Names and Symmetry in Computer Science

(Invited Tutorial)

Andrew M. Pitts
Computer Laboratory
University of Cambridge
Cambridge, UK
andrew.pitts@cl.cam.ac.uk

***Abstract*—Nominal sets provide a mathematical theory for some of the key concepts that arise when representing and computing with data involving atomic (or 'pure') names: freshness, abstraction and scoping of names, and finiteness modulo symmetry. This tutorial introduces the notion of nominal set and explains selected applications of it to logic in computer science, to automata, languages and programming.**

> "A pure name is nothing but a bit-pattern that is an identifier, and is only useful for comparing for identity with other such bit-patterns – which includes looking up in tables to find other information. The intended contrast is with names which yield information by examination of the names themselves, whether by reading the text of the name or otherwise. [. . .] like most good things in computer science, pure names help by putting in an extra stage of indirection; but they are not much good for anything else."
>
> Roger Needham [9, p. 90]

Such pure names are used in many different ways in formal languages and logics for describing and constructing computer systems. The complexity of computer systems has stimulated the development of compositional methods for specifying and reasoning about them. If one wishes to compose a whole out of parts, then one had better have mechanisms for hiding, or at least controlling access to, the identity of the names upon which each part depends. The prerequisite for devising such mechanisms and understanding their properties is a firm grasp of what it means for a piece of the system to *depend* upon a name. Although there are syntactic considerations, such as various notions of textual occurrence, this issue really concerns semantics: *what does it mean for the behaviour of a software system to depend upon the identity of some names*?

The theory of nominal sets, introduced in this context by Jamie Gabbay and myself [6], answers this question via a mathematical theory of structures involving names which involves some simple, but subtle ideas to do with symmetry whose origin lies in the permutation models of set theory with atoms (ZFA) of Fraenkel [4] and Mostowski [8]. The theory has been applied to the syntax and semantics of programming language constructs that involve binding and localising the scope of names [1], [10]; to logics that underly systems for machine-assisted reasoning about programming language semantics [13]; and to the automatic verification of process specifications in nominal calculi for concurrency [7]. Generalized forms of nominal sets are being applied to automata theory over infinite alphabets [3]. They also feature in recent work on the cubical sets model of Homotopy Type Theory and univalent foundations [2], [12].

This tutorial introduces the notions which are fundamental to the theory of nominal sets, that of a mathematical structure being *finitely supported* with respect to an action of name permutations and the complementary relation of *freshness* of names. For further reading I immodestly suggest the text book [11], which emphasises category theory over set theory, or the survey by Gabbay [5], which does the opposite.

References

[1] J. Bengtson, M. Johansson, J. Parrow, and B. Victor, "Psi-calculi: Mobile processes, nominal data, and logic," in *Twenty-Fourth Annual IEEE Symposium on Logic in Computer Science (LICS 2009), Los Angeles, USA*. IEEE Computer Society Press, Aug. 2009, pp. 39–48.

[2] M. Bezem, T. Coquand, and S. Huber, "A model of type theory in cubical sets," in *19th International Conference on Types for Proofs and Programs (TYPES 2013)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), R. Matthes and A. Schubert, Eds., vol. 26. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2014, pp. 107–128.

[3] M. Bojańczyk, B. Klin, and S. Lasota, "Automata theory in nominal sets," *Logical Methods in Computer Science*, vol. 10, no. 3, p. paper 4, Aug. 2014.

[4] A. A. Fraenkel, "Der begriff 'definit' und die unabhängigkeit des auswahlsaxioms," *Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-mathematische Klasse*, pp. 253–257, 1922.

[5] M. J. Gabbay, "Foundations of nominal techniques: Logic and semantics of variables in abstract syntax," *Bulletin of Symbolic Logic*, vol. 17, no. 2, pp. 161–229, 2011.

[6] M. J. Gabbay and A. M. Pitts, "A new approach to abstract syntax with variable binding," *Formal Aspects of Computing*, vol. 13, pp. 341–363, 2002.

1043-6871/15 $31.00 © 2015 IEEE
DOI 10.1109/LICS.2015.12

[7] U. Montanari and M. Pistore, "π-Calculus, structured coalgebras and minimal HD-automata," in *25th International Symposium on Mathematical Foundations of Computer Science, Bratislava, Slovak Republic,*, ser. Lecture Notes in Computer Science, vol. 1893. Springer-Verlag, 2000, pp. 569–578.

[8] A. Mostowski, "Uber die unabhängigkeit des wohlordnungssatzes vom ordnungsprinzip," *Fundamenta Mathematicae*, pp. 201–252, 1939.

[9] R. M. Needham, "Names," in *Distributed Systems*, S. Mullender, Ed. ACM Press, 1989, pp. 89–101.

[10] A. M. Pitts, "Alpha-structural recursion and induction," *Journal of the ACM*, vol. 53, pp. 459–506, 2006.

[11] ——, *Nominal Sets: Names and Symmetry in Computer Science*, ser. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 2013, vol. 57.

[12] ——, "Nominal presentations of the cubical sets model of type theory," in *20th International Conference on Types for Proofs and Programs (TYPES 2014)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), H. Herbelin, P. Letouzey, and M. Sozeau, Eds. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015, pp. ?–?, to appear.

[13] C. Urban, "Nominal reasoning techniques in Isabelle/HOL," *Journal of Automatic Reasoning*, vol. 40, no. 4, pp. 327–356, 2008.