Integrating Programs and Logic

New Ideas

• Building a distributed communications system in a very expressive programming language with a formal semantics is the key first step for proving properties of actual system code.

• The key to effectively supporting a real system with formal methods is to build the system in a programming environment that seamlessly integrates proof technology.

• The modular structure of Ensemble enables collaborative verification based on a common formal semantics definable in several verification systems.

Impact

• Delivery of a means to correctly optimize Ensemble layers will demonstrate that formal methods can enhance real system performance.

• Proving the defining properties of key Ensemble layers will greatly enhance confidence in that system and its applications as well as increase its capabilities.

• Release of Ensemble with a Logical Programming Environment to support it will be a first-of-a-kind model of how a system can be formally supported.

Schedule

1998
Spring
• Deploy a correctly optimized stack in a running application.

Fall
• Complete verification of ETO layer in Nuprl, specify EVS layers, add to documentation of system.

1999
Spring
• Integrate Ensemble into prototype Logical Programming Environment (LPE).

Fall
• Begin formal proofs of EVS properties.

Complete proofs of EVS properties; add to documentation base for system.

2000
Spring
• Integrate fastpath optimizer from Nuprl into LPE.

Fall
• Synthesize correct Ensemble layer from correctness proof.

Release integrated LPE for Ensemble with formal documentation libraries and packaged layer optimizer.