Natural Proofs for Data-structure Manipulation in C

Link: http://madhu.cs.illinois.edu/pldi14-NatProofsForC.pdf

Presented Work:

In this work, they developd a framework called VCD RYAD thatextends the V CC framework to provide an automated deduc- tive framework against separation logic specifications for C pro- grams based on natural proofs. We develop several new techniques to build this framework, including (a) a novel tool architecture that allows encoding natural proofs at a higher level in order to use the existing VCC framework (including its intricate memory model, the underlying type-checker, and the SMT-based verification infras- tructure), and (b) a synthesis of ghost-code annotations that cap- tures natural proof tactics, in essence forcing VCC to find natural proofs using primarily decidable theories.

Related Work:

The natural proof technique for heap verification developed by Qiuet provides a platform for powerful sound reasoning for specifications written in a dialect of separation logic called Dryad. Natural proofs are proof tactics that enable automated reasoning exploiting recursion, mimicking common patterns found in human proofs. However, these proofs are known to work only for a simple toy language.

Future Work:

However, natural proofs currently do not work for data-structures that cannot be defined recursively (such us DAGs, graphs, etc.). We have been able to prove some properties of Schorr-Waite algorithm only for trees, but not for general graphs. Several future directions are interesting. First, it would be in- teresting to see how VCD RYAD can be used for verifying larger pieces of code, and how the programmer's manual interactions for proving more complex properties can be orchestrated with the automatically generated annotations provided by VCD RYAD . Second, while the current work has focused on automatic proof tactics, loop invariants (and strengthening pre/post conditions so that they be- come inductive) is a hard task for the programmer, and automating this, especially for DRYAD specifications, would advance the us- ability of deductive verification tools further.