ABSTRACT

A common tool for proving the termination of programs is the well-founded set, a set ordered in such a way as to admit no infinite descending sequences. The basic approach is to find a termination function that maps the values of the program variables into some well-founded set, such that the value of the termination function is continually reduced throughout the computation. All too often, the termination functions required are difficult to find and are of a complexity out of proportion to the program under consideration. However, by providing more sophisticated well-founded sets, the corresponding termination functions can be simplified.

Given a well-founded set \( S \), we consider multisets over \( S \), "sets" that admit multiple occurrences of elements taken from \( S \). We define an ordering on all finite multisets over \( S \) that is induced by the given ordering on \( S \). This multiset ordering is shown to be well-founded. The value of the multiset ordering is that it permits the use of relatively simple and intuitive termination functions in otherwise difficult termination proofs. In particular, we apply the multiset ordering to prove the termination of production systems, programs defined in terms of sets of rewriting rules.

An extended version of this paper appeared as Memo AIM-310, Stanford Artificial Intelligence Laboratory, Stanford, California.

This research was supported in part by the United States Air Force Office of Scientific Research under Grant AFOSR-76-2909 (sponsored by the Rome Air Development Center, Griffiss AFB, NY), by the National Science Foundation under Grant MCS 76-83655, and by the Advanced Research Projects Agency of the Department of Defense under Contract MDA 903-76-C-0206.

1Current Address:
Department of Computer Science
University of Illinois
Urbana, Illinois 61801

2Current Address:
Department of Computer Science
Stanford University
Stanford, California 94305
I. INTRODUCTION

The use of well-founded sets for proving that programs terminate has been suggested by Floyd [1967]. A well-founded set consists of a set of elements $S$ and a transitive and irreflexive ordering $\succ$ defined on the elements such that there can be no infinite descending sequences of elements. The idea is to find a well-founded set and a termination function that maps the values of the program variables into that set such that the value of the termination function is continually reduced throughout the computation. Since, by the nature of the set, the value cannot decrease indefinitely, the program must terminate.

The well-founded sets most frequently used for this purpose are the natural numbers under the "greater-than" ordering and $n$-tuples of natural numbers under the lexicographic ordering. In practice using these conventional orderings often leads to complex termination functions that are difficult to discover. For example, the termination proofs of programs involving stacks and production systems are often quite complicated and require much more subtle orderings and termination functions. Finding an appropriate ordering and termination function for such programs is a well-known challenge among researchers in the field of program verification. In this paper, we introduce a powerful ordering that can sometimes make the task of proving termination easier.

II. THE MULTISET ORDERING

For a given partially-ordered set $(S, \succ)$, we consider multisets (sometimes called "bags") over $S$, i.e. unordered collections of elements that may have multiple occurrences of identical elements. For example, $\{3,3,4,0,0\}$ is a multiset of natural numbers; it is identical to the multiset $\{0,3,3,0,4,3\}$, but distinct from $\{3,4,0\}$.

We denote by $\mathcal{M}(S)$ the set of all finite multisets with elements taken from the set $S$.

For a partially-ordered set $(S, \succ)$, the multiset ordering $\gg$ on $\mathcal{M}(S)$ is defined as follows:

$$M \gg M'$$

if for some multisets $X, Y \in \mathcal{M}(S)$, where $\emptyset \not\in X$, $M' = (M \setminus X) \cup Y$ and $(\forall y \in Y) (\exists x \in X) x \succ y$.

In words, a multiset is reduced by the removal of at least one element (those in $X$) and their replacement with any finite number - possibly zero - of elements (those in $Y$), each of which is smaller than one of the elements that have been removed. Thus, if $S$ is the set $\mathbb{N}$ of natural numbers $0, 1, 2, \ldots$ with the $\succ$ ordering, then under the corresponding multiset ordering $\gg$ over $\mathbb{N}$, the multiset $\{3,3,4,0\}$ is greater than each of the three multisets $\{3,4\}$, $\{3,2,2,1,1,1,4,0\}$, and $\{3,3,3,3,2,2\}$. In the