Strategy and five-year project

VALS

Strategy and five-year project

Following the general policy of the LRI that suggests to group similar activities in larger teams, we decided to join the former teams ForTesSE and Toccata. The name of this new team is VALS, standing for "Verification/Validation of Algorithms, Languages and Systems". We detail below why this fusion makes sense in a scientific point of view.

VALS team members

The new team is directed by Burkhart Wolff, aside with Claude Marché as co-director.

Permanent Members (October 1st, 2013)			
Name	*First name*	*Position*	*Institution*
BENZAKEN	Véronique	PREX	PARIS SUD
BOLDO*	Sylvie	CR1	Inria
CHARGUÉRAUD*	Arthur	CR2	Inria
CONCHON*	Sylvain	PR2	PARIS SUD
CONTEJEAN*	Évelyne	CR1	CNRS
FILLIÂTRE*	Jean-Christophe	CR1	CNRS
GAUDEL	Marie-Claude	PR émérite	PARIS SUD
LONGUET	Delphine	MCF	PARIS SUD
MANDEL**	Louis	MCF	PARIS SUD
MARCHÉ*	Claude	DR2	Inria
MELQUIOND*	Guillaume	CR1	Inria
NGUYEN	Kim	MCF	PARIS SUD
PASKEVICH*	Andrei	MCF	PARIS SUD
PAULIN-MOHRING*	Christine	PREX	PARIS SUD
VOISIN	Frédéric	MCFHC	PARIS SUD
WOLFF	Burkhart	PR1	PARIS SUD
ZAÏDI	Fatiha	MCF	PARIS SUD

* member of the LRI-Inria joint team Toccata, directed by C. Marché.
** currently on leave ("détachement") at the Collège de France.

Temporary Personnel (October 1st, 2013)			
Name	*First name*	*Position*	*Institution*
AÏSSAT	Romain	Doc.	PARIS SUD (AM)
CLOCHARD	Martin	Doc.	ENS Paris
DROSS	Claire	Doc.	AdaCore (CIFRE)
DUMBRAVA	Stefania	Doc.	PARIS SUD (AM)
FELIACHI	Abderrahmane	Post-doc	EURO-MILS
GONDELMAN	Léon	Doc.	PARIS SUD (ANR BWare grant)
IM	Hyeonseung	Post-doc	PARIS SUD (ANR Typex grant)
KHEFIFI	Rania	Doc.	PARIS SUD (CDD)
LELAY	Catherine	Doc.	Inria (Digiteo PhD grant)
MARTIN-DOREL	Erik	Post-doc.	Inria (ANR Verasco grant)
MEBSOUT	Alain	Doc.	PARIS SUD (AM)
NEMOUCHI	Yakoub	Doc.	PARIS SUD (CDD)
NGUYEN	Huu Nghia	Doc.	PARIS SUD (AM)
TAFAT-BOUZID	Asma	Post-doc	PARIS SUD (ATER)
TUONG	Frédéric	Doc.	IRT SystemX (CDD)
WENZEL	Markus	Post-doc	ANR Paral-ITP

Self Assessment

Strengths: One of the particular strengths of both former teams ForTesSE and Toccata are their tradition of combining theory and practice, fundamental and applied research. Their research ranges from semantic models for specification- and programming languages, over concrete know-how in automated and interactive theorem-prover technology, down to the design and implementation of recognized tools and tool-chains for a variety of verification techniques. Successful applications, partly in collaboration with industrial partners, demonstrate that VALS will belong to the global players in the field of applied formal methods.

Both former parts of the VALS team have a strong national and international network with academic and industrial partners. We engage in various ANR and European projects. We also have intense local cooperation with major scientific players on the plateau de Saclay such as the CEA; here lies the key for its success in the development of recognized formal methods tools in an academic environment, together with the fact that it attracted a high number of permanent researchers.

Both former parts of VALS have a strong publication record and a high academic recognition in their respective fields, which is reflected in the participation of numerous program committees and conference organizations.

We'd like to add that we enjoy our collaborative style of research and the vividness of our group.

Weaknesses: While VALS has a clear focus on the foundational research axes, it can be asserted that its efforts in the various application domains is quite scattered driven by a perhaps too large variety of partnerships and collaborations. It would be desirable if the number of collaborations could be reduced to a smaller number of larger/more intensive partnerships.

With respect to the former Toccata part of the VALS team, it was criticized in the past that its collaborations are too French-centric. It was also recommended to address fundamental computing trends like concurrency more actively.

With respect to the former ForTesSE part of the VALS team, it can be criticized that its permanent staff is slightly over-aged, and needs a more active recruiting strategy to attract strong personal and to achieve a size which is more sane. It is particularly desirable that full-time researchers join the team on testing issues.

In order to maintain the quality of tools and documentation, the team should be reinforced by engineers.

Opportunities: The world of computing is changing: becoming ubiquitous, there are larger, more complex and more safety- and security-critical software systems whose quality must be assured by appropriate verification technologies. This is reflected by the growing demand for formal certification processes, e.g. Common Criteria ISO/IEC 15408 require the use of formal methods, both in Test and Proof, as developed in VALS.

