute arbitrary sets, not only arithmetical ones (this idea for predicate formulas was considered by Plisko in [12]). Second, the complexity of a set is defined as the minimum Kolmogorov complexity of its elements.

Informally, the *Kolmogorov complexity* $K(x)$ of a number x is the length of the shortest description of x. Formally, we fix any computable partial function F such that for every computable partial function G there is a constant c such that $\forall e \exists e' (\ell(e') \leq \ell(e) + c,\ F(e') = G(e))$, where $\ell(e)$ is the length of the binary representation of the number e. It is easy to prove that such functions exist, see [6]. Then we put $K(x) \rightleftharpoons \min\{\ell(e) \mid F(e) = x\}$.

We state a few important properties of Kolmogorov complexity (they are proved in the monograph [6]):

[1] The word "weakest" means that the number of realizable formulas is maximal.

1. $\exists c \forall x\, K(x) \le \ell(x) + c$;
2. for any partial computable function f $\quad \exists c \forall x\, K(f(x)) \le K(x) + c$;
3. $\forall x, y \quad K(\langle x, y\rangle) \le K(x) + K(y) + O(\log(K(x) + K(y)))$;
4. the set $\{\langle x, n\rangle \mid K(x) < n\}$ is recursively enumerable;
5. the set $\{x \mid K(x) < n\}$ contains at most $2^n - 1$ elements.

Let the *Kolmogorov complexity of a set* X be $K(X) \rightleftharpoons \min\{K(x) \mid x \in X\}$ (and $K(\emptyset) = \infty$).

It can be easily proved (by induction, using the properties 2, 3) that

$$K(\Phi(X_1, \ldots, X_n)) \le K(\bigwedge_{X_i \neq \emptyset} X_i) + O(1) \le \sum_{X_i \neq \emptyset} K(X_i) + O(\log \sum_{X_i \neq \emptyset} K(X_i))$$

for any propositional formula $\Phi(p_1, \ldots, p_n)$ and for any sets $X_1, \ldots, X_n$ such that $\Phi(X_1, \ldots, X_n) \neq \emptyset$.

Definition 4.

$$L_{O(1)} = \{\Phi \mid K(\Phi(X_1, \ldots, X_n)) = O(1)\}$$
$$L_{o(\Sigma)} = \{\Phi \mid K(\Phi(X_1, \ldots, X_n)) = o(\sum_{X_i \neq \emptyset} K(X_i))\}$$

It follows from the definition that $L_{O(1)}$ and $L_{o(\Sigma)}$ are superintuitionistic logics, $L_{O(1)} \subseteq L_{o(\Sigma)}$, $L_{O(1)} \subseteq \mathfrak{R}_{O(1)}$.

Theorem 3. $L_{O(1)} = L_{o(\Sigma)} = \mathfrak{J}$.

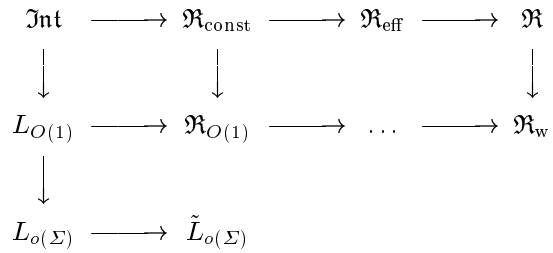
In the third approach, we substitute only finite sets for variables and measure the complexity of finite sets as follows. Fix some computable enumeration of all finite sets of natural numbers. Let the complexity $\tilde{K}(X)$ of a finite set X be the Kolmogorov complexity of its number in this enumeration. Note that $\tilde{K}(\emptyset)$ is finite in contrast to $K(\emptyset) = \infty$. Note also that a set $\Phi(X_1, \ldots, X_n)$ can be infinite even for finite $X_1, \ldots, X_n$, therefore the complexity of $\Phi(X_1, \ldots, X_n)$ must be measured as earlier.

Definition 5. *A propositional formula* $\Phi(p_1, \ldots, p_n)$ *belongs to the set* $\tilde{L}_{o(\Sigma)}$ *if* $K(\Phi(X_1, \ldots, X_n)) = o(\tilde{K}(X_1) + \ldots + \tilde{K}(X_n))$ *for all finite sets* $X_1, \ldots, X_n$.

In contrast to the previous cases, it is not obvious that $\tilde{L}_{o(\Sigma)}$ is a superintuitionistic logic. Nevertheless the following theorem is true.

Theorem 4. $\tilde{L}_{o(\Sigma)} = \mathfrak{J}$.

Let us represent relations between the described logics on two diagrams. On the first one, we represent relations that are clear immediately from the definitions ($A \longrightarrow B$ denotes $A \subseteq B$).



Our results significantly simplify this scheme, showing that many inclusions here are actually equalities:

$$\mathfrak{Int} \subset \mathfrak{R}_{\mathrm{const}} \subseteq \mathfrak{R}_{\mathrm{eff}} \subseteq \mathfrak{R} \subset \mathfrak{R}_{\mathrm{w}} = \mathfrak{R}_{O(1)} = L_{O(1)} = L_{o(\Sigma)} = \tilde{L}_{o(\Sigma)} = \mathfrak{J} \ .$$

The rest of the paper is organized as follows. The proofs of Theorems 2, 3, 4 (and Plisko's proof of the Theorem 1) are based on Medvedev's characterization of logics with the intuitionistic positive fragment. In the next section we formulate this and some other logical results, which will be used. In the Appendix A we prove Medvedev's theorem, because no proof has been published yet and we need a stronger formulation than Medvedev's original one. Section 3 is devoted to properties of the weak realizabilities and contains proofs of Theorems 2, 3, 4. The proofs use one technical lemma; its proof is given in Appendix B.

