Consistency and Completeness of Specs

Property verification is predominantly used in two forms in pre-silicon validation, namely (a) Formal Property Verification (FPV), and (b) Assertion-based Validation (ABV). In both forms, the properties are written in a formal specification language. FPV techniques formally verify whether *all* possible behaviors of the design satisfy the given properties. ABV is a simulation-based approach, where the properties are checked over a simulation run – the verification is thereby confined to only those behaviors that are encountered during the simulation.

The first task in both FPV and ABV is to write a set of formal properties that cover the design intent – these properties represent the formal design specification. Recent experience shows that this is a non-trivial task even for an engineer who is familiar with the property specification languages. The most dominating questions that must be addressed while developing a property suite are:

- ***Are my properties consistent?*** If not then the property may fail on a valid design, and the validation engineer will have to debug both the specification and the implementation in order to isolate the problem.

- ***Have I written enough properties?*** If the answer to this question is negative, then we have a more serious problem. All the properties may pass on an invalid design because the erroneous behavior was not covered by the incomplete set of properties.

New technology developed by the Formal-V group enables the designer to verify the satisfiability, realizability and sanity of a given specification. We have also addressed the coverage problem and proposed a new style of coverage analysis for property specifications. The proposed approach analyzes the completeness of a specification against a fault model. It is applicable both in FPV as well as in ABV.

Publications out of this work:

1. Das, S., Banerjee, A., Basu, P.,Dasgupta, P., Chakrabarti, P.P., Mohan, C.R., Fix L., Formal Methods for Analyzing the Completeness of an Assertion Suite against a High-Level Fault Model, In Proc. of VLSI 2005

2. Roy, S., Das, S., Basu, P., Dasgupta, P., Chakrabarti, P. P., SAT-based solutions for Consistency Problems in Formal Property Specifications for Open Systems, In Proc. of ICCAD 2005

3. Das, S., Basu, P.,Dasgupta, P., Chakrabarti, P.P., Syntax-driven approximate coverage analysis for an assertion suite against a high-level fault model. In Proc. of VDAT 2005.