Scientific Report

regarding the implementation of the project

PN-II-ID-PCE-2011-3-0439

from October 2011 to October 2013

The implementation of the project during the period October 2011 to October 2013 was performed within the three objectives specified in project proposal:

I. Foundations of structured specifications;

II. Universal approach to formal verification; and

III. Institution theoretic approach to logic combination.

1 Foundations of structured specifications

Research under this objective focused on the introduction of a new approach to the theory of structured specifications that is based on a new level of abstraction, and that includes the study of technical fundamental properties that are necessary for the structuring of programs and specifications. The results obtained are the subject of works [12, 15, 5, 6]. The main technical contributions are as follows:

1. The definition of the concept of *abstractly* structured institution as a special case of the concept of institution morphism [24]. This represents a general framework for the theoretical study of structured specifications and of software that provides both independence of any particular choice of structuring operators (hence this is applicable to a wide range of structuring formalisms) and the unification of the two major theoretical approaches to structuring: Goguen and Burstall's, property oriented [24], and that of Sannella and Tarlecki, model oriented [31, 32].

2. Theorems of existence of colimits and of model amalgamation by lifting from the level of the base (logical) institution to the level of the the institution of abstract specifications. These are the two technical properties that bear the greatest importance in the theory of structured specifications.

3. Development of the concept of 'normal form' for abstract structured specifications, and based on the existence of normal forms (see [32]), the development of lifting results of important logical properties from the base institution to that of the structured specifications; these include compactness, interpolation, and complete proof systems.

4. The introduction of the concept of *comorphism of abstractly structured institutions* by extending the well known concept comorphism of institutions [?]. This formalizes the intuitive idea of coding a theory of structuring specifications (such as that of Goguen and Burstall) into another structuring theory(such as that of Sannella and Tarlecki), the latter being supposed to be more complex. It is this defined a category of abstractly structured institutions, whose role is essential for the development of heterogeneous specification languages that can vary both the core logic and also at the level of the structuring mechanism; the second dimension of the structuring of specifications is not considered, for example, in languages such as CafeOBJ [17] and HetCasl [30].

5. The development of an automatic construction of 'simple' comorphisms of institutions from comorphisms of abstractly structured institutions, as well the investigation of some of the most important properties of these encodings: conservativness, amalgamation of models [3] and liberality [26, 10].

6. The development of the concept of pushout-style parameterization with 'sharing' (the body of the the parameterized specification and the instance of the parameter may have nonempty intersection) within abstractly structured institutions as appropriate generalization of the respective concept developed in [16].

7. The generalization of the concept of 'inclusion system' [18] to 'quasi-inclusions' by relaxing the partial order condition to a preorder; this allows their lifting from the level of the category of signatures of the base institution to that of the category of abstract specifications, i.e. the category of signatures of the abstractly structured institution. The main reason for this concept is the impossibility of this lifting in the case of the inclusion systems.

8. The study of free extensions of morphisms (of signatures) along quasi-inclusions. Free extensions of signature morphisms is the main technical tool in the study of instantiations of multi-parametric specification with 'sharing'.

9. The study of parameterized objects and their instantiations in categories with a distributive system of quasi-inclusions.

10. The study of functors for parameterization in abstractly structured institutions so as to lift colimits and quasi-inclusion systems.

11. Theorem of isomorphism between the results of sequential instantiation and of parallel instantiations for multi-parametric abstractly structured specifications. This is a double-extension of the main result of [16]:

12. extension to the abstractly structured institutions, introduced in [12], and

13. extension of the concept of 'sharing' to allow 'sharing' situations between different parameters for multi-parametric specifications.

14. Existence theorem for pushouts of morphisms of signatures in the institution of hidden sorted algebras (called $\underline{HA}$). The existence of pushouts in the category of signatures is the most fundamental property in order to have structuring specification system based on that logic.