2 Logics with the Intuitionistic Positive Fragment

Medvedev in [8] proposed a convenient criterion characterizing whether all positive formulas of a given superintuitionistic logic are deducible in $\mathfrak{Int}$. Using this criterion, Medvedev proved that the logic of finite problems has the intuitionistic positive fragment. We will use it for logics of weak realizabilities.

Definition 6 (Medvedev, 1962). A critical implication *J is a positive formula that has the form*[2]

$$J = \bigwedge_{i=1}^{k} ((P_i \to Q_i) \to Q_i) \to R \ ,$$

where P_i are conjunctions of variables, Q_i and R are disjunctions of variables, for all i, the formulas P_i and Q_i have no common variables and none of P_i, Q_i, R is empty.

It can be easily checked that critical implications are not deducible in $\mathfrak{Int}$.

Theorem 5 (Medvedev, 1962). *Let Φ be an arbitrary positive formula such that $\mathfrak{Int} \nvdash \Phi$. Then there exists a critical implication J such that $(\mathfrak{Int} + \Phi) \vdash J$.*

[2] We keep Medvedev's notation for critical implications and their subformulas.

We need a stronger statement. For every $n > 0$ fix the weakest[3] critical implication J_n in the variables $p_1, \ldots, p_n$:

$$J_n = \bigwedge_{\emptyset \neq E \subset \{1,\ldots,n\}} ((\bigwedge_{j \notin E} p_j \to \bigvee_{i \in E} p_i) \to \bigvee_{i \in E} p_i) \to \bigvee_{i=1}^{n} p_i. \qquad (1)$$

Theorem 6. *Let $\Phi(q_1, \ldots, q_m)$ be a positive formula such that $\mathfrak{Int} \nvdash \Phi$. Then $\mathfrak{Int} \vdash (\Phi^* \to J_n)$ for some $n > 0$, where Φ^* is the result of substituting some formulas of the form $\vee(\wedge p_i)$ (p_i are variables of J_n) for the variables $q_1, \ldots, q_m$ in Φ.*

This theorem is proved in Appendix A.

To prove the main results we need another criterion, which was proved by Jankov in [3].

Theorem 7 (Jankov, 1968). *A superintuitionistic logic L has the intuitionistic positive fragment iff $L \subseteq \mathfrak{J}$, where $\mathfrak{J} = \mathfrak{Int} + \{\neg p \vee \neg\neg p\}$.*

In other words, the logic $\mathfrak{J}$ is the greatest logic with the intuitionistic positive fragment. This criterion is convenient for axiomatically specified logics (note that the logic $\mathfrak{J}$ is decidable). Conversely, Medvedev's criterion is more convenient for semantically specified logics (as logics of realizability). To prove our results we use both criteria. First, using Medvedev's criterion, we prove that a logic L (one of the weak realizability logics) has the intuitionistic positive fragment. Then, using Jankov's criterion, we prove that $L \subseteq \mathfrak{J}$.

3 Weak Realizabilities

In this section we prove our main results.

To prove that $\mathfrak{R}_{\mathrm{w}}$ and $\mathfrak{R}_{O(1)}$ are closed under substitution we note that substituting arithmetical sets $A_1, \ldots, A_n$ in a propositional formula $\Phi(\Psi_1, \ldots, \Psi_k)$ is equivalent to substituting the arithmetical sets $\Psi_i(A_1, \ldots, A_n)$ in Φ. The closure under *modus ponens* is obvious: applying all "possible realizations" of $\Psi \to \Phi$ to all "possible realizations" of Ψ, we get a set of "possible realizations" of Φ.

Let us consider $L_{O(1)}$, $L_{o(\Sigma)}$, $\tilde{L}_{o(\Sigma)}$. Obviously, $L_{O(1)} \subseteq L_{o(\Sigma)}$. Since for nonempty finite sets $K(X) \leq \tilde{K}(X) + O(1)$, we get $L_{o(\Sigma)} \subseteq \tilde{L}_{o(\Sigma)}$. The inclusion $L_{O(1)} \subseteq \mathfrak{R}_{O(1)}$ follows from the property 5 of Kolmogorov complexity. Each formula from $\mathfrak{Int}$ has a realization, which does not depend on substituted sets, and therefore $\mathfrak{Int} \subseteq L_{O(1)}$.

