SCHOOL OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING
MONASH UNIVERSITY

TECHNICAL REPORT 2000/58

Correct interaction between programs and proofs

I Poernomo and J N Crossley

ABSTRACT

In this paper we describe our protocol for the interaction between a theory and the programs extracted from it. This protocol leads to the expansion of the theory and the production of more powerful programs. The methodology we use for automatically extracting "correct" programs from proofs is a development of the well-known Curry-Howard process. Although program extraction has been developed by many authors (see, for example, [9], [5] and [12]), our presentation has a number of novel features. These include
1. first of all, a mimicking of ordinary mathematical practice in the constraction of new mathematics and likewise the use of established computer programs when we extract programs from formal proofs.
2. the use of a (first-order) many-sorted logic (so we have an underlying logic that is as close as possible to standard usage),
3. a conceptual distinction between programs and proofs of theorems about programs, and
4. a *dynamic* system that is "open" in the sense that new axioms and functions may be added to it in the course of a proof and then used in later proofs (subject to an obvious consistency requirement).

An implementation of our methodology is the **Fred** system that runs under Windows 95/98/NT. (The name **Fred** stands for "Frege-style dynamic [system]".) As an example of this system and our protocol we describe a constructive proof of the well-known theorem that every graph of even parity can be decomposed into a list of disjoint cycles. Given such a graph as input, the extracted program produces a list of such cycles as promised.