A bunched logic for ℓ^p spaces

June Wunder
Arthur Azevedo de Amorim   Patrick Baillot   Marco Gaboardi

June 27, 2021

Boston University

Sensitivity

An important property of functions is s-sensitivity – related to lipschitz continuity and non-expansiveness.

$$d(f(x), f(y)) \leq s \cdot d(x, y)$$

Sensitivity

Sensitivity is useful for Differential Privacy, AI, etc which has motivated programming languages that track sensitivity at the type level

This talk

Graded affine linear bunched logic for tracking sensitivity in different ℓ^p spaces.

Prior Work: Fuzz

A higher order language for writing differentially private database queries.

$$x_1 :_{r_1} \tau_1, x_2 :_{r_2} \tau_2, \ldots, x_n :_{r_n} \tau_n, \vdash e : \tau'$$

Fuzz requires tracking the sensitivity of each variable.

Prior Work: Fuzz

A higher order language for writing differentially private database queries.

$$x_1 :_{r_1} \tau_1, x_2 :_{r_2} \tau_2, \ldots, x_n :_{r_n} \tau_n, \vdash e : \tau'$$

Fuzz requires tracking the sensitivity of each variable.

Connection to LL

Fuzz comes from bounded linear logic. $\otimes, \&, \oplus, \multimap, !_r A$

$$\frac{\Gamma \vdash e : \tau_1 \otimes \tau_2 \qquad \Delta, x :_r \tau_1, y :_r \tau_2 \vdash e' : \tau'}{\Delta + r\Gamma \vdash \textbf{let } (x, y) = e \textbf{ in } e' : \tau'} \otimes\mathrm{E}$$

Connection to LL

Fuzz comes from bounded linear logic. $\otimes, \&, \oplus, \multimap, !_r A$

$$\frac{\Gamma \vdash e : \tau_1 \otimes \tau_2 \qquad \Delta, x :_r \tau_1, y :_r \tau_2 \vdash e' : \tau'}{\Delta + r\Gamma \vdash \textbf{let } (x, y) = e \textbf{ in } e' : \tau'} \otimes\mathrm{E}$$

Semantics of Fuzz

$$x :_r \tau \vdash e : \tau'$$

$$\Longrightarrow$$

$$(!_r \tau) \multimap \tau'$$

$$\Longrightarrow$$

$$f : [\![\tau]\!] \to [\![\tau']\!]$$

(f is r-expansive)

Problem!

Fuzz natively supports two metric spaces for pairs, which is not expressive enough for some applications.

$$A \otimes B \triangleq [\![A]\!] \times [\![B]\!]; d(x, y) = d(x_1, y_1) + d(x_2, y_2)$$

$$A \,\&\, B \triangleq [\![A]\!] \times [\![B]\!]; d(x, y) = max\{d(x_1, y_1), d(x_2, y_2)\}$$

ℓ^p Metric

These metrics are special cases of the ℓ^p metric.

$$\ell^p(x, y) = \sqrt[p]{|x_1 - y_1|^p + |x_2 - y_2|^p}$$

Other ℓ^p norms are useful for different forms of DP, machine learning, etc

A Partial Solution: Duet

Duet extended Fuzz with ℓ^1, ℓ^2, and ℓ^∞ matrices as primitives. We present a logic for managing ℓ^p metrics natively.

$$\mathbb{M}_\ell[m, n]\ \tau$$

$$\ell \in \text{norm} ::= \ell^1 \mid \ell^2 \mid \ell^\infty$$

Example: Duet Overestimation

Suppose that we have a function which takes a pair in the ℓ^2 metric, is 2-sensitive to the first argument, and 1-sensitive to the second.

$$f : (!_2\mathbb{R}) \otimes_2 \mathbb{R} \multimap \mathbb{R}$$

This type is not expressible in Duet. Instead both elements must be treated as 2-sensitive.

$$f : (\mathbb{M}_{\ell_2}[2,1](!_2\mathbb{R})) \multimap \mathbb{R}$$

Contributions

We present a logic based on Fuzz's type system using bunched implications to manage function sensitivity under different ℓ^p metrics. Our main results:

- Semantics in metric spaces
- Proof of Cut Elimination

Formulas of ℓ^p Logic

$$A ::= 1 \mid \bot \mid \mathbb{R} \mid !_s A \mid A \multimap_p A \mid A \otimes_p A \mid A \oplus A$$

$$p \in \mathbb{R}^{\geq 1} \cup \{\infty\}$$

$$s \in \mathbb{R}^{\geq 0}$$

Formulas of ℓ^p Logic

$$A ::= 1 \mid \bot \mid \mathbb{R} \mid !_s A \mid A \multimap_p A \mid A \otimes_p A \mid A \oplus A$$

$$p \in \mathbb{R}^{\geq 1} \cup \{\infty\}$$

$$s \in \mathbb{R}^{\geq 0}$$

Bunched Environments

The strength of our logic comes from Bunches

$$\Gamma ::= \cdot \mid [A]_s \mid \Gamma \,,_p \Gamma$$

The $[A]_s$ form is the same sensitivity tracking in the environment as in Fuzz.

$\Gamma,_p \Gamma$ denotes two subtrees connected using the ℓ^p metric.

Bunches originally come from the Bunched Implications (BI) Logic and Separation Logic.

