Quantifiers for Quantitative Logics in Coq: a New Project Description

Jairo Miguel Marulanda-Giraldo[1], Ekaterina Komendantskaya[1,2], Alessandro Bruni[3], Reynald Affeldt[4], and Matteo Capucci[5]

[1] Southampton University, UK
[2] Heriot-Watt University, UK
[3] IT-University of Copenhagen, Denmark
[4] National Institute of Advanced Industrial Science and Technology (AIST), Japan
[5] Independent Researcher, Italy**

Abstract. The development of propositional logics for quantitative metric reasoning is a well established area of research. However, it remains uncertain how to develop semantics for first-order logics that maintain strong guarantees. A promising approach is to interpret quantifiers as expected values on Lp-spaces. In this on-going project, we explore how to formalize semantics for first-order quantitative logics using the Mathematical Components library in the Coq proof assistant. With this formalization, we seek to give strong semantics for quantifiers, verify their behavior with respect to other logical connectives, as well as prove the soundness and completeness of the resulting logics.

Keywords: Programming Languages · Machine Learning · Loss Functions · Differentiable Logics · Interactive Theorem Proving.

1 Motivation

Quantitative logics, i.e. logics that have semantic interpretations into interval domains instead of the Boolean $\{0, 1\}$ have been studied for decades, and date back to the ideas of Kleene, Gödel and Lukasievicz at the start of the 20th century [15]. Fuzzy logics [15], and the logics of Lawvere quantale [15, 4, 10] are important examples of quantitative logics. To illustrate, let us have a toy syntax with atomic propositions and conjunction, such that

$$\Phi \ni \phi := A \,|\, \phi \wedge \phi \tag{1}$$

Where A is interpreted in a domain $D \in \mathbb{R} \cup \{-\infty, \infty\}$. D varies among logics and restricts the interpretation of connectives. For example, the Gödel logic has an interpretation on $[0, 1]$ with conjunctions interpreted as *min*.

Recently, there was a surge of interest in quantitative logics, stimulated by the growing interest in *safer machine learning* [8]. Generally, it is considered

** Funded by the Advanced Research + Invention Agency (ARIA)

to be desirable to be able to use machine learning algorithms in a way that imposes certain logical specifications during training [14, 18]. Quantitative logics have been shown to effectively translate arbitrary logical specifications into real-valued functions. Such functions in turn can be used as *loss functions* in standard gradient-descent algorithms. It has been shown that such specification-driven loss functions help to improve the adherence of the resulting neural networks to specifications [11].

Nevertheless, there is one fundamental problem that quantitative logics face in this domain. Many specifications of interest for machine learning are first-order, yet the majority of quantitative logic results concern propositional syntax [16, 15, 4]. Generalising some sound and complete propositional fuzzy logics to first-order logic often comes at a cost of either completeness or function continuity. For example, among several known fuzzy logics [16, 15], the only first-order extension that is sound and complete involves the Gödel logic, that interprets conjunction as a *min*, disjunction as a *max*, and universal and existential quantifiers via an infimum and supremum [3]. However, connectives of this logic are not continuous and therefore not suitable for gradient-descent algorithms.

Recently, a promising solution was proposed by Capucci, interpreting quantifiers as *p-means* [6], a generalization of p-norms over a probability space [5]. This new semantics gives hope that the open problem of finding a suitable approach to quantification in quantitative logics will soon find its resolution, and we can soon find a logic that is sound and complete relative to this new quantitative semantics.

It has been shown that verifying soundness and continuity of quantitative logics results in laborious proofs that are prone error [7, 16, 1]. To overcome these challenges, rigorous computer formalizations of propositional semantics for quantitative logics have been proposed [1]. Extending these formalizations to first-order logics is a non trivial challenge that is yet to be overcome. In particular, the new semantics proposed by Capucci presents a particular challenge for formal verification, since, unlike the previous formalizations of quantitative logics [1], it now also involves results from real analysis and probability. Most notably, it involves formalisation of measure spaces, probability spaces, Lebsegue integrals, as well as the use of results such as Jensen's and Hölder's inequalities [13].

