別紙４

報告番号	※　　第　　号

主　論　文　の　要　旨

論文題目 Formalization of Equational Reasoning in the Set-Theoretic Interpretation of Type Theory
(型理論の集合論的意味論を用いた等式変形証明法の形式化)

氏　名　　才川　隆文

論　文　内　容　の　要　旨

The method of equational reasoning is a style for mathematical proofs which heavily uses rewriting along equations.
Not only values but propositions are rewritten using equivalence lemmas.

This style is common in proofs of pure mathematics but not so much in proofs written using computerized proof assistants. Proofs assistants are softwares that aid human users to write and check mathematical proofs. They are based on systems of formal logic, in which proofs are expressed as tree structures. Using such representations of proofs, it is easier for the users of proof assistants to proceed with a deductive style of proof.

These two styles are quite different in terms of the management of hypotheses in the proofs. The deductive style of proofs traverses and constructs a tree of proofs. The hypotheses may appear or disappear based on the shape of tree, resulting in the localization of proofs at each point of the proof tree.

On the other hand, equational rewriting basically does not discard hypotheses. One can chain many steps of reasoning without paying constant attention to the proof tree structure: they are freed from the low-level tree expression of

proofs.

This thesis is based upon the foundational studies on formal logic, especially on equational reasoning. We formalize using a proof assistant various aspects of equational reasoning. Especially we focus on the formalization of monadic equational reasoning on effects. Effects are features of computer programs that have been long considered to be a difficult target for equational reasoning. We have worked out a framework to formally perform equational reasoning on the effects of programs.
The formalization includes both theories which are applied to proofs on concrete programs, and models which assure the consistency of those theories.

We also extend the method of equational reasoning by developing a framework for category theory. This framework features the use of concrete categories on the contrary to many other formalization attempts. This design choice leads to the lightweight usability of our framework. It enables shallow embedding and direct reasoning on programs whose properties can only be captured at categorical level. As a specific example, we construct the first formalized model of the theory of combined probabilistic and nondeterministic choice. It has been the subject of extensive research and is known to be tricky.

This construction of model is backed by the formalization of convex spaces. Convex spaces arise as an algebraic abstraction of convex sets in vector spaces. They appear in various domains of pure and applied mathematics.
Although it is also an equational theory, it is poor in algebraic properties such as linearity of vector operations and does not allow easy rewriting.
We investigated its accompanying theory of conical spaces, which is an abstraction of real cones in vector spaces, and have proper linearity in its operations. We have devised a method to prove properties of convex spaces by embedding them into conical spaces and projecting them back. This method was only recently noticed in the literature and our specific applications turns out to be new.