15. Theorem of existence of an inclusion system for the category of $\underline{HA}$ signatures by lifting the strong inclusion system of the category of signatures of the institution of many-sorted algebras (denoted $\underline{MSA}$). This result provides the possibility to develop the concept of import of modules for structured behavioural specifications.

16. The proof of idempotency, commutativity and of associativity of the union of signatures in $\underline{HA}$, all of which are partial algebraic rules because of the partiality of the union of signatures in $\underline{HA}$.

17. The proof of the distributivity of union over intersection for signatures in $\underline{HA}$ as a partial algebraic conditional rule.

18. The development of the concept of 'abstract behavioural specification' based on the concept of abstractly structured institution [12] over $\underline{HA}$. This ensures a concept of behavioural specification general enough to not depend on any particular choice of a set of structuring operators, making it applicable to a wide range of structuring formalisms for behavioural specification languages.

19. The proof of partial algebraic rules for abstractly structured behavioural specifications based on the algebraic properties of the union of signatures in $\underline{HA}$.

2 Universal approach to formal verification

Research under this objective so far has had two main directions: the lifting of the logic programming paradigm to service-oriented computing, and study of formal verification of systems specified in hybridized logics by translation to first-order logic. The results obtained are the subject of the works [8, 7, 19]. The main technical contributions are as follows:

1. The definition of algebraic structures appropriate for the study of modules specific to the service-oriented computing paradigm [23] – both from the static perspective, refereeing to the structure of the modules, and dynamic, refereeing to the manner in which modules interact (service discovery and binding).

2. A parameterized construction (by an arbitrary logic) of an institution of *asynchronous* relational networks that allows to define service specifications, of models of these specifications – corresponding to orchestration of components that depend on external services – and of the process of searching for services and of their connecting components to the applications executed by clients.

3. Establishing a rigorously founded theoretical analogy between service-oriented computing [23, 22] and classical logic programming [27]. This analogy involves developing a general theory of logic programming, through which we can identify

4. the concept of Herbrand universe with orchestration class without external requirements, called “ground”,

5. variables with the so-called service requirements,

6. terms with service delivery through ‘ports’,

7. clauses with modules corresponding to services,

8. queries with applications executed by clients,

9. logic programs with service repositories, and

10. derivation by resolution with the mechanism dedicated to discovering of services and their connection to the applications.

The following results are shared with the objective *Institution theoretic approach to logic combination*:

11. Encoding abstract hybridized institutions into first order logic ($\underline{FOL}$) by lifting abstract comorphisms $\mathcal{I} \to \underline{FOL}^{\mathrm{pres}}$ (where $\underline{FOL}^{\mathrm{pres}}$ means the institution of $\underline{FOL}$ theories) to comorphisms $\mathcal{HI} \to \underline{FOL}^{\mathrm{pres}}$ (where $\mathcal{HI}$ means a hybridization of $\mathcal{I}$). If $\mathcal{HI}$ means a logic combination between traditional hybrid logic [1] and the logic/institution $\mathcal{I}$, then the resulting comorphism $\mathcal{HI} \to \underline{FOL}^{\mathrm{pres}}$ is a combination of the encoding given by the initial comorphism $\mathcal{I} \to \underline{FOL}^{\mathrm{pres}}$ and the standard encoding [4] of traditional hybrid logic into $\underline{FOL}$.

12. Theorem lifting the conservativeness property of the base comorphism $\mathcal{I} \to \underline{FOL}^{\mathrm{pres}}$ to a comorphism $\mathcal{HI} \to \underline{FOL}^{\mathrm{pres}}$. The main implication of this result is ability to shift a formal verification in $\mathcal{HI}$ to one in $\underline{FOL}$, with the advantage of using highly developed technologies for formal verification in $\underline{FOL}$.

13. Case study of a formal specification in a hybridization of partial algebras containing both the translation in first order logic and the formal verification of some properties of the specification through encoding in first order logic and by using the theorem provers [35] and Darwin [2].