It holds $K(\Phi) \leq K(\Psi \to \Phi) + K(\Psi) + O(\log(K(\Psi)))$ (it follows from the properties 3, 2), hence $L_{O(1)}$, $L_{o(\Sigma)}$, $\tilde{L}_{o(\Sigma)}$ are closed under *modus ponens*. The closure of $L_{O(1)}$, $L_{o(\Sigma)}$ under substitution follows from the bound $K(\Phi(X_1, \ldots, X_n)) \leq K(\bigwedge_{X_i \neq \emptyset} X_i) + O(1) \leq \sum_{X_i \neq \emptyset} K(X_i) + O(\log \sum_{X_i \neq \emptyset} K(X_i))$. Thus $L_{O(1)}$, $L_{o(\Sigma)}$ are

[3] For any other critical implication J with the same variables we have $\mathfrak{Int} \vdash J \to J_n$.

superintuitionistic logics. We cannot prove this for $\tilde{L}_{o(\Sigma)}$ immediately: if a formula contains an implication, then the corresponding set may be infinite even for finite substituted sets, and therefore the closure under substitution is not so obvious. However $\tilde{L}_{o(\Sigma)}$ is closed under a restricted substitutions. More specifically, we can substitute formulas without implications, as it holds that $\tilde{K}(\bigwedge Y_i) \leq \sum \tilde{K}(Y_i) + O(\log \sum \tilde{K}(Y_i))$. The last bound can be proved by induction, using the trivial inequalities $\tilde{K}(\bot) = O(1)$, $\tilde{K}(X \wedge Y) \leq \tilde{K}(X) + \tilde{K}(Y) + O(\log(\tilde{K}(X)))$, $\tilde{K}(X \vee Y) \leq \tilde{K}(X) + \tilde{K}(Y) + O(\log(\tilde{K}(X)))$.

Now we proceed to relations between the Jankov logic $\mathfrak{J}$ and weak realizabilities. It follows from Jankov's criterion (Theorem 7) and Theorem 1 that the logic of (Kleene) realizability $\mathfrak{R}$ is a subset of $\mathfrak{J}$. It can be easily checked that $\neg p \vee \neg\neg p \notin \mathfrak{R}$, and therefore $\mathfrak{R} \neq \mathfrak{J}$.

Lemma 1.

1. $\neg p \vee \neg\neg p \in L_{O(1)}$;
2. $p \vee \neg p \notin L_{o(\Sigma)}$;
3. $p \vee \neg p \notin \mathfrak{R}_{\mathrm{w}}$.

Proof.

1. If $X = \emptyset$, then $\neg X = \mathbb{N}$; if $X \neq \emptyset$, then $\neg X = \emptyset$ and $\neg\neg X = \mathbb{N}$. Hence $K(\neg X \vee \neg\neg X) \leq \max\{K(\langle 0,0\rangle), K(\langle 1,0\rangle)\} = O(1)$.
2. Let $X = \{x \mid K(x) = n\}$. Then $K(X) = n$, $\neg X = \emptyset$, and $K(X \vee \neg X) = K(\{0\} \times X) = n + O(1) \neq o(n)$.
3. Let us fix an arbitrary number $i > 0$ and any arithmetical enumeration $B_1(x), B_2(x), \ldots$ of all families of sets from Σ_i. Let us take the arithmetical family of sets $D(x) = \{r \mid \langle 0, r\rangle \notin B_x(x)\}$.
   Assume that a family $B_k(x) \in \Sigma_i$ weakly realizes $D(x) \vee \neg D(x)$, i. e., for any m the set $B_k(m)$ is finite and $B_k(m) \cap (D(m) \vee \neg D(m)) \neq \emptyset$. Consider the set $D(k)$. Since $B_k(k)$ is finite, the set $D(k)$ is not empty, and the set $\neg D(k)$ is empty. Then $D(k) \vee \neg D(k) = \{\langle 0, r\rangle \mid r \in D(k)\}$, and $B_k(k) \cap (D(k) \vee \neg D(k)) = \{\langle 0, r\rangle \mid r \in D(k) \text{ and } \langle 0, r\rangle \in B_k(k)\} = \emptyset$. Thus B_k does not weakly realize $D \vee \neg D$, and this contradiction proves that the formula $p \vee \neg p$ does not belong to $\mathfrak{R}_{\mathrm{w}}$.

□

This lemma implies, in particular, that $\mathfrak{Int} \neq L_{O(1)}$, and $L_{o(\Sigma)}$, $\mathfrak{R}_{\mathrm{w}}$ are strictly contained in the set of classically true formulas. In addition, the logic $L_{O(1)}$ (and therefore $L_{o(\Sigma)}$, $\tilde{L}_{o(\Sigma)}$, $\mathfrak{R}_{O(1)}$, $\mathfrak{R}_{\mathrm{w}}$) includes the Jankov logic $\mathfrak{J}$.

Thus, to prove Theorems 2 and 3 it is sufficient to prove that $L_{o(\Sigma)}$ and $\mathfrak{R}_{\mathrm{w}}$ are contained in $\mathfrak{J}$, i. e., have the intuitionistic positive fragment. By Theorem 6 we must prove that no critical implication belongs to these logics.

The proof is based on the following lemma. We say that a program q *enumerates* a set A if $A = \{q(i) \mid i \in \mathbb{N}\}$, and a program q *co-enumerates* a set A if q enumerates the complement of A.

Lemma 2. *Given natural numbers m, n and a program q that enumerates a set $M \subset \mathbb{N}$ of cardinality not greater than 2^m we can effectively construct programs $a_1, \ldots, a_n$ that co-enumerate non-empty sets $A_1, \ldots, A_n$ respectively such that M and $J_n(A_1, \ldots, A_n)$[4] are disjoint; in addition, any element of $A_1, \ldots, A_n$ is not greater than $C2^{Cm}$ where C depends on n only.*

The proof is given in Appendix B.

Theorem 8. *The logics $\mathfrak{R}_{\mathrm{w}}$ and $L_{o(\Sigma)}$ have the intuitionistic positive fragment.*

Proof.