Coq's Mathematical Components library (*MathComp*) [17], is a particularly good fit for this task, due to its extensive mathematical libraries. Many of the above mentioned standard, but by no means trivial, results from the measure theory are formalized in the librarie's modules on algebra and analysis. Yet some, like the encoding of extended real numbers, still require further development.

In this extended abstract, we introduce the mathematical definitions underlying the novel approach to quantification proposed by Capucci in [6], explain its relation to the available mathematical libraries in Coq, and report on our current work on formalizing the novel semantics. With this formalization, we will contribute towards developing the semantics for quantifiers in quantitative logics. Tangentially, we will extend *MathComp*as necessary. In the long term, this formalization is expected to become part of a larger collaborative project [2], that develops the novel first-order quantitative logic, and provides its full formalization in Coq, including the formalisation of the soundness and completeness results for the logic.

2 Preliminaries

Here we introduce some useful concepts from measure theory. After some basic definitions, we introduce the geometric mean, as well as the essential supremum and infimum. We then use these definitions to define the p-mean, and lastly introduce the dual operator [6], which will be present in the logical semantics.

The following definitions of measurable functions, measure and probability spaces, as well as Lebesgue integral are standard [9] and already form part of the analysis module of *MathComp*[17].

Definition 1 (Measurable Space. Measurable Function). *Let S_1, S_2 be sets and $\mathfrak{S}_1, \mathfrak{S}_2$ be σ-algebras. The pairs $(S_1, \mathfrak{S}_1)$ and $(S_2, \mathfrak{S}_2)$ are* ***measurable spaces****.*
$f : S_1 \to S_2$ is a ***measurable function*** *if and only if for every $E \in \mathfrak{S}_2$ the pre-image of E under f is in $\mathfrak{S}_1$. That is, for all $E \in \mathfrak{S}_2$*

$$f^{-1}(E) = \{x \in S_1 \mid f(x) \in E\} \in \mathfrak{S}_1 \tag{2}$$

Definition 2 (Measure. Measure Space). *Let S be a set and $\mathfrak{S}$ be a σ-algebra over S. A* ***measure*** *on $(S, \mathfrak{S})$ is a function $\mu : \mathfrak{S} \to [0, \infty]$ that satisfies*

1. *$\mu(\emptyset) = 0$*
2. *if $\{A_i : i \in I\}$ is a countable, pairwise disjoint collection of sets in $\mathfrak{S}$ then*

$$\mu\left(\bigcup_{i \in I} A_i\right) = \sum_{i \in I} \mu(A_i) \tag{3}$$

The triple $(S, \mathfrak{S}, \mu)$ is a ***measure space****.*

Definition 3 (Probability Space. Random Variable). *Let $(S, \mathfrak{S}, \mathbb{P})$ be a measure space. If $\mathbb{P}(S) = 1$, then $(S, \mathfrak{S}, \mathbb{P})$ is a* ***probability space****. A* ***random variable*** *with values in T is a measurable function $X : S \to T$.*

Definition 4 (Simple Function. Lebesgue Integral). *Let $(S, \mathfrak{S})$ be a measurable space, I a finite index set, $a_i \in \mathbb{R}$ for each $i \in I$ and $\{A_i : i \in I\}$ a collection of sets in $\mathfrak{S}$ that partition S. Then $f = \sum_{i \in I} a_i \mathbf{1}_{A_i}$ is a* ***simple function****.*
If μ is a measure of $(S, \mathfrak{S})$ then:

1. *If $f = \sum_{i \in I} a_i \mathbf{1}_{A_i}$ is a nonnegative simple function. The* ***Lebesgue integral*** *of f is*

$$\int_S f \, d\mu = \sum_{i \in I} a_i \mu(A_i) \tag{4}$$

2. *If $f : S \to [0, \infty]$ is a measurable function. The **Lebesgue integral** of f is*

$$\int_S f\, d\mu = sup \left\{ \int_S g\, d\mu : g \text{ is simple and } 0 \leq g \leq f \right\} \tag{5}$$

3. *If $f : S \to \mathbb{R} \cup \{-\infty, \infty\}$ is a measurable function.*
   *The **Lebesgue integral** of f is*

$$\int_S f\, d\mu = \int_S max(f, 0)\, d\mu - \int_S max(-f, 0)\, d\mu \tag{6}$$

   Assuming at least one of the integrals on the right is finite.

