1 An Example of Construction of a Lattice of Guarded Literals

To demonstrate the construction of a meet-semilattice from a set of equations and inequalities via a subset lattice, we use an algorithm for constructing a meet-semilattice of expressions from our previous paper [2] on a small set of equations. We do not change any algorithm related to the construction of the meet-semilattice as it is not the focus of this paper. The presentation is self-contained and aims to clarify the concepts of a non-contradictory sub-set of expressions, overlapping assumptions, a subset lattice and a meet-semilattice of expressions.

The actual meet-semilattices which were used in our experimental results, can be found at our web-page [1] as a pair of two files: a file of user-defined summaries (library of summaries), and a file of the meet-semilattice structure, which order the summaries in the former file. Any decision that was made here, was for the sake of the example; in the actual construction of the sine meet-semilattice we made different decision, mainly because we used ∼40 equations and inequalities of trigonometric definitions, identities and inequalities in our experiments, and not 3 identities as in this example.

It is the best to note that we did not use any of the lattices in this small example in our evaluation of the algorithms in this paper.

Construction of a Meet-semilattice Small Example. In the example, we augment the solver with a set of equations (with their guards) about the sin function, arranged in a meet-semilattice. These equations are taken from an existing set of lemmas of the Coq proof assistant [3] for $\sin x$:

$$f_1 \equiv \mathit{sin\_eq\_0\_0} \equiv$$

$$\equiv x = (k \cdot PI) \text{ with the assumption } \sin x = 0 \text{ for some positive integer } k;$$

$$f_2 \equiv \mathit{sin\_eq\_O\_2PI\_0} \equiv$$

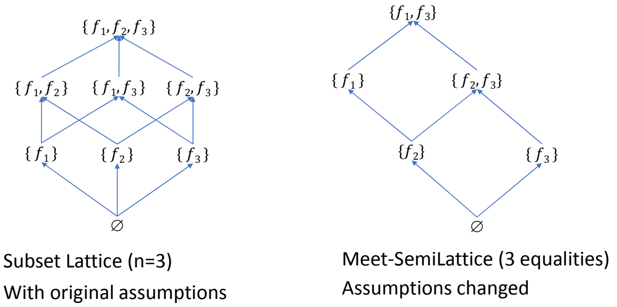
$$\equiv x = 0 \vee x = PI \vee x = 2 \cdot PI \text{ with the assumption } 0 \leq x \wedge x \leq 2 \cdot PI \wedge \sin x = 0;$$

$$f_3 \equiv \mathit{sin\_period} \equiv$$

$$\equiv \sin{(x + 2 \cdot k \cdot PI)} = \sin x \text{ with the assumption } \mathit{true} \text{ for some positive integer } k.$$

The original subset lattice consists of all subsets of the set $\{f_1, f_2, f_3\}$. It is analysed and reduced as described in [2] to remove contradicting expressions and equivalent elements. In this example, the set $\{f_2\}$ generalises $\{f_1\}$, and there are no contradictory expressions in the set $F_{\sin} = \{f_1, f_2, f_3\}$.

To construct the meet-semilattice from a subset lattice, we **removed** two equivalent elements: $\{f_1, f_2\}$ (that is equivalent as a formula to $\{f_1\}$) and $\{f_1, f_2, f_3\}$ (that is equivalent as a formula to $\{f_1, f_3\}$). Assumptions of the elements $\{f_2\}$ and $\{f_3\}$ **are re-written** to eliminate the case where two or more assumptions of elements of a unique meet, refer to the same input value (e.g., both elements referred to $\sin 0$). In that case, we added the negation of the assumptions of $\{f_2\}$ to the assumption of $\{f_3\}$; and for $\{f_1\}$ and $\{f_2, f_3\}$, we added the negation of the assumption of $\{f_2, f_3\}$ to the assumption of $\{f_1\}$, for the same reason (e.g., both elements referred to $\sin 0$ and $\sin PI$). The size of the meet-semilattice is smaller and contains half of the chains from minimal to maximal elements than the original subset lattice. The *maximal element* is $\{f_1, f_3\}$. In larger meet-semilattice we expect to have more than a single maximal element. With a large set of equations and inequalities, the size of the meet-semilattice is expected to be significantly small than the size of the original subset lattice as we reported in our evaluation with the meet-semilattices for sin and cos functions ($F_{\sin}$ was a set of $\sim$40 equations and inequalities of trigonometric definitions, identities and inequalities in the experiments of the LB-CEGAR algorithm.



Subset Lattice (n=3)
With original assumptions

Meet-SemiLattice (3 equalities)
Assumptions changed

Figure 1: *Original subset lattice and reduced meet-semilattice, for properties of the* sine *function in* LRA*.*

Figure 1 shows the original subset lattice on the left, and the resulting meet-semilattice of expressions on the right. In the lattice traversal, we start from the bottom element $\emptyset$ and traverse the meet-semilattice until we either prove that the program is safe or find a real counterexample (or show that a further theory refinement is needed) by using each iteration the guarded literals in the current element.

References

[1] http://verify.inf.usi.ch/content/trig_refinement

[2] Even-Mendoza, K., Asadi, S., Hyvärinen, A.E.J., Chockler, H., Sharygina, N.: Lattice-based refinement in bounded model checking. In: Verified Software. Theories, Tools, and Experiments - 10th International Conference, VSTTE 2018, Oxford, UK, July 18-19, 2018, Revised Selected Papers. Lecture Notes in Computer Science, vol. 11294, pp. 50–68. Springer (2018)

[3] The coq proof assistant. https://coq.inria.fr/