Divergences on Monads and Relational Liftings

Tetsuya Sato\textsuperscript{1} and Shin-ya Katsumata\textsuperscript{2}

\textsuperscript{1} Seike University
\textsuperscript{2} National Institute of Informatics

\textbf{Introduction.} Comparing the behavior of two runs of programs is one of the fundamental activities in the development of systems. One recent successful framework of this kind is a probabilistic variant of Benton’s relational Hoare logic, called \textit{apRHL}. This is introduced by Barthe et al. to formally verify differential privacy of randomized mechanisms (i.e., probabilistic programs) based on statistical divergences. The soundness of apRHL hinges on two key technical concepts: \textit{composable} statistical divergences and \textit{graded relational liftings} of monads recovered the divergences.

In this work we generalize apRHL to support comparisons of various computational effects based on divergences. This generalization demands us to redevelop the key technical concepts of apRHL. For this, we introduce a general notion of \textit{divergences on monads}, and construct graded relational liftings recovering divergences on monads using the codesinty lifting technique.

We consider the following categorical setting: (1) \((\mathcal{C}, 1, \times)\) is a well-pointed cartesian category. (2) \((T, \eta, (-)^f, \theta)\) is a strong monad on \(\mathcal{C}\). (3) \(U : (\mathcal{C}, 1, \times) \to (\text{Set}, 1, \times)\) is a functor strictly preserving finite products. (4) \((-) : U \to \mathcal{C}(1, -)\) is a natural isomorphism (thus, \(U\) is faithful). A notational convention: for \(f : I \to J\) and \(x \in UI\), by \(f \bullet x\) we mean \(Uf(x) \in UJ\). \textbf{Meas} is the category of all measurable spaces and measurable functions. \(G\) and \(G_s\) are the Giry monad and its subprobabilistic variants.

\textbf{Divergences on Monads.} We introduce the notion of \textit{divergences on monads}, which captures various kinds of quantitative difference between two computational effects. Let \((Q, \leq, 0, +)\) and \((M, \leq, 1, \cdot)\) be partially ordered monoids. Assume that \((Q, \leq)\) is a complete lattice.

An \(M\)-\textit{graded} \(Q\)-\textit{divergence} on \(T\) is a family \(\{\Delta^p_I : UTI \times UTI \to Q\}_{m \in M, I \in \mathcal{C}}\) of functions satisfying the monotonicity condition on \(M: m \leq n \Rightarrow \forall I \in \mathcal{C}. \forall c, c' \in UTI, \Delta^p_I(c, c') \leq \Delta^p_I(c, c').\) We say that \(\Delta\) is:

\textbf{Unit-Reflexive} if for any \(I \in \mathcal{C}\) and \(i \in UI\), we have \(\Delta^I_{\eta I} \cdot i, \eta I \cdot i \leq 0\).

\textbf{Composable} if for any \(I, J \in \mathcal{C}\), \(m, m' \in M, c, c' \in UTI\) and \(f, g: I \to TJ\), we have \(\Delta^m_{J^m} \circ (f^J \bullet c, g^J \bullet c') \leq \Delta^m_I (c, c') + \sup_{i \in UI} \Delta^p_I(f \bullet i, g \bullet i)\).

Table 1 shows examples of unit-reflexive and composable \(M\)-graded \(Q\)-divergences. Here, \(\mathcal{R}^+ = ([0, \infty], \leq, 0, +), \mathcal{Z} = (\varepsilon \cup [\infty, -\infty], +, 0, \leq)\) and \(\mathcal{H} = ([0, \infty], +, (0, 0))\) are pomonoids. The divergence DP is used for differential privacy in apRHL; \(\text{KL}\) is the Kullback-Leibler divergence; the monad \((\mathcal{H} \times -)\) describes deterministic computation with upper and lower bounds of costs, and \(\text{Clnt}\) is a divergence describing the difference of costs of two runs of programs.
Graded Relational Lifting. We now construct graded relational liftings recovering divergences. We fix a unit-reflexive and composable $M$-graded $Q$-divergence $\Delta$ on $T$. First, we define the category $\text{BRel}(\mathbb{C})$ of binary relations over $\mathbb{C}$. An object is a triple $X = (X_1, X_2, R_X)$ of $X_1, X_2 \in \mathbb{C}$ and an arbitrary subset $R_X \subseteq U X_1 \times U X_2$. An arrow $(X_1, X_2, R_X) \to (Y_1, Y_2, R_Y)$ is a pair $f_1 : X_1 \to Y_1$ and $f_2 : X_2 \to Y_2$ such that $(U f_1 \times U f_2)(R_X) \subseteq R_Y$. The evident projection functor sending $(X_1, X_2, R_X)$ to $(X_1, X_2)$ is denoted by $p$; $\text{BRel}(\mathbb{C}) \to \mathbb{C}$. $\text{Eq}_I$ denotes the equality relation $(I, I, \{(c, c) | c \in \text{UTI}\})$ for each $I \in \mathbb{C}$.

Second, we convert the divergence $\Delta$ into a family of binary relations. We define $\tilde{\Delta}(m, v) = (TI, TI, \{(c, c') | \Delta^{p}(c, c') \leq v\})$ for any $I \in \mathbb{C}$ and $(m, v) \in M \times Q$. Finally, in an analogous way as graded $TT$-lifting [1], we define a family $\{T^{\Delta}(m, v)\}_{(m, v) \in M \times Q}$ of $\text{BRel}(\mathbb{C})$-object constructors by

$$T^{\Delta}(m, v)X = \bigcap_{I \in \mathbb{C}} T^{\tilde{\Delta}}(m, v, X).$$

We define $T^{\Delta}(m, v)X = \bigcap_{I \in \mathbb{C}} T^{\tilde{\Delta}}(m, v, X)$. This is a desired graded relational lifting for divergences that recovers the $M$-graded $Q$-divergence $\Delta$.

Theorem 1. (1) The family $\{T^{\Delta}(m, v)\}_{(m, v) \in M \times Q}$ forms a $M \times Q$-graded lifting of the monad $T \times T$ along the functor $p$; $\text{BRel}(\mathbb{C}) \to \mathbb{C}^2$. (2) We have $T^{\Delta}(m, v)\text{Eq}_I = \tilde{\Delta}(m, v)$ for any $I \in \mathbb{C}$ and $(m, v) \in M \times Q$.

Example 1. The graded relational lifting used in a study [2] of program logic for verification of differential privacy is $G^{\text{DP}}_s$ and in fact this is the same as $G^{\text{DP}}_s$ because of the equality $\text{DP}^f_2(c, c') = \sup_{f : J \to G_s} \text{DP}^f_2(f^1 \circ c, f^2 \circ c')$.

Acknowledgements. The authors thank to Justin Hsu, Marco Gaboardi, Borja Balle and Gilles Barthe for discussions. This research was supperted by JST ERATO HASUO Metamathematics for Systems Design Project (No. JPMJER1603).

References