Modular Static Analysis using SMT

Julien Henry

February 13, 2013

Algorithm 1 Modular Static analysis using SMT

```
function IORelation(Block $B(X, X')$, Property $P(X')$)
    while SMTsolve($X \wedge B(X, X') \wedge \neg P(X')$) do
        $M \leftarrow$ getModel()
        $(B_1, \dots, B_n) \leftarrow$ AbstractedBlocks($M$)
        Refine($B_1, \dots, B_n, M$)
        Update($B(X, X')$)
        if Refine has not updated anything then
            return $(B(X, X'), unknown)$
        end if
    end while
    return $(B(X, X'), true)$
end function

function Update(Block $B(X, X')$)
    Compute $B^{over}(X, X')$ using one of S, G, PF, DIS techniques
    Possibly refine $B^{under}(X, X')$
end function

function Refine(Block $B_1(X_1, X_2), \dots, B_n(X_n, X_n + 1)$, $M$)
    $res \leftarrow false$
    while $res \neq true$ do
        if $M(X_{i+1}) \nsubseteq B_i^{under}(X_i, X_{i+1})$ then
            $res \leftarrow$ IORelation($B_i(X_i, X_{i+1}), M(X_{i+1})$)
        end if
    end while
end function
```

Some comments on Algorithm 1 :

- IORelation
    - We want to refine the invariant $B(X, X')$ so that the property $P(X')$ becomes true.

  - We find a path that goes outside $P(X')$, and try to refine the precision of the abstracted blocks we go through. Once we have refined abstracted blocks, we recompute $B(X, X')$ (it should be smaller than the previous one, we can also intersect with the previous one).
  - We keep doing this until the property becomes true. At some point, we may return *unknown*.

- Update
  - This function recomputes an invariant for the block B, using a technique we choose from S, G, PF, DIS. In this way, we can strengthen the invariant incrementally when the previous one is not sufficient.
  - We should also keep an underapproximation of B to avoid refining useless blocks. This underapproximation can start at $\bot$ and be updated incrementally.

- Refine
  - We have a list of blocks that may be interesting to refine. We also have the model of the trace going wrong.
  - If the model fits with the underapproximation of a block B_i, there is no hope to cut the trace by refining B_i. More generally, we could temporarily replace in $B(X, X')$ the invariant $B^{over}(X_i, X_{i+1})$ by $B^{under}(X_i, X_{i+1})$, and see whether $B(X, X') \wedge P(X')$ is still *sat*. If so, we do not refine it.