On Proving Termination through Transfer Functions

Oliver Theel and Felix C. Gärtner*

Darmstadt University of Technology
Department of Computer Science
D-64283 Darmstadt, Germany

Phone: (+49)-6151-16-5306/3908
Fax: (+49)-6151-16-5410
Email: {theel|felix}@informatik.tu-darmstadt.de

Notions of termination appear in nearly every area of computer science. We have encountered one of these notions in the context of self-stabilizing distributed algorithms. An algorithm is said to be *self-stabilizing* if, starting from any state, it is guaranteed to reach a pre-defined set of legal states in finite time. This is called the *convergence* property of such algorithms. Together with the additional requirement that the set of legal states is closed under normal system operation, this ability can be seen as a very powerful method of achieving fault-tolerance: self-stabilizing algorithms tolerate *any* kind of transient failure in a non-masking way, even those failures which were unforseeable at design time.

Proving convergence of self-stabilizing algorithms is an instance of proving termination, and so all the methods that exist in the literature can be applied. However, the existing methods in computer science seemingly all boil down to a well-foundedness argument: basicly, one has to devise a well-founded ordering relation on system states and then show that in every state transition of the algorithm either a legal state is reached or the transition decreases the "order value" of the states involved. An equivalent proof method is to exhibit a corresponding *termination function* (commonly called *convergence function* in the self-stabilization literature). However, just like in the area of termination, devising such a termination function requires some creativity. In self-stabilization finding such a function is especially difficult since it must consider *all* states of the algorithm and capture the very "essence" of the convergence property.

Currently we are investigating methods to prove termination by adopting results from *control theory.* The objective of this part of electrical engineering is to "stabilize" real-world processes (like motors, power supplies and other electric or electronic devices) by devising special control components around the process (i.e., a control circuit) to guarantee that the process' output will stabilize to

*This author's work was supported by the Deutsche Forschungsgemeinschaft (DFG) as part of the "Graduiertenkolleg ISIA" at Darmstadt University of Technology.

a certain value (like speed, voltage etc.) whenever external influences disturb normal operation.

The central part of proving the stability of such a control circuit is to calculate the input-to-output behavior of the process alone (its so called *transfer function*) and then "plug in" controller components that influence this transfer function in predefined ways. By adding these components, the transfer function of the overall control circuit is changed. Basic theorems of control theory offer a set of sufficient conditions proving that the overall transfer function will converge to some predified value.

The similarities in the problem statement are obvious. No so obvious are the similarities in proof techniques. While the traditional approach of convergence functions uses a state-based reasoning approach based on some form of logic, the control theory approach can be characterized as investigating the limits behavior of the overall transfer function. This involves solving non-linear differential equations, calculating function transformations and dealing with residues and complex numbers. While other proof methods similar to termination functions exist in control theory, the usual approach which we will present in the talk seems to have very little resemblance to the standard well-foundedness approach of computer science. For example, while the traditional termination functions are necessarily monotonic and stop decreasing at some finite point in time, the transfer functions are not necessarily monotonic (i.e., they can oscillate with decreasing amplitude around the target value) and converge only in the limit.

In the talk, we will present the control theory approach as sketched in this abstract. We are interested in obtaining some expert comments from the termination community on the above and some other open questions we have. We plan to illustrate the topic with an example algorithm which can be easily proved correct using the control theory approach but which we have found no easy way of proving using a well-foundedness argument.