1. By Theorem 6, it is sufficient to prove that for every n the critical implication J_n does not belong to $\mathfrak{R}_{\mathrm{w}}$. Fix an i. Let $D(x)$ be an arithmetical family of sets such that for all k the set $D(k)$ is finite and for every family $B(x) \in \Sigma_i$ there exists k such that $B(k)$ is infinite or $D(k) = B(k)$ (for example, $D(k) = B_k(k)$ for finite $B_k(k)$ and is empty otherwise). Applying Lemma 2 to the set $M = D(k)$ and $m = \lceil \log_2 |D(k)| \rceil$, we get sets $A_1(k), \ldots, A_n(k)$. It is clear that the relation $x \in A_j(k)$ is arithmetical for all $j \leq n$. By construction, for every k the set $D(k)$ is disjoint with $J_n(A_1(k), \ldots, A_n(k))$. Therefore for any family $B(x) \in \Sigma_i$ there exists $k \in \mathbb{N}$ such that the set $B(k)$ is infinite or $B(k)$ and $J_n(A_1(k), \ldots, A_n(k))$ are disjoint.

2. It is sufficient to prove that for every n the critical implication J_n does not belong to $L_{o(\Sigma)}$. Applying Lemma 2 to the set of numbers with Kolmogorov complexity less than m, we get finite non-empty sets $A_1^m, \ldots, A_n^m$ such that $K(A_i^m) \leq Cm + O(1)$, but $K(J_n(A_1^m, \ldots, A_n^m)) \geq m$. □

It remains to prove Theorem 4.

Proof (of Theorem 4). We know that $\mathfrak{J} \subseteq \tilde{L}_{o(\Sigma)}$. To prove that $\tilde{L}_{o(\Sigma)} \subseteq \mathfrak{J}$ we need a stronger version of Theorem 7. In [3], actually the following is proved. Suppose a formula $\Phi(q_1, \ldots, q_k)$ is not deducible in $\mathfrak{J}$. Then there is a positive formula Ψ that is not deducible in $\mathfrak{Int}$ and a formula Φ^* that is a result of substituting new variables and the constant $\bot$ for $q_1, \ldots, q_k$ in Φ such that $\mathfrak{Int} \vdash (\Phi^* \to \Psi)$.

Since in Theorem 6 only substitutions of the form $\vee(\wedge p_i)$ are used and the set $\tilde{L}_{o(\Sigma)}$ is closed under such substitutions and *modus ponens*, it is sufficient to prove that $J_n \notin \tilde{L}_{o(\Sigma)}$ for all n.

Let us take the sets $A_1^m, \ldots, A_n^m$ constructed in the second part of the previous theorem's proof. Lemma 2 says that $A_i^m \subseteq \{1, \ldots, C2^{Cm}\}$ and we have programs that co-enumerate these sets. If we know the exact cardinalities of A_i^m, then we know the cardinalities of $\{1, \ldots, C2^{Cm}\} \setminus A_i^m$ and can effectively find all elements of $\{1, \ldots, C2^{Cm}\} \setminus A_i^m$; hence we can find A_i^m (their numbers in the enumeration of all finite sets). Thus we have $\tilde{K}(A_i^m) \leq Cm + O(1)$. This completes the proof, as $K(J_n(A_1^m, \ldots, A_n^m)) \geq m$. □

[4] Recall that $J_n(p_1, \ldots, p_n)$ is the weakest critical implication in variables $p_1, \ldots, p_n$ defined by (1).

4 Acknowledgments

The new approach to realizability considered in this paper is proposed by Alexander Shen. The authors are grateful to Alexander Shen and Andrej A. Muchnik for useful discussions.

The authors were partially supported by the Russian Foundation for Basic Research grants 01-01-01028 and 01-01-00505.

References

1. M. C. Fitting. *Intuitionistic Logic, Modal Theory and Forcing*. North-Holland, Amsterdam, 1969.
2. V. A. Jankov. O svjazi mezhdu vyvodimost'ju v intuitsionistskom ischislenii vyskazyvanij i konechnymi implicativnymi strukturami. *Doklady AN SSSR*, v. 151, N. 6, 1963, pp. 1293–1294.
3. V. A. Jankov. Ob ischislenii slabogo zakona iskluchennogo tret'jego. *Izvestija AN SSSR*, ser. matem., v. 32, N. 5, 1968, pp. 1044–1051.
4. S. K. Kleene. *Introduction to metamathematics*. New York, 1952.
5. A. Kolmogoroff. Zur Deutung der intuitionistishen Logik. *Mathematische Zeitschrift*, Bd. 35, H. 1, S. 57–65.
6. M. Li, P. Vitányi. *An introduction to Kolmogorov complexity and its applications*. New York, Springer-Verlag, 1997.
7. L. L. Maksimova, D. P. Skvortsov, V. B. Shehtman. Nevozmozhnost' konechnoj aksiomatizatsii logiki finitnyh zadach Medvedeva. *Doklady AN SSSR*, v. 245, N. 5, 1979, pp. 1051–1054.
8. Yu. T. Medvedev. Finitnye zadachi. *Doklady AN SSSR*, v. 142, N. 5, 1962, pp. 1015–1018.
9. Yu. T. Medvedev. Interpretatsija logicheskih formul posredstvom finitnyh zadach i eyo svjaz' s teoriej realizuemosti. *Doklady AN SSSR*, v. 148, N. 4, 1963, pp. 771–774.
10. Yu. T. Medvedev. Ob interpretatsii logicheskih formul posredstvom finitnyh zadach. *Doklady AN SSSR*, v. 169, N. 1, 1966, pp. 20–24.
11. V. E. Plisko. O realizuemyh predikatnyh formulah. *Doklady AN SSSR*, v. 212, N. 3, 1973, pp. 553–556.
12. V. E. Plisko. Nekotorye varianty ponjatija realizuemosti dlja predikatnyh formul. *Izvestija AN SSSR*, ser. matem., v. 42, N. 3, 1978, pp. 636–653.
13. G. F. Rose. Propositional calculus and realizability. *Transactions of the American Mathematical Society*, v. 75, N. 1, 1953, pp. 1–19.
14. A. Shen, N. Vereshchagin. Logical operations and Kolmogorov complexity. *Theoretical Computer Science*, v. 271, 2002, p. 125–129.