3 Institution theoretic approach to logic combination

The research under this objective was to study hierarchical combinations of logic systems, as well as their semantic (model theoretic) and proof theoretic properties. This was done on the directions of hybridized logics and of many-valued logics. The results obtained are the subject of the works [14, 13, 19, 9, 20]. The main technical contributions are as follows:

1. New definition of combination between hybrid logic and any other logic by internalizing the concepts of hybrid logic at the level of abstract institutions. This process, called *hybridization* of institutions is developed both at the syntactic and the semantic levels. It extends the internalisation of Kripke semantics developed in [21, 28] with the concept of constrained *models*, which is axiomatized as a subfunctor (satisfying some specific

properties of rather general nature) of model functor in the hybridized institutions with unconstrained models. Hybridized institutions with constrained models accomodate a large class of hybrid logics from the literature in which different types of 'sharing' between semantic entities are considered. An important parameter of the process of hybridization consists of an axiomatization of the quantification space, a general approach that, due to the concept of constrained models, includes a great diversity of kinds of quantification from the literature.

2. The proof of the Satisfaction Condition for hybridized institutions with constrained models.

3. Definition of the concept of quasi-variety of categories models in hybridized institutions, a process that has two aspects:

   3.1. The definition of the concept of sub-model in hybridized institutions based on the concept of *inclusion system*. The inclusion systems for categories of models in the base institution are lifted up to the hybridization by means of a flattening construction of the Grothendieck category kind.

   3.2. The construction of direct product of models in hybridized institutions from the direct products of models in the base institution.

4. Preservation results (of the satisfaction relation between models and sentences) by sub-models and direct products in hybridized institutions.

5. The derivation of a general result of existence of initial models of theories in hybridized institutions. This result allows for a specification methodology based on initial semantics in a variety of combinations between hybrid logic and other logics.

6. The development of concrete examples of hybridization that can be used in formal specifications of dynamic systems. These examples include both traditional and new examples of hybrid logic, such as hybridization of logics with partial functions.

7. The definition of a general abstract framework (called $\mathcal{I}(L)$) for the description of many-valued semantics. In $\mathcal{I}(L)$ the residuated lattice of the truth values L is fixed but considered abstract, the atomic syntax (the signatures category and the functor of the atomic sentences) is also considered completely abstract, while the model categories and the satisfaction relation $\models$ are defined generically. From the perspective of the problem of combining logical systems, $\mathcal{I}(L)$ can be considered a combination of traditional many-valued logic [25] (called $\underline{MVL}$) with different logics whose atomic syntax atomic are an instance of the abstract atomic syntax of $\mathcal{I}(L)$.

8. Proof that $\mathcal{I}(L)$ is an institution [24]; in particular the proof of the Satisfaction Condition for $\mathcal{I}(L)$.

9. Theorem of a conservative embedding of $\underline{MVL}$ into $\mathcal{I}(L)$, the main implication is that for L fixed the semantic deduction relation of $\underline{MVL}$ coincides with that of $\mathcal{I}(L)$ which allows for the replacement of the traditional semantics of $\underline{MVL}$ with the categorical one of $\mathcal{I}(L)$.

10. Definition of fuzzy multi-algebras as a fuzzy extension of classical multi-algebras [34]; this allows for a fuzzy approach to algebraic non-determinism.

11. Theorem of a conservative embedding of the logic of fuzzy multi-algebras into $\mathcal{I}(L)$. As in the case of the embedding of $\underline{MVL}$, the main implication of this result is the possibility of the replacement of the semantics of fuzzy multi-algebras with the categorical semantics of $\mathcal{I}(L)$.

12. Proof that $\mathcal{I}(L)$ has model amalgamation. In general, this is one of the fundamental properties that assist the development of a model theory for an institution, in this case $\mathcal{I}(L)$.

13. Proof that $\mathcal{I}(L)$ admits the method of diagrams [11]. Overall, this is one of the fundamental properties that ensures the development of a model theory for an institution, in this case $\mathcal{I}(L)$.

