Exploration by model-checking of timing anomaly cancellation in a processor

Topic	Hardware model, formal methods, real-time systems, timing analysis
Lab, city and country	VERIMAG, Grenoble, France
Team in the lab	Shared Resources
Advisors	Lionel Rieg, Catherine Vigouroux — first.last@univ-grenoble-alpes.fr

General presentation of the topic In planes and cars, any failure may lead to injuries for driver or passengers. For these critical systems, correct operations also means satisfying some temporal constraints (for instance, answering within 50ms). In order to ensure these timing constraints, one must prove that their Worst Case Execution Time (WCET) is bounded. Static timing analysis is composed of hardware and software model to estimate a bound on this WCET. For dynamic behaviour such as out-of-order execution, building a static model may lead to accuracy and complexity issues.

Static timing models are built by composing smaller models for each component of the system. Such a composition is meaningful provided the global worst-case scenario can be built from local worst-case scenarios for each component. Unfortunately, this assumption may be wrong due to timing anomalies. A timing anomaly happens whenever a local worst-case behaviour (a cache miss, for instance) leads to a shorter global execution than the local best case (a cache hit may cost more). In the case of a cache hit, this may happen if the access is terminated earlier and a time window is free for executing something else in the pipeline that will impact the total execution time. A timing anomaly may happen even for in-order processors, in which instructions are not reordered.

Objective of the internship The objective of this internship is to develop a processor model to explore timing anomalies and their long-term effects. Our previous experiments suggested that the total execution time increase is often quickly cancelled: later instructions do not exhibit it. Furthermore, when assessing safe bounds for WCET, the conflicts between several components are taken into account by interference delays. In practice, these interference delays are big enough to encompass the effect of timing anomalies. Thus, it may not be necessary to consider an extra margin for them.

In this internship, the focus will be on the exploration of the impact of timing anomalies beyond the initial occurrence of the timing anomaly, likely using a model-checker (but other tools may be considered). A model checker is a tool to formally verify properties, stated as logical formulas, on a model. We also plan to target a model for a real hardware platform, going further than our current small in-order processor model.

The main question is at which level should the model be designed in order to stay accurate while keeping the complexity low enough for practical usage. The state of the art covers these topics: WCET analysis, timing anomaly definition and hardware model by model checking. In this internship, there is both a theoretical part with the study of a convenient model and its implication on long-term behavior of timing anomalies and a practical part with the implementation of the corresponding model in a model-checker to formally validate the claims.

Bibliographic Reference J. Eisinger, I. Polian, B. Becker, S. Thesing, R. Wilhelm, and A. Metzner. 2006. *Automatic Identification of Timing Anomalies for Cycle-Accurate Worst-Case Execution Time Analysis.* (DDECS'06)

Benjamin Binder, Mihail Asavoae, Florian Brandner, Belgacem Ben Hedia, and Mathieu Jan. 2022. *The Role of Causality in a Formal Definition of Timing Anomalies.* (RTCSA'22)