A Proof of Medvedev's Theorem

The proof is divided into three lemmas. We begin with some notation. Let F be a finite Kripke frame. The Heyting algebra of this frame is denoted by $H(F)$ (the maximal and minimal elements of $H(F)$ are denoted by $\mathbf{1}$ and $\mathbf{0}$ respectively), and the logic of propositional formulas that are valid in $H(F)$ is denoted by $L(F)$

(about Kripke semantics see monograph [1]). Let $\sigma(F)$ be the Kripke frame consisting of all proper subsets of the set F ordered by inclusion. Every such frame is isomorphic to one of the frames $\sigma_n = \sigma(\{1, \ldots, n\})$.

Lemma 3. *If Φ is a positive formula and $\mathfrak{Int} \nvdash \Phi$, then for some n it holds that $\Phi \notin L(\sigma_n)$.*

The proof is omitted.

The idea of the next definition and lemma is taken from Jankov's paper [2].

Definition 7. *Let variables q_a correspond to elements a of an algebra $H(F)$. We say that $X_\Pi(F)$ is a* positive characteristic formula *of the frame F, if $X_\Pi(F) = Y_F \to q_\omega$, where $\omega \rightleftharpoons F \setminus \{0_F\}$ is the greatest non-identity element of $H(F)$, Y_F is the conjunction of all formulas of the forms*

$$q_a \wedge q_b \leftrightarrow q_{a \cap b},$$
$$q_a \vee q_b \leftrightarrow q_{a \cup b},$$
$$(q_a \to q_b) \leftrightarrow q_{a \to b},$$

where $a, b \in H(F)$.

Lemma 4. *Let Φ be a positive formula, F a finite Kripke frame. Then $\Phi \notin L(F) \Leftrightarrow (\mathfrak{Int}{+}\Phi) \vdash X_\Pi(F)$. And if $\Phi \notin L(F)$, then there exist $a_1, \ldots, a_k \in H(F)$ such that $\mathfrak{Int} \vdash \Phi(q_{a_1}, \ldots, q_{a_k}) \to X_\Pi(F)$.*

The proof is similar to one in [2].

Lemma 5. *For any n it holds $(\mathfrak{Int} + X_\Pi(\sigma_n)) \vdash J_n$.*

Moreover, $\mathfrak{Int} \vdash (X^*_\Pi(\sigma_n) \to J_n)$, where $X^*_\Pi(\sigma_n)$ is the result of substituting the constant $\top$ for the variable q_1 and $\bigvee_{E \in a}(\bigwedge_{i \in E} p_i)$ for other variables q_a in $X_\Pi(\sigma_n)$ ($\bigwedge_{i=1}^n p_i$ is substituted for $q_\emptyset$), where $p_1, \ldots, p_n$ are variables of J_n.

Proof. Let F denote the frame σ_n. For any $E \subseteq \{1, \ldots, n\}$ let P_E be the formula $P_E = \bigwedge_{i \in E} p_i$, $P_\emptyset = \top$. For any $a \in H(F)$ put $Q_a = \bigvee_{E \in a} P_E$ (in particular, $Q_F = P_\emptyset = \top$, $Q_\omega = \bigvee_{i=1}^n P_{\{i\}} = \bigvee_{i=1}^n p_i$), $Q_\emptyset = P_{\{1,\ldots,n\}}$. It is easy to see that $\mathfrak{Int} \vdash (P_E \wedge P_{E'} \leftrightarrow P_{E \cup E'})$, $\mathfrak{Int} \vdash (P_E \to P_{E'})$ for $E' \subseteq E$, $\mathfrak{Int} \vdash (Q_\emptyset \to Q_a)$ for all $a \in H(F)$.

Let X^* be the result of substituting formulas Q_a for variables q_a in $X_\Pi(F)$. Then $X^* = Y^* \to \bigvee\limits_{i=1}^{n} p_i$, where Y^* is the conjunction of the formulas (for all $a, b \in H(F)$):

$$(Q_a \wedge Q_b) \leftrightarrow Q_{a \cap b} \tag{2}$$
$$(Q_a \vee Q_b) \leftrightarrow Q_{a \cup b} \tag{3}$$
$$(Q_a \to Q_b) \leftrightarrow Q_{a \to b} \tag{4}$$

We must prove that $\mathfrak{Int} \vdash (X^* \to J_n)$. It is sufficient to prove that the premise of J_n implies the premise of X^*, i. e., $\mathfrak{Int} \vdash (\bigwedge\limits_{\emptyset \neq E \subset \{1,\ldots,n\}} Z_E \to C)$ for all C from the conjunction Y^*, where $Z_E = (\bigwedge\limits_{j \notin E} p_j \to \bigvee\limits_{i \in E} p_i) \to \bigvee\limits_{i \in E} p_i$.