14. The definition of a graded concept of deductive system extending Tarski and Scott's concept of classic deductive system from the binary to the many-valued case.

15. The generalization of the concept of institution to the many-valued case. Proof that this determines a Galois connection between syntax and semantics.

16. Interpretation of many-valued institutions as graded deductive systems, and proof that this construction corresponds to a retract. The inverse of this retract is a technical artefact that allows for semantic arguments in purely deductive situations.

17. Theorem of transfer of soundness from inference rules to graded proofs.

18. Definition of many-valued closure systems. Definition of two interpretations of graded deductive systems as many-valued closure systems, the first as many-valued interpretation of Modus Ponens and the second corresponding to a semantic closure. While in the binary case these two interpretation are identical, in the many-valued case we show that former is weaker than the latter.

19. Study of the logic of graded consequence by introducing e concepts of logical connectors and quantifiers at two distinct levels: the deductive level and the semantic level. Sufficient conditions in which their presence at the semantic level induce their presence at the deductive level.

20. Preservation theorem of the soundness property by logical connctors and by quantifiers.

21. Generalization of the concept of compactness from binary deductive systems to graded deductive systems. Proof that systems of finitary graded rules generate compact graded deductive systems and of the fact that compactness is preserved by logical connectors and quantifiers.

References

[1] Carlos Areces, Patrick Blackburn, and Samuel R. Delany. Bringing them all together. *Journal of Logic and Computation*, 11:657–669, 2001.

[2] Peter Baumgartner, Alexander Fuchs, Hans de Nivelle, and Cesare Tinelli. Computing finite models by reduction to function-free clause logic. *Journal of Applied Logic*, 7(1):58–74, 2007.

[3] Tomasz Borzyszkowski. Logical systems for structured specifications. *Theoretical Computer Science*, 286(2):197–245, 2002.

[4] Torben Braüner. *Hybrid Logic and its Proof-Theory*, volume 37 of *Applied Logic Series*. Springer, 2011.

[5] Ionuţ Ţuţu. Parameterisation for abstract structured specifications. *Theoretical Computer Science*. To appear.

[6] Ionuţ Ţuţu. Comorphisms for structured institutions. *Information Processing Letters*, 113(894–900), 2013.

[7] Ionuţ Ţuţu. Logical foundations of services. In A.V. Jones and N. Ng, editors, *2013 Imperial College Computing Student Workshop (ICCSW'13)*, volume 35 of *OpenAccess Series in Informatics Dagstuhl*, pages 111–118, 2013.

[8] Ionuţ Ţuţu and Jose Fiadeiro. A logic-programming semantics of services. In R. Heckel and S. Milius, editors, *CALCO 2013*, volume 8089 of *Lecture Notes in Computer Science*, pages 299–313, 2013.

[9] Răzvan Diaconescu. Graded consequence: an institution theoretic study. *Soft Computing*. Submitted.

[10] Răzvan Diaconescu. Extra theory morphisms for institutions: logical semantics for multi-paradigm languages. *Applied Categorical Structures*, 6(4):427–453, 1998. A preliminary version appeared as JAIST Technical Report IS-RR-97-0032F in 1997.

[11] Răzvan Diaconescu. *Institution-independent Model Theory*. Birkhäuser, 2008.

[12] Răzvan Diaconescu. An axiomatic approach to structuring specifications. *Theoretical Computer Science*, 433:20–42, 2012.

[13] Răzvan Diaconescu. Institutional semantics for many-valued logics. *Fuzzy Sets and Systems*, 218:32–52, 2013.

[14] Răzvan Diaconescu. Quasi-varieties and initial semantics in hybridized institutions. *Journal of Logic and Computation*, DOI:10.1093/logcom/ext016.

[15] Răzvan Diaconescu and Ionuţ Ţuţu. Foundations for structuring behavioural specifications. *Journal of Logic and Algebraic Programming*. Submitted.

[16] Răzvan Diaconescu and Ionuţ Ţuţu. On the algebra of structured specifications. *Theoretical Computer Science*, 412(28):3145–3174, 2011.

