Datalog++

Magnus Madsen

# Proof Burdens

We are given the interval lattice , an abstract sum function and a widening function . We must now prove that:

1. That is a bounded join semi lattice:
   1. That is a partial ordering:
      1. is reflexive:
      2. is anti-symmetric:
      3. is transitive: .
      4. Bottom:
   2. exists and is a least upper bound:
      1. is total
      2. and
2. That sum is monotone:
   1. If and then
3. That is monotonic .
4. That is a widening: .
5. That, given a termination function , the image of the widening function has no infinite ascending chains.
   1. That is always non-negative.
   2. That is always decreasing.
   3. That satisfies :
      1. If then .
6. Distributivity

# Interval

The interval lattice is where

for any

for any

if and only if and .

**Partial Order?**

*Q0: Is it possible for an SMT solver to prove that the interval lattice is a partial order? In particular that the relation is:*

* Reflexive.
* Anti-symmetric.
* Transitive.

TBD: But, I think yes.

**Join?**

Prove that the least upper bound exists (join should be total) and that it really is a least upper bound according to the ordering.

**Sum**

We define the abstraction sum function as:

and

and

**Monotonicity**

*Q1: Is it possible for an SMT solver to prove that the sum function is monotone?*

Prove: If and then:

We can expand the above constraint to get:

And putting it together with the definition of :

and

and

, , and

which should be provable with linear arithmetic.

**Finiteness of Widening**

Define the widening function by:

*Q2: Is it possible for an SMT solver to prove that there are no infinite ascending chains?*

Let disprove that exist in :

Idea: Require the programmer to provide a termination function, i.e. a function which is:

* Always non-negative.
* Always decreasing.

For example, we could give the termination function:

We now need to prove the following:

1. The widening function satisfies .
2. The termination function is always non-negative and decreasing.

What exactly do we mean by a)? We mean that if then . This should be provable using linear arithmetic by expanding the definitions.

Proving b) looks more tricky, but if we add the constraint then it should be possible, similar to the above

If we believe the above works then we can immediately generalize to the abstract minus function. Multiplication and division, on the other hand, might not be provable. What else? We should be able to handle the sign lattice, polarity lattice and constant string lattice since these are weaker than the interval lattice.

What are some other lattices/domains to consider?

* Pentagons? (A slight generalization of intervals)
* Octagons? (probably not)
* Polyhedra? (probably not)
* Pointers?

**Work in Progress Questions:**

* How does monotonicity compose?
* How does widening compose?