Finally, it can be observed that there is for all tools (Frama-C, SparkAda, Isabelle, HOL-TestGen) an increasing number of users — reflected both by downloads and mailing list traffic.

New computing architectures — parallel / grid / cloud — represent new ways to master the inherent complexity of symbolic computing as is fundamental for the technologies developed in VALS. Such changes of basic technologies will have a profound effect both on verification methods, their demand by industrial partners, as well as their implementation.

Last but not least, we view the changes of the academic environment (catchword: Université Paris-Saclay) as a means to integrate verification engineering into traditional software engineering, which can be anchored more intensively into the bachelor and master programme of this institution — a way, to instruct and attract new scientific staff.

Threats: Advancing both fundamental research *and* tool development in an academic environment puts a team inevitably under a certain stress: Development of research tools is time-consuming and not always rewarding in terms of publications. While both former parts of VALS managed this balancing act quite well in the past, it can be safely stated that the complexity of underlying technology (e.g. multi-core architectures) and the demands of wider user groups (user interfaces, documentation) is growing. There is a perceivable threat that in the competition with industrial research institutions such as Microsoft Research, VALS might be outperformed simply by their investments both in terms of time and money. Just an example for the kind of concurrency we face: the white-box fuzz-testgeneration tool SAGE uses a ca. 100 man year effort involving a massive parallel server farm to solve billions of constraints by Z3; the approach is used to systematically detect errors in Win7, Windows and Office.

As mentioned earlier, it is particularly difficult to attract PhD students and scientific staff that fits into our profile: the necessary combination of mathematics, logic and software engineering is difficult to find on the national and international market of applicants.

In principle, the underlying technologies of our research are remarkably computing intensive, which is a problem when scaling-up to industrial size systems. An obvious answer to this threat are new computing paradigms (massive parallel computing, multi-core and grid computing); in order to cope with these trends, additional training and personnel will be necessary.

Strategy

Why does the fusion make sense? Test and proof, originally perceived as adversaries, have a lot in common in leading edge approaches: as "formal methods" (FM), they have both their roots in logic and discrete mathematics, and they share an interest in formal semantics for programming and specification languages, in modeling-approaches for programs and systems, as well as constraint-solving technologies and theorem provers. This mutual interest is reflected by recent collaborations between Toccata and ForTesSE (the Cubicle project). Last but not least, we identified a set of challenges that both former parts of the team would like to address together, listed below.

General objectives. We identified the following general trends in the scientific community that corresponds to our potential in the new VALS team:

1. making verification an easier to use, more wide-spread technology ;
2. gaining experience in non-standard application domains, for example hybrid and concurrent systems ;
3. advancing the prover technology: e.g. by non-linear arithmetic and parallel prover design ;
4. combining test and proof, e.g. by invariant-generation, verified optimized test-generations, etc. ;
5. combining proofs and probability.

We believe that the fused VALS team is an adequate structure, joining complementary skills and expertise of its members, to address these objectives. The detailed scientific programme below corresponds to

the way we plan to implement solutions to these objectives.

Scientific Programme

The scientific programme of VALS is structured into six activities. We detail each of these activities below, together with the list of participants. We then provide a list of a few challenges that we want to address in the future. The interest in those challenges is shared between the former parts of the team. We then discuss the application domains we target, and finally give a few elements of positioning.

Activities

Automated Deduction. Participants: S. Conchon (contact), F. Zaïdi, E. Contejean, G. Melquiond, A. Paskevich.

Automated Theorem Proving and its applications will remain an important activity of the team. This includes research around satisfiability modulo theories (Alt-Ergo prover), numerical constraint solving (Gappa solver), and applications like SMT-based model-checking (Cubicle).

Verified Computer Arithmetic. Participants: S. Boldo (contact), G. Melquiond, C. Marché, B. Wolff.

The research around numerical programs took a lot of importance in the past 5 five years in particular in Toccata. We want to pursue these efforts, towards several directions such as the verification of numerical analysis systems, hybrid systems.

Formalisation of Languages. Participants: B. Wolff (contact), E. Contejean (contact), A. Charguéraud, D. Longuet, V. Benzaken, Ch. Paulin, C. Marché, S. Boldo.

Formalizing in a broad sense is indeed an activity of all members of former teams, in particular using assistants like Coq and Isabelle. It will continue in the future, for formalizing semantics of languages, concurrency, mathematical/numerical theories, etc.

Data-Centric Languages and Systems. Participants: V. Benzaken (contact), K. Nguyen, E. Contejean. This activity aims at designing and developing programming languages as well as systems that seriously take into account massive data. This includes improving existing languages and systems. Ultimately it aims at providing formally verified implementations of data intensive management systems.

Formal Model-based Testing. Participants: F. Zaïdi (contact), B. Wolff, D. Longuet, F. Voisin, M.-C. Gaudel. Testing will remain a strong research activity of the team. Important directions will be to scale up testing techniques by handling efficiently the concurrency aspects of distributed systems (for instance Web services, wireless self-organised networks, etc.) as well as by advancing symbolic and probabilistic approaches. Moreover, we will investigate how to overcome the infeasible paths issues for the test of C programs by finding suitable combinations with static analysis methods.