[17] Răzvan Diaconescu and Kokichi Futatsugi. *CafeOBJ Report: The Language, Proof Techniques, and Methodologies for Object-Oriented Algebraic Specification*, volume 6 of *AMAST Series in Computing*. World Scientific, 1998.

[18] Răzvan Diaconescu, Joseph Goguen, and Petros Stefaneas. Logical support for modularisation. In Gerard Huet and Gordon Plotkin, editors, *Logical Environments*, pages 83–130. Cambridge, 1993. Proceedings of a Workshop held in Edinburgh, Scotland, May 1991.

[19] Răzvan Diaconescu and Alexandre Madeira. Encoding hybridized institutions into first order logic. *Mathematical Structures in Computer Science.*

[20] Răzvan Diaconescu, Till Mossakowski, and Andrzej Tarlecki. The institution theoretic scope of logic theorems. *Logica Universalis.* Submitted.

[21] Răzvan Diaconescu and Petros Stefaneas. Ultraproducts and possible worlds semantics in institutions. *Theoretical Computer Science*, 379(1):210–230, 2007.

[22] José L. Fiadeiro and Antónia Lopes. An interface theory for service-oriented design. In Dimitra Giannakopoulou and Fernando Orejas, editors, *Fundamental Approaches to Software Engineering*, Lecture Notes in Computer Science, pages 18–33. Springer, 2011.

[23] José L. Fiadeiro, Antónia Lopes, and Laura Bocchi. An abstract model of service discovery and binding. *Formal Aspects of Computing*, 23(4):433–463, 2011.

[24] Joseph Goguen and Rod Burstall. Institutions: Abstract model theory for specification and programming. *Journal of the Association for Computing Machinery*, 39(1):95–146, 1992.

[25] Petr Hájek. *Metamathematics of Fuzzy Logic.* Kluwer, 1998.

[26] H.-J. Kreowski and Till Mossakowski. Equivalence and difference between institutions: simulating Horn Clause Logic with based algebras. *Mathematical Structures in Computer Science*, 5:189–215, 1995.

[27] John Lloyd. *Foundations of Logic Programming.* Springer, 1984.

[28] Manuel-Antonio Martins, Alexandre Madeira, Răzvan Diaconescu, and Luis Barbosa. Hybridization of institutions. In Andrea Corradini, Bartek Klin, and Corina Cîrstea, editors, *Algebra and Coalgebra in Computer Science*, volume 6859 of *Lecture Notes in Computer Science*, pages 283–297. Springer, 2011.

[29] José Meseguer. General logics. In H.-D. Ebbinghaus et al., editors, *Proceedings, Logic Colloquium, 1987*, pages 275–329. North-Holland, 1989.

[30] Till Mossakowski. HetCasl – heterogeneous specification. Language summary. Technical report, CoFI: The Common Framework Initiative, 2004.

[31] Donald Sannella and Andrzej Tarlecki. Specifications in an arbitrary institution. *Information and Control*, 76:165–210, 1988.

[32] Donald Sannella and Andrzej Tarlecki. *Foundations of Algebraic Specifications and Formal Software Development.* Springer, 2012.

[33] Andrzej Tarlecki. Moving between logical systems. In Magne Haveraaen, Olaf Owe, and Ole-Johan Dahl, editors, *Recent Trends in Data Type Specification*, volume 1130 of *Lecture Notes in Computer Science*, pages 478–502. Springer, 1996.

[34] Michał Walicki and Sigurd Meldal. Algebraic approaches to nondeterminism - an overview. *ACM Computing Surveys*, 29, 1997.

[35] Christoph Weidenbach, Uwe Brahm, Thomas Hillenbrand, Enno Keen, Christian Theobald, and Dalibor Topic. Spass version 2.0. In *Proceedings of the 18th International Conference on Automated Deduction*, CADE-18, pages 275–279, London, UK, 2002. Springer-Verlag.