It can be easily checked that formulas (2) and (3) are deducible in $\mathfrak{Int}$. Let us consider formulas (4). Put $a_E = \{E'' \mid E \subseteq E'' \subset \{1,\dots,n\}\}$ and $b_E = \{E'' \subset \{1,\dots,n\} \mid E'' \cap E \neq \emptyset\}$, where $\emptyset \neq E \subset \{1,\dots,n\}$. Then $Q_{a_E} = P_E = \bigwedge\limits_{i\in E} p_i$ and $Q_{b_E} = \bigvee\limits_{i\in E} p_i$. Every a from $H(F)$ (except $\mathbf{1}$ and $\mathbf{0}$) can be represented as a union of a_E, and every b (except $\mathbf{1}$) can be represented as an intersection of $b_{E'}$. Hence, it is sufficient to deduce formulas (4) for $a = a_E$, $b = b_{E'}$. (The remaining cases with formulas containing $\mathbf{1}$ and $\mathbf{0}$ as a and b are simple.)

If $E \cap E' \neq \emptyset$, then $\mathfrak{Int} \vdash (Q_{a_E} \to Q_{b_{E'}})$ and $a_E \subseteq b_{E'}$ (if $E'' \supseteq E$, then $E'' \cap E' \supseteq E'' \cap E' \cap E = E' \cap E \neq \emptyset$), that is $a_E \to b_{E'} = \mathbf{1}$ and $(Q_{a_E \to b_{E'}}) = \top$.

Let $E \cap E'$ is empty. Then we claim that $a_E \to b_{E'} = b_{E'}$. Indeed, suppose $E'' \notin b_{E'}$, i. e., $E' \cap E'' = \emptyset$. Then $(E \cup E'') \cap E' = \emptyset$, therefore $E'' \subseteq E \cup E'' \in (a_E \setminus b_{E'})$, and $E'' \notin (a_E \to b_{E'})$. Since $E \subseteq \{1,\dots,n\} \setminus E'$, we have that $Z_{E'}$ implies (in $\mathfrak{Int}$) $(\bigwedge\limits_{j\in E} p_j \to \bigvee\limits_{i\in E'} p_i) \to \bigvee\limits_{i\in E'} p_i$. Thus $\mathfrak{Int} \vdash (Z_{E'} \to [(Q_{a_E} \to Q_{b_{E'}}) \leftrightarrow Q_{b_{E'}}])$. □

To complete the proof of Theorem 6 we show that we can avoid substituting the constant $\top$. Indeed, in Lemma 5 it is substituted for the variable $q_{\mathbf{1}}$ only. Using Lemma 3, let us choose n such that $\Phi \notin L(\sigma_{n-1})$. We can consider the frame σ_{n-1} as a subframe of σ_n, then $a_1,\dots,a_k \in H(\sigma_n)$ in Lemma 4 are subsets of the subframe σ_{n-1}, and therefore they are not equal to $\mathbf{1}$.

B Proof of Lemma 2

We start with $A_1,\dots,A_n$ equal to the set of all natural numbers less than $K_1,\dots,K_n$, respectively. The numbers $K_1,\dots,K_n$ will be specified later. Then we run an algorithm $\mathfrak{A}$ that removes certain elements from those sets; the algorithm is given m,n,q. By definition $J_n(A_1,\dots,A_n)$ is equal to $(\bigwedge\limits_{i=1}^{I}((P_i \to Q_i) \to Q_i)) \to R$. For brevity, we omit arguments in formulas P_i, Q_i, we assume that variables $t_1,\dots,t_n$ are replaced by $A_1,\dots,A_n$. We will assume also that $R = \{\langle j,a\rangle \mid a \in A_j\}$. First we will define auxiliary programs f_{ilr} for $i = 1,\dots,I$, $l = 1,\dots,2^m$, $r = 1,2,\dots$. We want to define them so that for every $e \in M$ there be $l = l(e)$, $r = r(e)$ such that

$$f_{ilr} \in (P_i \to Q_i)$$

for all $i \le I$ and $e(\langle f_{1lr},\dots,f_{Ilr}\rangle) \notin R$. The result of the program f_{ilr} on the input s will be computed by the same algorithm $\mathfrak{A}$. Using the Recursion theorem (see, e.g. [4, § 66, Theorem XXVII]), we may assume that the algorithm knows all the programs f_{ilr}. Indeed, the result of the program f_{ilr} on an input s is computed by the algorithm $\mathfrak{A}$ given s and i,l,r,m,n,q. Thus we can find the program f_{ilr} given i,l,r,m,n,q and the program of the algorithm $\mathfrak{A}$. As the algorithm knows i,l,r,m,n,q, to find f_{ilr} it needs only its own program. The

Recursion theorem just states (in one of its formulations) that we may assume that the algorithm knows its own program.