The following definitions relate specifically to the new quantifier semantics and already form a part of our new Coq development.

Definition 5 (Geometric Mean). *Let $f : S \to \mathbb{R} \cup \{-\infty, \infty\}$ be a measurable function and $(S, \mathfrak{S}, \mu)$ a measure space. The **geometric mean** of f is*

$$GM[f] = exp\left(\frac{1}{\mu(S)} \int_S ln\, |f| d\mu \right) \tag{7}$$

Definition 6 (Essential Supremum. Essential Infimum). *Let $(S, \mathfrak{S}, \mu)$ be a measure space, $A \in \mathfrak{S}$ and $f : S \to \mathbb{R} \cup \{-\infty, \infty\}$ a measurable function.*

1. *Let $U = \{a \in \mathbb{R} \cup \{-\infty, \infty\} : \mu(\{x \in X : a < f(x)\}) = 0\}$ and $inf(U)$ be the infimum of U. The **essential supremum** of f is*

$$ess\, sup\, (f) = \text{ if } U \neq \emptyset \text{ then } inf(U) \text{ else } \infty \tag{8}$$

2. *The **essential infimum** of f is*

$$ess\, inf\, (f) = -\, ess\, sup\, (-f) \tag{9}$$

Definition 7 (P-mean). *Let p be a real number, $(S, \mathfrak{S}, \mathbb{P})$ a probability space and $f : S \to \mathbb{R} \cup \{-\infty, \infty\}$ be a measurable function. The **p -mean** of f is*

$$\langle f \rangle_{S,p} = \begin{cases} GM[f] & p = 0 \\ \left(\int_S |f|^p d\mathbb{P} \right)^{1/p} & -\infty < p < \infty, p \neq 0 \\ ess\, sup\, (|f|) & p = \infty \\ ess\, inf\, (|f|) & p = -\infty \end{cases}$$

When S can be inferred from the context, we write $\langle f \rangle_p$.

Definition 8 (Dual Operator). *Let $a \in [0, \infty]$. Then the **duality** of a is*

$$a^* = \begin{cases} 1/a & a \in (0, \infty) \\ \infty & a = 0 \\ 0 & a = \infty \end{cases}$$

3 Proposed Semantics

We will introduce the main ideas for first-order quantitative logics through a toy example, following closely [6]. We begin by defining a small formal language. Let every probability space $(S, \mathfrak{S}, \mathbb{P})$, simply denoted as S, be a context of the language $\Phi(S)$. Let $s, s' \in S$ be either variables or constants, and $A(s) \in \mathcal{A}$ be an atomic proposition. Let us have negation and disjunction, as well as universal and existential quantifiers.

$$\begin{aligned} \Phi(S) \ni \phi(s) :=& \\ & A(s) \mid \neg\phi(s) \\ & \mid \phi(s) \vee \phi(s) \\ & \mid \forall^p (j \in J).\psi(s, j) \\ & \mid \exists^p (j \in J).\psi(s, j) \end{aligned} \tag{10}$$

Where $p \in [0, \infty]$ and $\psi \in \Phi(S \times J)$, for J another context.

We also derive implication as $\phi_1(s) \to \phi_1(s) := \neg\phi_1(s) \vee \phi_2(s)$. Assuming an oracle translates $A(s)$ into a value in $[0, \infty]$, the translation function $[\![\cdot]\!] : \Phi \to [0, \infty]$ is defined as follows:

$$\begin{aligned} & [\![\neg\phi(s)]\!] := [\![\phi(s)]\!]^* \\ & [\![\phi_1(s) \vee \phi_2(s)]\!] := [\![\phi(s)]\!][\![\phi(s)]\!] \\ & [\![\forall^p (j \in J).\psi(s, j)]\!] := \langle \lambda j.[\![\psi(s, j)]\!] \rangle_{J, -p} \\ & [\![\exists^p (j \in J).\psi(s, j)]\!] := \langle \lambda j.[\![\psi(s, j)]\!] \rangle_{J, p} \end{aligned} \tag{11}$$