A fragment of ℓ^p Logic

$$\frac{\Gamma \,,_p [A]_1 \vdash B}{\Gamma \vdash A \multimap_p B} \multimap\mathrm{R} \qquad \frac{\Gamma \vdash A \qquad \Delta([B]_s) \vdash C}{\Delta([A \multimap_p B]_1 \,,_p s\Gamma) \vdash C} \multimap\mathrm{L}$$

$$\frac{\Gamma \vdash A \qquad \Delta \vdash B}{\Gamma \,,_p \Delta \vdash A \otimes_p B} \otimes\mathrm{R} \qquad \frac{\Gamma([A]_s \,,_p [B]_s) \vdash C}{\Gamma([A \otimes_p B]_s) \vdash C} \otimes\mathrm{L}$$

A fragment of ℓ^p Logic

$$\frac{\Gamma \vdash A}{s\Gamma \vdash !_s A}\ !\mathrm{R} \qquad \frac{\Gamma([A]_{r\cdot s}) \vdash B}{\Gamma([!_r A]_s) \vdash B}\ !\mathrm{L}$$

$$\frac{\Gamma(\Delta\ ,_p \Delta') \vdash A \qquad \Delta \approx \Delta'}{\Gamma(\mathit{Contr}(p, \Delta, \Delta')) \vdash A}\ \textsc{Contr} \qquad \frac{\Gamma(\cdot) \vdash A}{\Gamma(\Delta) \vdash A}\ \textsc{Weak}$$

$$\mathit{Contr}(p, \cdot, \cdot) = \cdot$$

$$\mathit{Contr}(p, [A]_s, [A]_r) = [A]_{\ell^p(s,r)}$$

$$\mathit{Contr}(p, (\Gamma_1 ,_q \Gamma_2), (\Delta_1 ,_q \Delta_2)) = \mathit{Contr}(p, \Gamma_1, \Delta_1) ,_q \mathit{Contr}(p, \Gamma_2, \Delta_2)$$

A fragment of ℓ^p Logic

$$\frac{\Gamma \vdash A}{s\Gamma \vdash !_s A}\ !\mathrm{R} \qquad \frac{\Gamma([A]_{r\cdot s}) \vdash B}{\Gamma([!_r A]_s) \vdash B}\ !\mathrm{L}$$

$$\frac{\Gamma(\Delta\ ,_p \Delta') \vdash A \qquad \Delta \approx \Delta'}{\Gamma(Contr(p, \Delta, \Delta')) \vdash A}\ \textsc{Contr} \qquad \frac{\Gamma(\cdot) \vdash A}{\Gamma(\Delta) \vdash A}\ \textsc{Weak}$$

$$Contr(p, \cdot, \cdot) = \cdot$$

$$Contr(p, [A]_s, [A]_r) = [A]_{\ell^p(s,r)}$$

$$Contr(p, (\Gamma_1 ,_q \Gamma_2), (\Delta_1 ,_q \Delta_2)) = Contr(p, \Gamma_1, \Delta_1) ,_q Contr(p, \Gamma_2, \Delta_2)$$

Bunched Environments

Bunches also allow some properties to fall out naturally such as distributivity of plus ($\oplus$) over with (& or $\otimes_\infty$).

- $A \otimes_\infty (B \oplus C) \vdash (A \otimes_\infty B) \oplus (A \otimes_\infty C)$
- $(A \otimes_\infty B) \oplus (A \otimes_\infty C) \vdash A \otimes_\infty (B \oplus C)$

Weakening Properties

Our logic is affine which allows for sensitivity “Subsumption” as a derived rule.

$$\frac{\Gamma(!_s A) \vdash B \qquad s \leq s'}{\Gamma(!_{s'} A) \vdash B}$$

Main Results – Cut Elimination

$$\frac{\Gamma \vdash A \qquad \Delta(A) \vdash B}{\Delta(\Gamma) \vdash B}\ \textsc{Cut}$$

The Cut rule is admissible in ℓ^p Logic. This proof is made difficult by bunched environments and the generalized contraction rule.

Main Results – Metric Spaces Semantics

Every formula in ℓ^p logic is equipped with a metric space and every derivation has an interpretation as a non-expansive function as follows:

$$\Gamma \vdash A \implies [\![\Gamma]\!]_e \to [\![A]\!]_{lf}$$

$[\![Axiom]\!]_d \triangleq \lambda x.\ x$

$[\![\multimap R\ \pi]\!]_d \triangleq \lambda \Gamma.\ \lambda A.\ [\![\pi]\!]_d\ (\Gamma, A)$

$[\![\otimes R\ \pi_1\ \pi_2]\!]_d \triangleq \lambda(\Gamma, \Delta).\ ([\![\pi_1]\!]_d\ \Gamma), ([\![\pi_2]\!]_d\ \Delta)$

$[\![\otimes L\ \pi]\!]_d \triangleq \lambda \Gamma(a, b).\ ([\![\pi]\!]_d\ \Gamma(a, b))$

Where next?

There's a lot of places we can take this project next.

- *Probabilistic Setting*
  Fuzz and Duet have a feature for DP called the "probability monad." This is entirely missing from our logic currently.
- *Term Calculus*
  Extending Duet/Fuzz further to handle ℓ^p metrics natively would be welcome features.

Thank you!