The algorithm $\mathfrak{A}$ works as follows. We first partition every set A_j in 2^m sets A_{j1}, ..., A_{j2^m} of equal size. Then we enumerate the graph of the universal function $U(s,x)$. Without loss of generality we may assume that exactly one new value $U(s,x)$ appears on any step of that enumeration. After step t in the enumeration of the graph of U, the algorithm performs the following 5 steps denoted by $5t+1$, $5t+2$, $5t+3$, $5t+4$, $5t+5$. Let M^t stand for the part of M that has appeared on steps $1,\dots,t$ in the enumeration of U; in the similar way we define U^t and $s^t(x) = U^t(s,x)$.

Step $5t+1$. If on the step t in the enumeration of U a new element e was enumerated into the set M then we let $l(e)$ to be the first number $l = 1,\dots,2^m$ different from $l(e')$ for those $e' \in M$ that have appeared before e. Let also $r(e) = t$. Later the value $r(e)$ can increase but the value $l(e)$ will not change. The program e is declared *refuted*. Later, we may again declare it non-refuted. At the start all programs are declared non-refuted.

Step $5t+2$. If on the step t in the enumeration of U we find out that for some $e \in M^t$ the value $e^t(\langle f_{1l(e)r(e)},\dots,f_{Il(e)r(e)}\rangle)$ is defined and is equal to some $\langle j,a\rangle$ then we remove a from A_j (if it is there). Thus the sets A_j will decrease and we will denote by A_j^t that part of A_j that is obtained after this step. We define A_{jl}^t, P_i^t, Q_i^t, R^t in the similar way.

Step $5t+3$. Assume that for some $i \le I$ and some s we have $s^t \in P_i^t \to Q_i^t$. For every t the sets $A_1^t,\dots,A_n^t$ will be non-empty, therefore the sets P_i^t will be non-empty too. Thus there are only finitely many such programs s. For all such i,s and all $r \le t$, $l \le 2^m$ we define the value of f_{ilr} on s as follows. Let P_{il}^t stand for the set P_i with A_j replaced by A_{jl}^t and $s(P_{il}^t)$ for the set of all the results of the program s on tuples in P_{il}^t. We will define the initial cardinalities $A_1,\dots,A_n$ in such a way that for all t the following inequalities are true:

$$\begin{aligned} &|A_{jl}^t| > n|A_{j+1}| \quad \text{for all } j < n,\\ &|A_{nl}^t| > 0 \end{aligned} \tag{5}$$

for all $l \le 2^m$. This implies that there is $\langle j,a\rangle \in s(P_{il}^t) \subset Q_i^t$ such that

> for all $k < j$ there are two tuples in P_{il}^t, differing in kth coordinate and mapped by s to $\langle j,a\rangle$.

Indeed, assume that there is no such $\langle j,a\rangle$. Then pick for every $\langle j,a\rangle \in s(P_{il}^t)$ some $k < j$ such that all the tuples in P_{il}^t mapped by s to $\langle j,a\rangle$ have the same kth coordinate. The number of such tuples is at most

$$|P_{il}^t|/|A_{kl}^t| < |P_{il}^t|/(n|A_j^t|).$$

Therefore the number of tuples in P_{il}^t mapped by s to $\{j\} \times A_j^t$ is less than $|P_{il}^t|/n$. However every tuple in P_{il}^t is mapped by s to $Q_i^t = \bigcup_j \{j\} \times A_j^t$ (the union is over all those j for which A_j is a part of Q_i). Therefore P_{il}^t has less than $n|P_{il}^t|/n$ elements, which is a contradiction.

The value of f_{ilr} on s is defined as the first $\langle j, a\rangle \in s(P^t_{il})$ having the above property. The set of all tuples in P^t_{il} mapped by s to $\langle j, a\rangle$ is called *the base of* f_{ilr} on s.

Step $5t+4$. For all refuted $e \in M^t$ and all $i \leq I$ we make the following. If after step $5t+2$ the program $f_{il(e)r(e)}$ has become *incorrect*, that is, for some s it holds $s^t \in P^t_i \to Q^t_i$ but $f_{il(e)r(e)}(s) \notin Q^t_i$ then we change $r(e)$ and let $r(e) = t$. The program e is declared non-refuted. Note that if the program $f_{il(e)r(e)}$ has become incorrect that for some s, on steps $5t'+2$ with $t' \leq t$, we have removed $f_{il(e)r(e)}(s)$ and for every tuple from the base of $f_{il(e)r(e)}$ on s we have removed at least one component (otherwise $s^t \notin P^t_i \to Q^t_i$). Therefore such event cannot happen often compared to removing elements (we will specify this later).

Step $5t+5$. If on the step $5t+2$, due to removal of a from A_j, for some s, i, l, r the base of f_{ilr} on s decreases or the value $f_{ilr}(s)$ is removed then we declare f_{ilr} *suspicious* (as the chances that later it will become incorrect increase). For all non-refuted $e \in M^t$ and all $i \leq I$ such that $f_{il(e)r(e)}$ is declared suspicious we change the value of $r(e)$ and let $r(e) = t$. Note that all f_{ilt} are not suspicious as we started to define their values only on step $5t+3$. Hence before every step $5t'+2$ for all non-refuted program $e \in M^{t'}$ and all $i \leq I$ the programs $f_{il(e)r(e)}$ are not suspicious. We do not change, on this step, $r(e)$ for refuted programs e, even if $f_{il(e)r(e)}$ was declared suspicious.

