Divergences on Monads and Relational Liftings

Tetsuya Sato[1] and Shin-ya Katsumata[2]

[1] Seikei University
[2] National Institute of Informatics

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 *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: *composable* statistical divergences and *graded relational liftings* of monads recovers 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 *divergences on monads*, and construct graded relational liftings *recovering* divergences on monads using the codesinty lifting technique.

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

Divergences on Monads. We introduce the notion of *divergences on monads*, which captures various kinds of quantiative 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-graded Q-divergence* on T is a family $\{\Delta^m_I\colon UTI \times UTI \to Q\}_{m\in M, I\in\mathbb{C}}$ of functions satisfying the monotonicity condition on M: $m \leq n \implies \forall I \in \mathbb{C}. \forall c, c' \in UTI. \Delta^n_I(c, c') \leq \Delta^m_I(c, c')$. We say that Δ is:

Unit-Reflexive if for any $I \in \mathbb{C}$ and $i \in UI$, we have $\Delta^1_I(\eta_I \bullet i, \eta_I \bullet i) \leq 0$,
Composable if for any $I, J \in \mathbb{C}$, $m, m' \in M$, $c, c' \in UTI$ and $f, g\colon I \to TJ$, we have $\Delta^{m\cdot m'}_J(f^\sharp \bullet c, g^\sharp \bullet c') \leq \Delta^m_I(c, c') + \sup_{i\in UI} \Delta^{m'}_J(f \bullet i, g \bullet i)$.

Table 1 shows examples of unit-reflexive and composable M-graded Q-divergences. Here, $\mathcal{R}^+ = ([0, \infty], \leq, 0, +)$, $\mathcal{Z} = (\mathbb{Z} \cup \{\infty, -\infty\}, +, 0, \leq)$ and $\mathcal{H} = (\{(i, j) \in \mathbb{N}^2 \mid i \leq j\}, +, (0, 0))$ are pomonoids. The divergence DP is used for differential privacy in apRHL; KL is the Kullback-Leibler divergence; the monad $(\mathcal{H} \times -)$ describes deterministic computation with upper and lower bounds of costs, and CInt is a divergence describing the difference of costs of two runs of programs.

Δ	$\mathbb{C}$	T	M	Q	Definition
DP	**Meas**	G_s	$\mathcal{R}^+$	$\mathcal{R}^+$	$\mathsf{DP}^\varepsilon_I(\mu_1,\mu_2) = \sup_{M\in\Sigma_I}(\mu_1(M) - e^\varepsilon\mu_2(M))$
KL	**Meas**	G	1	$\mathcal{R}^+$	$\mathsf{KL}_I(\mu_1,\mu_2) = \int_I \mu_1(x)\log(\mu_1(x)/\mu_2(x))\ dx$
CInt	**Set**	$(\mathcal{H}\times -)$	1	$\mathcal{Z}$	$\mathsf{CInt}_I(((i,j),x),((k,l),y)) = \begin{cases} j-k & \text{if } x=y \\ \infty & \text{otherwise} \end{cases}$

Table 1. Examples of unit-reflexive and composable graded divergences

Graded Relational Lifting. We now construct graded relational liftings recovering divergences. We fix a unit-reflexive and composable M-graded Q-divergence Δ on T. First, we define the category $\mathbf{BRel}(\mathbb{C})$ 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 $R_X \subseteq UX_1 \times UX_2$. An arrow $(X_1, X_2, R_X) \to (Y_1, Y_2, R_Y)$ is a pair $f_1 \colon X_1 \to Y_1$ and $f_2 \colon X_2 \to Y_2$ such that $(Uf_1 \times Uf_2)(R_X) \subseteq R_Y$. The evident projection functor sending (X_1, X_2, R_X) to (X_1, X_2) is denoted by $p \colon \mathbf{BRel}(\mathbb{C}) \to \mathbb{C}^2$. Eq_I denotes the equality relation $(I, I, \{(c,c) | c \in UTI\})$ for each $I \in \mathbb{C}$.

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

$$T^{\tilde{\Delta}I}(m,v)X = \left(TX_1, TX_2, \left\{(c,c') \;\middle|\; \begin{array}{r}\forall(f_1,f_2)\in\mathbf{BRel}(\mathbb{C})(X,\tilde{\Delta}I(m',v')).\\ (f_1^\sharp \bullet c, f_2^\sharp \bullet c') \in \tilde{\Delta}I(m\cdot m', v+v')\end{array}\right\}\right).$$

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

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 $p\colon \mathbf{BRel}(\mathbb{C}) \to \mathbb{C}^2$.* (2) *We have $T^\Delta(m,v)\mathrm{Eq}_I = \tilde{\Delta}I(m,v)$ 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_s^{DP1} and in fact this is the same as G_s^{DP} because of the equality $\mathsf{DP}^\varepsilon_J(c,c') = \sup_{f\colon J\to G_s 1} \mathsf{DP}^\varepsilon_1(f^\sharp \bullet c, f^\sharp \bullet c')$.

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

References

1. Shin-ya Katsumata. Parametric effect monads and semantics of effect systems. In Suresh Jagannathan and Peter Sewell, editors, *The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014*, pages 633–646. ACM, 2014.
2. Tetsuya Sato. Approximate relational hoare logic for continuous random samplings. In Lars Birkedal, editor, *The Thirty-second Conference on the Mathematical Foundations of Programming Semantics, MFPS 2016, Carnegie Mellon University, Pittsburgh, PA, USA, May 23-26, 2016*, volume 325 of *Electronic Notes in Theoretical Computer Science*, pages 277–298. Elsevier, 2016.