processor which can implement any existing and hypothetical protocols of converting parallel information into sequences of discrete signals [10, 11].

LITERATURE CITED


APPLICATION OF THE RULE OF INFERENCE IN INFORMAL MATHEMATICAL PROOFS

N. Nansalmaa* UDC 681.3.06.14

Mart'yanov's works [1, 2] on automatic theorem proving by the invariant transformation method examine transformations of formulas of restricted predicate calculus (RPC), which are formal analogs of certain steps of substantive (not formal) mathematical proofs. As noted in [3], one class of these transformations (the \( \zeta \)-transformations) is a derived form of the rule of inference. We will illustrate this with an example.

Suppose we are to prove the assertion

\[
\Phi = \begin{cases} 
\text{given } A, B, ..., & \\
\text{prove } T, &
\end{cases}
\]

The formula \( \Gamma = A \rightarrow C \) is an axiom of the branch of mathematics we are considering. Then we apply the rule of inference to the formulas \( \Gamma \) and \( A \) from the "given" and proceed to prove the assertion:

\[
\Phi' = \begin{cases} 
\text{given } A, B, ..., C, & \\
\text{prove } T, &
\end{cases}
\]

If we represent the assertion \( \Phi \) by a RPC formula, then the "given" will be the premise of the implication and "prove" will be the conclusion; the use of the axiom \( \Gamma \) will be an application of the rule of inference to the premise of the implication \( \Phi \). This transformation scheme from \( \Phi \) to \( \Phi' \) produces a modification of the rule of inference, which in [1, 3] is called the \( \zeta \)-transformation of formulas. Note that the given scheme does not provide a complete idea of the potential of the \( \zeta \)-transformation as a total of logical inference. As we see from [4-7], the \( \zeta \)-transformations of formulas use numerous other logical rules and combinations of rules. This feature demonstrates that the \( \zeta \)-transformations, as one element is an automatic theorem proving system, have "large-block" structure in Glushkov's sense: "... A system is

*Deceased.

said to have large-block structure if the logical tools are not restricted to a fixed small number of simple axioms and rules of inference, but encompass a whole wealth of propositions and procedures from the substantive areas of mathematics [6]. A similar tendency, that is, an effort to use rules of inference which have substantive mathematical meaning, can be discerned in other approaches to automatic proving and deduction of theorems [7-11]; this tendency has grown markedly stronger in recent times.

A practical realization of the method of invariant transformations [the AVTODOT automatic theorem prover — a joint development of the Irkutsk Computer Center of the Siberian Branch of the Academy of Sciences of the USSR (IrVTs SO AN SSSR) and the A. A. Zhdanov Irkutsk State University (IGU)] has demonstrated that the $\zeta$-transformations, as they are defined in [1, 2], are not sufficiently effective. For this reason another definition of the $\zeta$-transformations has been adopted in the AVTODOT system; the following example will illustrate its meaning.

Suppose the assertion we are to prove is of the form

$$\Phi = \begin{cases} \text{given} A, B \lor C, \\
\text{prove} \ A \lor C \end{cases}$$

If the formula $\Gamma = A \circ B \rightarrow D$ is an axiom in the area of mathematics we are considering, then the rule of inference is applied to the formulas $\Gamma$ and $A \circ B$ from the "given" and we proceed to prove the assertion

$$\Phi' = \begin{cases} \text{given} A, (B \circ D) \lor C, \\
\text{prove} \ A \lor C \end{cases}$$

This example corresponds fairly often to the situations encountered in substantive proofs, where known facts are extended for one of the alternatives present in the "given." Below, we will call such transformations the $\Delta \zeta$-transformations.

In the present work we will discuss the conditions under which these transformations are valid. All the information necessary to understand this article can be found in [12-14].

Let $\mathcal{K}$ be a class of models of the signature $\sigma$. Let $L_0$ be a set of formulas of the signature $\sigma$. Then the mapping $\varphi: L_0 \rightarrow L_0$ is an invariant (valid) transformation of formulas with respect to the class of models $\mathcal{K}$ if for any formula $\Phi \in L_0$ we have

$$\mathcal{K} \models \Phi \iff \mathcal{K} \models \varphi(\Phi).$$

In the rest of this paper we will drop the phrase "with respect to the class of models $\mathcal{K}$" because we will focus only on a single class of models.

With the formula

$$A = Q(A_1(\overline{x}) \circ A_2(\overline{x}) \rightarrow A_3(\overline{x}))$$

we associate the transformation $\Delta \zeta_A$ such that if the formula

$$\Phi = P(D_1(\overline{z}) \circ (D_2(\overline{z}) \lor D_3(\overline{z})) \rightarrow E(\overline{z}))$$

and the formulas

$$D_1(\overline{z}) = E_1(\overline{z}) \circ A_1(\overline{x}), \quad D_2(\overline{z}) = E_2(\overline{z}) \circ A_2(\overline{x}),$$

then

$$\Delta \zeta_A(\Phi) = P(D_1(\overline{z}) \circ (D_2(\overline{z}) \circ A_3(\overline{x}) \lor D_3(\overline{z})) \rightarrow E(\overline{z})),$$

where $Q$ and $P$ are quantifier prefixes and $\overline{x}$ and $\overline{z}$ are tuples of variables.

By definition, suppose that, without $A_2$, the action of the $\Delta \zeta$-transformations is analogous to the $\zeta_A$-transformation [1, 2]. Thus, our validity theorems are a generalization of the corresponding validity theorems for the $\zeta$-transformations.

The variable $x$ is called an essential $\exists$-variable of the formula $\Phi = P_1 \exists x P_2(U(x, \overline{y}) \rightarrow W(x, \overline{y}))$ with respect to a class of models $\mathfrak{F}$, if $\mathfrak{F} \models \Phi, \mathfrak{F} \models \Gamma$, where $\Gamma = P_1 \forall x P_2(U(x, \overline{y}) \rightarrow W(x, \overline{y}))$.

In the rest of this paper we will use the following notation:

$\forall \overline{x}$ — for all the variables of the tuple $\overline{x}$ bound by $\forall$-quantifiers;

$P_1\overline{x}_i$ for the variables of the tuple $\overline{x}_i$ bound by arbitrary quantifiers;

$\neg (P_1\overline{x}_i)$ for the variables of the tuple $\overline{x}_i$ bound by converse quantifiers relative to the quantifiers in $P_1\overline{x}_i$. 

519