It remains to show that we can define the initial cardinalities of $A_1, \ldots, A_n$ so that for all t the inequalities (5) are true. Assume that this is proven. Then let t be a step after which the set $A^t_1, \ldots, A^t_n$ and M^t remains stable. We have to prove that the sets M and $J_n(A^t_1, \ldots, A^t_n)$ do not intersect. Let $e \in M = M^t$. The value $r(e)$ does not change after step t in the enumeration of U. After each step $5t'+3$ for $t' \geq t$ for all s we have

$$s^{t'} \in (P^t_i \to Q^t_i) \quad \Longrightarrow \quad f_{il(e)r(e)}(s) \text{ is defined and belongs to } Q^t_i.$$

Hence

$$f_{il(e)r(e)} \in (P^t_i \to Q^t_i) \to Q^t_i.$$

Assume that $e(\langle f_{1l(e)r(e)}, \ldots, f_{Il(e)r(e)}\rangle)$ is defined and belongs to R^t. Then on a step t' in the enumeration of U we find out that this is the case and remove $e(\langle f_{1l(e)r(e)}, \ldots, f_{Il(e)r(e)}\rangle)$ from R on step $5t'+2$, which is a contradiction.

To prove that the inequalities (5) are true for an appropriate choice of initial cardinalities of $A_1, \ldots, A_n$ we need to upper bound the total number of removals of elements on steps $5t+2$. Let N_k stand for the number of steps $5t+2$ such that an element $\langle k, a\rangle$ was removed on that step. Such steps are called *steps of rank* k. We will prove that

$$N_k \leq 2^{m+1}(N_1 + \ldots + N_{k-1}) + 2^{m+1}.$$

Note that after each removal the number of refuted program is incremented by 1. Some of those programs may become later non-refuted. Let K_0 stand for the number of triples $\langle e, t_1, t_2\rangle$ such that program e was declared refuted on step

$5t_1+2$ and later, for the first time, it was declared non-refuted on step $5t_2+4$. Obviously,

$$N_1+\ldots+N_n \le K_0+2^m.$$

Let us upper bound K_0. For every of those triples $\langle e,t_1,t_2\rangle$ there is s,i such that, on steps between $5t_1+2$ and $5t_2+2$, we remove $f_{il(e)r(e)}(s)$ and remove some component from all tuples in the base of $f_{il(e)r(e)}$ on s. Fix i,s for all those triples. If some of those removals happens on step $5t+2$ we say that this step is *connected* with the triple $\langle e,t_1,t_2\rangle$, and if that was a removal of the second type (that is, a removal of a component from a base), we say that this step is *strongly connected* with the triple $\langle e,t_1,t_2\rangle$. Divide triples $\langle e,t_1,t_2\rangle$ into three categories: (1) those connected with at least on step of rank strictly less than k, (2) those connected only to steps of rank k or greater and strongly connected to at least on step of rank strictly greater than k, and (3) those connected only to steps of rank k or greater and strongly connected only to steps of rank k.

The number of triples of the first type is at most $2^m(N_1+\ldots+N_{k-1})$. Indeed, for every different triples $\langle e,t_1,t_2\rangle$ and $\langle e,t_1',t_2'\rangle$ with the same first component the intervals $[t_1,t_2]$ and $[t_1',t_2']$ are disjoint. If a step $5t+2$ is connected to the triple $\langle e,t_1,t_2\rangle$ then $t_1\le t\le t_2$ therefore it is connected to no other triple $\langle e,t_1',t_2'\rangle$. Hence the total number of triples connected to any step is at most $|M|\le 2^m$.

The number of triple of the second type is at most $N_{k+1}+\ldots+N_n$. Indeed, any step is strongly connected with at most one triple: for all different e_1,e_2 and all j the sets $A_{jl(e_1)}$ and $A_{jl(e_2)}$ are disjoint, hence on every step we cannot remove some component both from a tuple in a base of $f_{i'l(e_1)r(e_1)}$ and from a tuple in a base of $f_{i''l(e_2)r(e_2)}$.

The number of triples of the third type is at most $N_k/2$. To show this it suffices to prove that every triple $\langle e,t_1,t_2\rangle$ of the third type is strongly connected to at least two steps of rank k. Assume that $f_{il(e)r(e)}(s)$ is equal to $\langle j,a\rangle$. All the removals of components of tuples from the base of $f_{il(e)r(e)}$ on s were done on steps of rank k. The definition of a critical implication implies that $j\ne k$. Since $f_{il(e)r(e)}(s)$ was removed on a step of rank k or greater we conclude that $k<j$. Thus the base of $f_{il(e)r(e)}$ on s has two tuples with different k-coordinates, which cannot be removed on the same step of rank k.

So we have proven that

$$N_1+\ldots+N_n \le 2^m(N_1+\ldots+N_{k-1})+N_k/2+N_{k+1}+\ldots+N_n+2^m,$$

therefore

$$N_k \le 2^{m+1}(N_1+\ldots+N_{k-1})+2^{m+1},$$

hence $N_k\le 2^{m+1}(2^{m+1}+1)^{k-1}<2^{(m+2)n}$. For the last inequality in (5), it is sufficient to let $|A_n|=2^{(m+2)(n+1)}$. For other inequalities in (5) we need $|A_{k-1}|2^{-m}>n|A_k|+N_{k-1}$ for all $k=n,\ldots,2$. The second term in the right hand side of this inequality is less than the first one. Therefore it suffices to let $|A_{k-1}|=n2^{m+1}|A_k|$. Finally we obtain the bound $|A_k|=2^{(m+2)(n+1)}(n2^{m+1})^{n-k}$.