This gives us a family of quantifiers parametrized by p. Note we can view the previous translations as random variables. That is, for any $\phi(s) \in \Phi(S)$ there exists a measurable function $f : S \to [0, \infty]$ such that

$$[\![\phi]\!] := \lambda s.[\![\phi(s)]\!] = f \tag{12}$$

As an example of the utility of these semantics, we can use them to construct the *softmax operator*, used in machine learning to turn a vector of real numbers into a probability distribution [12]. Let $f : S \to [0, \infty]$ be a measurable function such that $[\![\phi]\!] = f$ for some $\phi(s) \in \Phi(S)$. Then the softmax of f is the function

$$softmax(f)(x) := \frac{f(x)}{\int_S f d\mathbb{P}} = [\![\forall^1 (s \in S).(\phi(s) \to \phi(x))]\!] \tag{13}$$

4 Work in progress on the Coq formalization

In "Taming Differentiable Logics with Coq Formalisation" a formalization for several quantitative logics was developed [1]. We seek to expand this formalization so it is suitable for reasoning about first-order quantitative logics, with p-means as the semantics for quantifiers. So far, p-means have been encoded as follows:

```
Definition geo_mean P f :=
    expeR (\int[P]_x lne (f x)).

Definition ess_supe f :=
    ereal_inf ([set r | mu ([set x | r < f x]) = 0]).

Definition ess_infe f := - ess_supe (\- f).

Definition Pmean P p f :=
  match p with
  | p%:E =>
        if p == 0 then geo_mean P f
        else (\int[P]_x `|f x| `^ p) `^ p^-1
  | +oo => ess_supe P (abse \o f)
  | -oo => ess_infe P (abse \o f)
  end.
```

Which corresponds to definition 7. Here the encodings of the geometric mean and the essential infimum are novel, while the encodings of the p-mean and the essential supremum are extensions of previous implementations able to take functions that go to extended reals.

In the machine learning community there is a general consensus on the desirable properties of loss functions - convexity or continuity are widely considered desirable [14]. From a logic perspective, there is no consensus as to how to define soundness for quantitative logics. In the future, we intend to follow the general approach applied by Ślusarz et al. That is, for a typed FOL, take provable FOL formulae to characterize the set of true FOL formulae [16]. Moreover, Varnai and Dimarogonas suggest characterizing quantitative logics in terms of their *geometric properties*, valuable for optimization tasks [18]. As for quantifiers, Currently we are working to formalize and prove the following properties in Coq, which were presented by Capucci [6].

Lemma 1 (Properties of Quantifiers). *Let $(S, \mathfrak{S}, \mathbb{P})$ be a probability space, $p \in \mathbb{R} \cup \{-\infty, \infty\}$ and $f : S \to \mathbb{R} \cup \{-\infty, \infty\}$ a measurable function. Then*

1. $\langle f \rangle_1$ *equals the expected value of* f.
2. $\langle f \rangle_{-p} = \langle f^* \rangle_p^*$

   This implies $[\![\forall^p (j \in J).\psi(s,j)]\!] = [\![\neg\exists^p (j \in J).\neg\psi(s,j)]\!]$.
3. *Let* $a \in [0, \infty]$, *then* $\langle af^* \rangle_{-p} = a(\langle f \rangle_p)^*$

   This implies $[\![\forall^p (j \in J).(\psi(s,j) \to \phi(s))]\!] = [\![(\exists^p (j \in J).\psi(s,j)) \to \phi(s)]\!]$.

4. *Let* $a \in [0, \infty]$*, then* $a\langle f \rangle_p = \langle af \rangle_p$

   This implies $[\![\phi(s) \to \forall^p (j \in J).\psi(s, j)]\!] = [\![(\forall^p (j \in J).(\phi(s) \to \psi(s, j))]\!]$.

5. *Let* $g : S \to \mathbb{R} \cup \{-\infty, \infty\}$ *be a measurable function such that* $g \leq f$*, then* $\langle g \rangle_p \leq \langle f \rangle_p$.

