Ideal-Based Algorithms for the Symbolic Verification of Well-Structured Systems

Philippe Schnoebelen

LSV, CNRS & ENS Paris Saclay, Cachan, France
phs@lsv.fr

Abstract

We explain how the downward-closed subsets of a well-quasi-ordering \((X, \leq)\) can be represented via the ideals of \(X\) and how this leads to simple and efficient algorithms for the verification of well-structured systems.

1998 ACM Subject Classification F.1.1 Models of Computation, F.3.1 Specifying and Verifying and Reasoning about Programs

Keywords and phrases Well-structured systems and verification, Order theory

Digital Object Identifier 10.4230/LIPIcs.MFCS.2017.85

Category Invited Talk

1 Summary of the talk

Well-structured systems, also known under the acronym “WSTSS”, are a family of infinite-state models for which generic verification algorithms exist [1, 2, 13, 18, 23]. With WSTSS, the main ingredient for decidability is the existence of an ordering on configurations that enjoys two properties:

- it is a well-quasi-ordering (a WQO): every infinite sequence \(c_0, c_1, c_2, \ldots\) of configurations contains an increasing pair \(c_i \leq c_j\) with \(i < j\);
- transitions are monotonic: if the system can perform a step \(c \rightarrow c'\) then from any configuration \(d \geq c\), a “similar” step is possible, i.e., there is some \(d \rightarrow d'\) with \(d' \geq c'\).

The most well-known instances of WSTSSs are some families of counter machines or vector addition systems [8, 12]. For simplicity, we shall assume that the WQO set of configurations for these systems is \(\text{Conf} = (\mathbb{N}^d, \leq)\) for some dimension \(d \in \mathbb{N}\), where the component-wise ordering \(\leq\) is given by \(u = (u_1, \ldots, u_d) \leq v = (v_1, \ldots, v_d) \iff u_1 \leq v_1 \land \cdots \land u_d \leq v_d\).

Another well-known instance are the lossy channel systems [4, 7], where for simplicity we assume that the set of configurations is \((\Sigma^*, \leq)\) for some finite alphabet \(\Sigma = \{a, b, \ldots\}\) of messages, and where \(\leq\) is the subword ordering \(^1\) given by

\[ u \leq v \iff \exists a_1, \ldots, a_f \in \Sigma : \exists v_0, \ldots, v_f \in \Sigma^* : u = a_1 a_2 \cdots a_f \land v = v_0 a_1 v_1 a_2 \cdots a_f v_f. \]

Algorithms for the verification of safety properties of WSTSSs usually involve reasoning and computing with upward-closed and/or downward-closed sets of configurations. A set \(U \subseteq \text{Conf}\) is upward-closed \(^2\) if \(c \in U \land c \leq c' \implies c' \in U\), and there is a similar definition

---

\(^1\) That \((\Sigma^*, \leq)*\) is a WQO is known as Higman’s Lemma.

\(^2\) That \((\Sigma^*, \leq)*\) is a WQO is known as Higman’s Lemma.
for downward-closed subsets. These sets are usually infinite (like \(\text{Conf}\) itself) and symbolic representations or data structures are needed in algorithms handling them.

For upward-closed subsets, a well-known representation relies on the existence of minimal bases, i.e., the fact that the set of minimal elements of any subset is finite and unique (modulo equivalence). This representation is generic: it works for any WQO. Furthermore, it enjoys several nice algorithmic properties, e.g., testing inclusion between upward-closed subsets reduces to a quadratic number of comparisons between individual configurations, and the union of upward-closed sets is very easy to compute. In the case of \((\mathbb{N}^d, \leq_x)\) or \((\Sigma^*, \leq_\ast)\), algorithms for computing intersections reduce to easy computations of least upper bounds between elements.

For downward-closed subsets, one cannot rely on a mirror notion of maximal elements and this makes symbolic computations harder to envision. The question of finding a generic approach for computing with downward-closed sets was first raised in [14].

In the case of \((\mathbb{N}^d, \leq_x)\), a symbolic technique was popularized by Karp and Miller with their classic algorithm for coverability in VAS [19]. They define \(\mathbb{N}_\omega = \mathbb{N} \cup \{\omega\}\) —where the set of natural numbers is completed with a new infinite element \(\omega\) that is larger than any finite number— and consider \(d\)-tuples over \(\mathbb{N}_\omega\). It turns out that this is exactly what we need to represent downward-closed subsets of \(\mathbb{N}^d\). For \(\sigma = (s_1, \ldots, s_d) \in \mathbb{N}_\omega^d\), we let \(\downarrow \sigma = \{c \in \mathbb{N}^d \mid c \leq_x \sigma\}\) denote the downward-closed subset of \(\mathbb{N}^d\) generated by \(\sigma\) and call it an ideal of \((\mathbb{N}^d, \leq_x)\). Then downward-closed subsets of \(\mathbb{N}^d\) can be denoted in a unique way by finite unions of incomparable ideals. Computing unions and intersections with such representations, and deciding inclusion between them, use simple algorithms that are uncannily similar to what happened with the finite-basis representation for upward-closed subsets.

If we now consider \((\Sigma^*, \leq_\ast)\), a very elegant representation for downward-closed subsets was proposed by Abdulla et al. in [3]. They show that any downward-closed \(D \subseteq \Sigma^*\) can be represented by a simple regular expression (a SRE), obtained as a union of concatenations of atoms of the form \(\Gamma^*\) for a subalphabet \(\Gamma \subseteq \Sigma\), or of the form \(a^+ \epsilon\) for some letter \(a \in \Sigma\). Furthermore, these SREs support simple and efficient algorithms for unions, intersections, comparisons, and more.

It turns out that concatenations of atoms denote exactly the ideals of \((\Sigma^*, \leq_\ast)\). Formally, an ideal of a WQO \((X, \leq)\) is a nonempty downward-closed directed subset \(D \subseteq X\). Being directed means that for all \(x, y \in D\) there is some \(z \in D\) with \(x \leq z \wedge y \leq z\). Given any WQO \((X, \leq)\), the downward-closed subsets of \(X\) can be written as unions of finitely many pairwise incomparable ideals, and this decomposition is unique. This property explains the nice algorithmic properties we observed with \(\mathbb{N}^d\) and the SREs over \(\Sigma\), and it generalizes to any WQO where we can provide effective characterizations for the ideals.

In the second part of the talk, we show how such effective characterizations exist for most of the WQOs one encounters in practice. This is done by considering the most common ways of constructing new WQOs from previous ones (sequence extension, powerset, but also substructures and quotients) and characterizing the ideals of the new WQOs in terms of the ideals of the earlier ones.

We illustrate these constructions with lesser known WSTSs like priority channel systems [17], or data nets [20] and timed-arc Petri nets [5].

**Acknowledgments.** This talk is based on joint work with J. Goubault-Larrecq, S. Hhalfon, P. Karandikar, K. Narayan Kumar, S. Schmitz, and it has further profited from many discussions with A. Finkel, J. Leroux and G. Sutre. Most of the presented definitions and
results can be found in recent works like [6, 9, 10, 11, 16, 21, 22]. A full version of these notes is in preparation [15].

References


