平成30年度 情報工学コース卒業研究報告要旨

酒井研究室 研究室	氏　名	SHIN　Donghoon
卒業研究題目	A Proof Assistant for Constrained Rewriting Induction with Lemma Generation Based on Equality Derivation	

Recently, logically constrained term rewriting systems (LCTRSs, for short) have attracted attention as a framework of analyzing imperative programs by means of transformations into rewriting systems. LCTRSs are extensions of term rewriting systems by attaching logical constraints to rewrite rules. A rewriting rule is applied to a term if the attached constraint is satisfied by the matching substitution. LCTRSs can represent the transition of terms expressing executing states of programs and conditions of control statements separately. Fuhs et al. have extended a verification method based on rewriting induction (RI, for short), which has been proposed for TRSs, to LCTRSs. RI can be applied to verification of equivalence between two functions defined by not only functional but also imperative programs.

The RI framework consists of some inference rules. To prove equivalence of two terms w.r.t. arbitrary instances, we apply inference rules to the set of initial equations of terms until the set becomes empty. To automate the verification based on RI, we need a strategy of applying inference rules to sets of equations to be proved. Unfortunately, a complete strategy to succeed in proving all equations that can be proved by RI has not been developed yet. In addition, we often need lemma equations to succeed in proving given equations. For these reasons, it is worth developing both strategies of applying inference rules for RI, and methods for lemma generation.

Ctrl (Constrained Term Rewriting tooL) has been developed for verifying properties of LCTRSs. Ctrl can try to verify equivalence of two terms by means of RI with some complex built-in strategy of the application of inference rule, which makes backtracking for possible branches of the application. Due to the complex strategy, it is very hard for developers to not only modify Ctrl to test temporal strategies under a trial-and-error approach, but also add a new method for lemma generation to Ctrl.

In this study, we aim at developing a verification tool based on RI for LCTRSs, which is useful in making a trial-and-error to test both many strategies for the application of inference rules and methods for lemma generation. To this end, we develop a tool, so-called a proof assistant, that interacts with Ctrl by means of its manual mode in order to apply inference rules to sets of equations to be proved. As a consequence, we no longer have to modify Ctrl.

The developed tool performs as follows. The tool first reads a file in which an LCTRS and equations to be proved are specified by a user; Then, the tool calls Ctrl with the manual mode, sending the file to Ctrl, and Ctrl waits for the interaction with the tool; Finally, the tool starts to interact with Ctrl by sending commands for the manual mode of Ctrl, which are specified by the user or the tool itself. In this way, the tool performs as a user interface for the manual mode of Ctrl. To ease a trial-and-error for finding successful commands of the manual mode, the tool can automatically use commands that are rewritten in a file as an extra information.

The tool has three original commands which Ctrl does not have: (1) addition of a user-specified equation to the present set, (2) conjunction/disjunction of a user-specified formula to the constraint of the head constrained equation in the present set, and (3) a new generalization method of equations, which adds equalities derived from the original formula into the generalized one. The new generalization method is based on the one implemented in Ctrl. The original method in Ctrl drops some equalities related to initialization of accumulators. Unfortunately, such a way may drop equivalence between some variables, which should be kept to succeed in proving the present constrained equation. For each pair of variables in the equation, the new generalization method tests whether the constraint derives equivalence of variables in the pair, and adds the derived equivalence into the generalized constraint as equalities between variables.

Finally, we introduce a naive strategy of the application of inference rules to the developed tool, automating the application of inference rules with the new generalization method. We report that the naive strategy and the new generalization method succeed in automatically proving an equation which Ctrl cannot prove automatically.