6. *Let* $A \subseteq S$ *then* $\langle f|_A \rangle_{A,p} \leq \langle f|_S \rangle_{S,p}$*. Where* $f|_A$ *is* f *bounded to* A.

7. $\langle f \rangle_p$ *is continuous in* p.

8. *If* $0 \neq f$ *or* $p \neq 0$ *, then* $\langle f \rangle_p$ *is monotonic increasing in* p.

9. $\lim_{p \to \infty} \langle f \rangle_p = \langle f \rangle_\infty$

10. $\lim_{p \to -\infty} \langle f \rangle_p = \langle f \rangle_{-\infty}$

Note, item 8 , item 9 and item 10 together imply that quantifiers are bounded by the essential infimum and supremum of the input function. This gives the interpretation a certain independence from the size of the domain.

In order to prove these properties in Coq, we are currently working on extending the analysis module of *MathComp*. In particular, Hölder's inequalities must be generalized to functions that go to the extended reals. In this process, a bug in the encoding of the power function was found and is being corrected.

5 Conclusions

In this extended abstract we described our work in progress. We presented the main ideas behind quantitative logics and explained their use in machine learning. We presented a promising translation for bounded quantifiers and introduced some desirable properties for this translation, following closely [6]. We argued for the usefulness of a computer formalization to tackle this challenge. Lastly, we presented some preliminary progress in formalization of these results in Coq. The main author is a first year PhD student.

References

[1] Reynald Affeldt et al. "Taming Differentiable Logics with Coq Formalisation". In: *arXiv preprint arXiv:2403.13700* (2024).

[2] Robert Atkey et al. "Quantitative Predicate Logic as a Foundation for Verified ML". In: *ARIA grant* (2024).

[3] Matthias Baaz, Norbert Preining, and Richard Zach. "First-order Gödel logics". In: *Annals of Pure and Applied Logic* 147.1-2 (2007), pp. 23–47.

[4] Giorgio Bacci et al. "Propositional logics for the Lawvere quantale". In: *Electronic Notes in Theoretical Informatics and Computer Science* 3 (2023).

[5] Jean Bourgain. *New classes of Lp-spaces*. Vol. 889. Springer, 2006.

[6] Matteo Capucci. “On Quantifiers for Quantitative Reasoning”. In: *arXiv preprint arXiv:2406.04936* (2024).

[7] Marco Casadio et al. “Neural network robustness as a verification property: a principled case study”. In: *International conference on computer aided verification*. Springer. 2022, pp. 219–231.

[8] David Dalrymple. *Safeguarded AI: constructing guaranteed safety*. Programme Thesis. 2024.

[9] Richard M Dudley. *Real analysis and probability*. Chapman and Hall/CRC, 2018.

[10] Marc Fischer et al. “DL2: training and querying neural networks with logic”. In: *International Conference on Machine Learning*. PMLR. 2019, pp. 1931–1941.

[11] Thomas Flinkow, Barak A Pearlmutter, and Rosemary Monahan. “Comparing Differentiable Logics for Learning with Logical Constraints”. In: *arXiv preprint arXiv:2407.03847* (2024).

[12] Michael Franke and Judith Degen. “The softmax function: Properties, motivation, and interpretation”. In: (2023).

[13] Nicholas D Kazarinoff. *Analytic inequalities*. Courier Corporation, 2014.

[14] Lev Borisovich Klebanov, Svetlozar Todorov Rachev, and Frank J Fabozzi. *Robust and non-robust models in statistics*. Nova Science Publishers Hauppauge, 2009.

[15] George Metcalfe, Nicola Olivetti, and Dov M Gabbay. *Proof theory for fuzzy logics*. Vol. 36. Springer Science & Business Media, 2008.

[16] Natalia Ślusarz et al. “Logic of differentiable logics: Towards a uniform semantics of DL”. In: *arXiv preprint arXiv:2303.10650* (2023).

[17] Mathematical Components Team. *Mathematical components library*. https://github.com/math-comp/math-comp. 2007.

[18] Peter Varnai and Dimos V Dimarogonas. “On robustness metrics for learning STL tasks”. In: *2020 American Control Conference (ACC)*. IEEE. 2020, pp. 5394–5399.