Abstract. Using only a simple transition relation one cannot model commands that may or may not terminate in a given state. In a more general approach commands are relations enriched with termination vectors. We reconstruct this model in modal Kleene algebra. This links the recursive definition of the \texttt{do od} loop with a combination of the Kleene star and a convergence operator. Moreover, the standard \texttt{wp} operator coincides with the \texttt{wlp} operator in the modal Kleene algebra of commands. Therefore our earlier general soundness and relative completeness proof for Hoare logic in modal Kleene algebra can be re-used for \texttt{wp}. Although the definition of the loop semantics is motivated via the standard Egli-Milner ordering, the actual construction does not depend on Egli-Milner-isotony of the constructs involved.

1 Introduction

Total correctness has been extensively studied, a.o. using relational methods. One line of research (see e.g. [3]\cite{8}\cite{9}\cite{12}\cite{24}) provides strongly demonic semantics for regular programs. There, however, one cannot model commands that may or may not terminate in a given state. A second line of research (e.g. [4]\cite{5}\cite{13}\cite{23}\cite{25}) provides a weakly demonic semantics that allows such more general termination behaviour. We reconstruct the latter approach in modal Kleene algebra. This provides a new connection between the recursive definition of the \texttt{do od} loop and a combination of the Kleene star with convergence algebra. Moreover, it turns out that the standard \texttt{wp} operator coincides with the \texttt{wlp} operator of a suitable modal algebra of commands. Therefore the general soundness and relative completeness proof for Hoare logic in modal Kleene algebra given in [21] can be re-used for \texttt{wp} (where now, of course, expressiveness has to cover termination). Although the definition of the loop semantics is motivated via the standard Egli-Milner ordering, its actual construction does not depend on Egli-Milner-isotony of the constructs involved. A number of simple proofs are omitted due to lack of space; they can be found in the technical report [22].

2 Weak and Modal Semirings

A weak semiring is a quintuple \((S, +, 0, \cdot, 1)\) such that \((S, +, 0)\) is a commutative monoid and \((S, \cdot, 1)\) is a monoid such that \(\cdot\) distributes over \(+\) and is left-strict,
i.e., $0 \cdot a = 0$. $S$ is idempotent if $+$ is. In this case the relation $a \leq b \overset{\text{def}}{=} a + b = b$ is an order, called the natural order on $S$, with least element 0. Moreover, $\cdot$ is isotope w.r.t. $\leq$. A semiring is a weak semiring where $\cdot$ is also right-strict, i.e., $a \cdot 0 = 0$.

An important idempotent semiring is REL, the algebra of binary relations under union and composition over a set. Other interesting examples of weak idempotent semirings can be found within the set of endofunctions on an upper semilattice $(L, \sqcup, \sqcap)$ with least element $\sqcap$, where addition is defined as $(f + g)(x) = f(x) \cup g(x)$ and multiplication by function composition. The set of disjunctive functions (satisfying $f(x \sqcup y) = f(x) \sqcup f(y)$) forms a weak idempotent semiring. The induced natural order is the pointwise order $f \leq g \iff \forall x.f(x) \leq g(x)$. The subclass of strict disjunctive functions (satisfying additionally $f(\sqcap) = \sqcap$) even forms an idempotent semiring. These types of semirings include predicate transformer algebras and are at the centre of von Wright’s algebraic approach [27].

A (weak) test semiring is a pair $(S, \text{test}(S))$, where $S$ is a(weak) idempotent semiring and $\text{test}(S) \subseteq [0, 1]$ is a Boolean subalgebra of the interval $[0, 1]$ of $S$ such that $0, 1 \in \text{test}(S)$ and join and meet in $\text{test}(S)$ coincide with $+$ and $\cdot$. This definition corresponds to the one in [18]. In REL the tests are partial identity relations (also called monotypes or coreflexives), encoding sets of states. We use $a, b, \ldots$ for general semiring elements and $p, q, \ldots$ for tests. By $\neg p$ we denote the complement of $p$ in $\text{test}(S)$ and set $p \rightarrow q = \neg p + q$. Moreover, we sometimes write $p \land q$ for $p \cdot q$ and $p \lor q$ for $p + q$. We freely use the Boolean laws for tests. An important property is

$$p \cdot a \cdot q \leq 0 \iff a \cdot q \leq \neg p \cdot a .$$

For $(\Rightarrow)$ we note $a \cdot q = (p \neg p) \cdot a \cdot q = p \cdot a \cdot q + \neg p \cdot a \cdot q = \neg p \cdot a \cdot q \leq \neg p \cdot a$ by $q \leq 1$. For $(\Leftarrow)$ we have $a \cdot q \leq \neg p \cdot a \Rightarrow p \cdot a \cdot q \leq p \cdot \neg p \cdot a = 0 \cdot a = 0$.

A (weak) modal semiring is a pair $(S, [])$, where $S$ is a (weak) test semiring and the box $[ ] : S \rightarrow (\text{test}(S) \rightarrow \text{test}(S))$ satisfies

$$p \leq [a]q \iff p \cdot a \cdot \neg q \leq 0 , \quad [(a \cdot b)]p = [a]([b]p) .$$

The diamond is the de Morgan dual of the box, i.e., $\langle a \rangle p = \neg[a] \neg p$.

The box generalises the notion of the weakest liberal precondition wp to arbitrary weak modal semirings. When $a$ models a transition relation, $[a]p$ models those states from which execution of $a$ is impossible or guaranteed to terminate in a state in set $q$. In REL one has $(x, x) \in [R]q \Leftrightarrow \forall y : xRx \Rightarrow (y, y) \in q$. In arbitrary weak semirings the box need not exist; for more details see [10].

The box axioms are equivalent to the equational domain axioms of [10]. In fact the domain of element $a$ is $r[a] \overset{\text{def}}{=} \neg[a]0$. Hence $r[a]$ provides an abstract characterisation of the starting states of $a$. Conversely, $[a]q = \neg r[a \cdot \neg q]$. Most of the consequences of the box axioms shown originally for strict modal semirings in [10] still hold for weak modal semirings (see [20]), in particular,

$$[a](p \cdot q) = [a]p \cdot [a]q , \quad \langle a \rangle (p + q) = [a]p + [a]q , \quad (2)$$

$$[a + b]p = [a]p + [b]p , \quad \langle a + b \rangle p = \langle a \rangle p + \langle b \rangle p , \quad (3)$$

$$[p]q = p \rightarrow q , \quad \langle p \rangle q = p \cdot q . \quad (4)$$