Towards Randomized Bounded Arithmetic

Melissa Antonelli[1] , Ugo Dal Lago[1] , Davide Davoli[1] , Isabel Oitavem[4] , and Paolo Pistone[1]

[1] University of Bologna & Inria
{melissa.antonelli2,ugo.dallago,davide.davoli5,paolo.pistone2}@unibo.it

[2] NOVA University of Lisbon
oitavem@fct.unl.pt

Background. The development of (deterministic) computational models has considerably benefitted from the discovery of interactions between logic and theoretical computer science. For example, quantified Boolean logic was shown to provide a characterization of the full polynomial hierarchy [9, 10], while the correspondence between simply-typed λ-calculi and logical proof systems was revealed by the so-called Curry-Howard correspondence [12]. Surprisingly, probabilistic computation – which is nowadays pervasive in almost every area of computer science and technology – has not been touched in the same way by such fruitful interchanges.

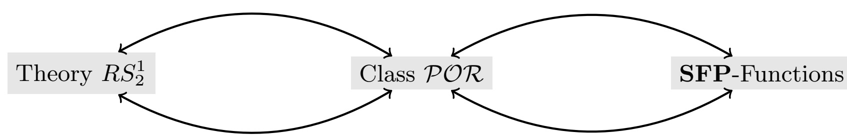
Recently, first achievements in this direction have been presented by some of the authors. In particular, in [3, 2, 1], inherently quantitative logics are introduced and their relations with specific aspects of probabilistic computation are investigated. Intuitively, the fundamental ingredient of this approach consists in extending standard logical systems with a new class of measure-quantified expressions in the form $\mathbf{C}^q A$ (and $\mathbf{D}^q A$), basically expressing that the argument formula A is true in a portion of its possible interpretations having at least (or at most) measure $q \in \mathbb{Q}_{[0,1]}$. Specifically, in [3], it is defined a first-order language, extending that of standard Peano Arithmetic (**PA**, for short) via so-called measure-quantifiers, and the formulas of which are interpreted as measurable sets. Starting from these ideas, our goal is to define a novel *randomized bounded theory*, to provide a logical characterization of some *probabilistic* complexity classes.

Characterizing Probabilistic Classes. One of the original motivations for the development of bounded arithmetics was their connection with computational complexity [4]. Informally, a first-order theory of arithmetic T is said to define a numerical function f when there is a formula F such that: (i) $T \vdash (\forall x)(\exists y!)F(x, y)$, and (ii) for every x, $F\big(x, f(x)\big)$. In particular, condition (ii) implies the existence of a proof in T providing an algorithm to compute f. Of course, not all computable functions are effectively computable, and concretely it is often desirable to restrict analysis to feasibly computable functions, that is to polynomial-time computable ones. To do so, Buss introduced some formal theories, called *bounded arithmetics*, which are fragments of **PA** including function symbols with specific growth-rate and new, *bounded* quantifiers. These allow Buss to characterize complexity classes in terms of families of arithmetical formulas. Specifically, he proved that the set of polynomial-time computable function is logically characterized by formulas which are Σ^b_1-definable in the corresponding bounded theory S^1_2.

This fact is very insightful but, again, no similar result exists when switching to the probabilistic framework. So, the following (open) question naturally arises: Is it possible to obtain an analogous characterizations for *probabilistic* classes? The contribution of our work consists precisely in giving a positive answer to this query. In particular, our core idea is that of generalizing the standard conditions for definability of functions in a theory to the quantitative setting using a language inspired by the one presented in [3]. Concretely, the first step in our argument consists in relating bounded formulas with some effective model for *probabilistic* computation. To this aim, we introduce three new classes of functions and prove them equivalent:

1. The *class of polynomial-time oracle recursive functions*, called $\mathcal{POR}$, that is a class of functions from (finite and infinite) strings to strings defined by extending Ferreira's class of polynomial-time functions [6] (which is basically the word version of the corresponding class by Cobham [5]) with a *query function* accessing an oracle from the Cantor space [3].
2. The *class of functions which are* Σ_1^b*-representable in* RS_2^1, where RS_2^1 is our *randomized bounded theory*. This theory is expressed in a new "probabilistic word language", i.e. a first-order word language with equality by [7], augmented by the "probabilistic" predicate $\mathsf{FLIP}(\cdot)$, providing an i.i.d. sequence of bits [3].
3. The *class of* **SFP**-*functions*, that is the class of functions computable by polynomial-time *stream machines*, i.e. Turing machines with $k+1$-tape, one of which is treated as a read-only oracle tape. These machines differ from standard probabilistic Turing machines [11, 8], as their access to randomness is close to that of $\mathcal{POR}$'s query functions.

Our main result consists in proving that the class of functions which are Σ_1^b-representable in RS_2^1 is precisely the class of polynomial-time computable ones which, in turn, coincides with the class of **SFP**-functions. Then, starting from this equivalence, it becomes possible to characterize probabilistic classes by means of formulas of the bounded theory RS_2^1 together with counting quantifiers, defined as in [3]. For instance, functions corresponding to problems in $\mathbb{BPP}$, could be logically characterized by replacing usual condition (ii) with one concerning a counting-quantified formula, e.g. $\mathbf{C}^{2/3}F(x, f(x))$.



References

[1] Antonelli, M., Dal Lago, U. and Pistone, P. Curry and Howard Meet Borel, In *LICS '22*.

[2] Antonelli, M., Dal Lago, U. and Pistone, P. On Counting Propositional Logic and Wagner's Hierarchy. In *ICTCS*, 3072, pp. 107–121, 2021.

[3] Antonelli, M., Dal Lago, U. and Pistone, P. On Measure Quantifiers in First-Order Arithmetic. in *Connecting with Computability*, pp. 12–24, Springer, 2021.

[4] Buss, S.R. *Bounded Arithmetic*. Bibliopolis, 1986.

[5] Cobham, A. The Intrinsic Computational Difficulty of Functions. in *Logic, Methodology and Philosophy of Science II*, pp. 24–30. North-Holland, 1964.

[6] Ferreira, F. Polynomial-Time Computable Arithmetic and Conservative Extensions, Ph.D. Dissertation, 1988.

[7] Ferreira, G. and Oitavem, I. An interpretation of S_2^1 in Σ_1^b-NIA. *Portugaliae Mathematica*, 63:427–450, 2006.

[8] Gill, J. Computational Complexity of Probabilistic Turing Machines. *J. Comp.* 6(4):675–695, 1977.

[9] Meyer, A.R. and Stockmeyer, L.J., The Equivalence Problem for Regular Expressions with Squaring Requires Exponential Space. In *SWAT*, pp. 125–129, 1972.

[10] Meyer, A.R. and Stockmeyer, L.J., Word Problems Requiring Exponential Time (Preliminary Report). In *STOC*, pp. 1–9, 1973.

[11] Santos, E.S. Probabilistic Turing Machines and Computability, *AMS*, 22(3):704–710, 1969.

[12] Sørensen, M.H. and Urzyczyn, L.J., *Lectures on the Curry-Howard Isomorphism*, Elsavier, 2006.