Deductive Program Verification. Participants: J.-C. Filliâtre (contact), A. Charguéraud, A. Paskevich, C. Marché, G. Melquiond, Ch. Paulin, B. Wolff.

Our approach of deductive program verification is in need for improved techniques for modular reasoning, support for genericity, for higher-order programs, for refinement-based approaches. This is a key towards scaling-up, in particular via the development of reusable verified libraries.

Transverse challenges we want to address, shared by both former teams

Non-linear arithmetic. Critical software often involves numerical computations on physical quantities. *Hybrid systems* are those which mix continuous quantities and discrete ones. Such a system can be modeled typically by transitions systems guarded by numerical constraints. In all cases, the constraints involved are usually non-linear ones, hence both in the contexts of testing and proving, it is desirable to rely on automated decision procedures able to check the satisfiability of such kind of constraints.

Parallelism and verification. The challenge raised by parallelism in the context of verification is two-fold: a challenge as a target as well as an implementation means of verification tools. Testing of concurrent programs requires the definition of efficient architectures for distributed testing. Besides the challenge of modeling concurrence, already addressed in the activity *Formalisation of Languages*, there is the necessity to profit from advances in recent hardware: since 2005, there are no further increases of CPU clock-rates; increasing computing power can only be gained by addressing multi-core and grid computing platforms. This represents a sensible paradigm shift both in algorithmic design as well as system architecture.

Combination of dynamic and static analysis. Combining the respective power of dynamic methods (test, run-time checking) ans static analysis is an interesting research direction per se, and is certainly a way to leverage adoption of formal methods in industry. It is indeed required in certification processes in industry. We already have short-term plans to go in such a direction, in the context of platforms like Spark2014 for Ada, Frama-C for C code (and its executable-ACSL specification language), but also in our own platform Why3 for which we plan to provide an environment for directly executing annotated programs.

Verified languages, systems and tools An emerging trend is the verification of the analysis tools themselves, as exemplified by the CompCert verified compiler. The assurance level provided by a system is directly related the size of its *Trusted Code Base*, i.e. the core of the system that is not verified, the remaining being verified on top of that core. Libraries (e.g. Flocq, ALEA) and tools (e.g. HOL-TestGen) built on top of assistants (e.g. Coq, Isabelle/HOL) have a small TCB, whereas standalone tools (e.g. automated theorem provers) have a large one. This challenge aims at reducing the TCB of such tools to small cores, thus producing "verified" tools. We target the development of verified theorem provers, verification condition generators, interpreters, compilers including compilers for data-centric languages, etc.

Probabilities and Verification Scaling-up to large size systems is always a challenge for formal methods. The use of randomized methods is a very promising approach to solve scaling-up issues, ensuring a probabilistic guarantee of the results. Randomized methods have a great potential to apply on many domains including formal testing and proving. Besides, studying verification of randomized programs and systems, which have important application in security, must be continued.

Application areas

VALS will continue to seek for academic and industrial partners to advance and apply its technologies; this covers in particular projects concerning code-verification (in particular numeric algorithms involving floats), security infrastructures, web services, embedded and operating systems, etc. We will try to find more strategic partnerships with companies and larger shares in research projects.

Positioning in the local, national and international context

The domain of formal methods for software engineering is historically a major axis of research in the LRI. This domain of research is important in the context of the institutional evolutions of the "Plateau de Saclay", in the recent past, the present and for the future. In the past years, the RTRA Digiteo played an important role for the development of collaborative research on the Plateau, and Software Engineering was one of its seven themes of its research programme. In the present, software was also important in the "investissements d'avenir": SciLex is one of the three action lines of the Labex DigiCosme, centered on the reliability of software ; the IRT SystemX, which is more focused on industrial applications, has one theme around embedded systems, where the same problematic appears. We are strongly involved in all these actions.

The near future is the creation of the Université Paris-Saclay, and the creation of a large computer science department. The interest in formal software engineering methods will be shared by several institutions: Inria Saclay, CEA, LSV, ENSTA ParisTech, etc. The new VALS team aims at playing a central role is this future join of forces on the Plateau. Also, we are strongly involved in the new Master programme of the future STIC department. This would be a new mean to attract students, e.g. from engineering schools, to do a PhD thesis.

Our strategy also fits in the national context. We are members of both GDR of CNRS "Génie de la Programmation et du Logiciel" and "Informatique Mathématique". We will continue collaborations with

many teams in France. At the international level, we want to develop our contacts with major institutions and sites of our domain, such as Microsoft Research, ETH Zürich, Imperial College London, etc. Our involvement in the IFIP WG 1.9/2.5 is also representative of our involvement in world-wide trends.

We plan to continue and improve our collaborations with industrial partners, in particular the companies that promote formal methods. These collaborations are not only a precious source of concrete challenges and real case studies: they are a key for the spreading and the transfer of our methods and tools in the industry.