Computational Interpretations of Differential Logic

Jim Laird (University of Bath)

May 30, 2013

Computational Interpretations of Linear Logic

Samson's "Computational Interpretations of Linear Logic" (1993)

- Gave a "translation" from (french) logic to (english) computation.
- Introduced novel concepts — in particular, the idea of *proofs as processes*.
- Initiated much research into linear type theories for programming languages and process calculi.

Bellin and Scott (1994) showed that proofs as processes can be framed naturally in Milner's "Synchronous π-calculus". We will give operational and denotational interpretations of the latter, linking back to Samson's original work.

"Differential Logic"

A collection of formalisms for reasoning about *linearization*:

- Differential lambda-calculus (Erhard and Regnier) — λ-calculus with an operator obeying chain and product rules, Taylor expansion, etc.
- Differential Categories (Blute, Cockett and Seely) — categorical models for the above, based on models of LL.
- Differential nets (Ehrhard and Regnier) — graphical formalism for differential structure.

More differential ideas:

- The differential λ-calculus is "the same" as Boudol's *resource λ-calculus* (Tranquilli).
- There is an encoding of the finitary π-calculus in differential nets. (Ehrhard and Laurent).
- Manzonetto, McCusker and L. have studied free constructions of differential models based on relations, and on games — latterly (with Pagani) with a quantitative flavour.

Motivations - and connections to Samson's work

Aim - to understand the french results, and recast them in a quantitative setting, with a denotational semantics, yielding:

- A *quantitative* account of resource-sensitive computation.
- A typed (non-interleaving) model of concurrency.
- A modular way to combine structure (e.g. sequentiality) and valuations.
- A way to describe compact closed categories and bialgebras (cf. Fock Space).

A Calculus of Solos

E&L's representation of the π-calculus essentially factors via the Calculus of Solos (the Fusion Calculus without prefixing), which can encode the π-calculus via a clever trick due to Laneve. We will work with a typed, simplified version.
Terms are formed according to the grammar:

$$p, q ::= k \in S \mid x(\vec{y}) \mid \nu a.p \mid p|q \mid !p$$

where S is a set of constants ("scalars"), $a, b, c \ldots$ range over channel names, and $x, y, \ldots$ are metavariables ranging over channel *ends* $(a^+, a^-, b^+, b^-, \ldots)$

Types

- Channel ends are given complementary types:

$$T = X \mid X^* \mid \mu X.(T_1, \ldots, T_n)$$

  $(X^*)^* = X$ and $\mu X.(T_1, \ldots, T_n)^* = \mu X.(T_1^*, \ldots, T_n^*)$.
- Given a type $T = \mu X.(T_1, \ldots, T_n)$, let $T.i$ be the unfolding of the ith component — i.e. $T_i[T/X][T^*/X^*]$

Typing Judgements

$$\frac{}{x(y_1,\ldots,y_n)\vdash\Gamma,x\colon T;y_1\colon T.1^*,\ldots,y_n\colon T.n^*}$$

$$\frac{}{k\vdash\Gamma;\_}\,k\in S$$

$$\frac{p\vdash\Gamma;\Delta \qquad \vdash q;\Gamma;\Delta'}{p|q\vdash\Gamma;\Delta,\Delta'}$$

$$\frac{p\vdash\Gamma;\Delta,a^+\colon T,a^-\colon T^*}{\nu a.p\vdash\Gamma;\Delta}$$

$$\frac{p\vdash\Gamma;\_}{!p\vdash\Gamma;\_}$$

$$\frac{p\vdash\Gamma,x\colon T;\Delta}{p\vdash\Gamma;\Delta,x\colon T}$$

Evaluation Semantics

Fix a total Σ-semiring (commutative semiring with all countable sums) $R = (|R|, \Sigma, 0, ., 1)$ and interpretation of scalars in R.

$$\frac{}{(\{\};C)\Downarrow_R 1} \qquad \frac{(T;C)\Downarrow e}{(s,T;C)\Downarrow s.e}$$

$$\frac{(p,T;C,a)\Downarrow_R e}{(\nu a.p,T;C)\Downarrow_R e} \qquad \frac{(p,q,T;C)\Downarrow_R e}{(p|q,T;C)\Downarrow_R e}$$

$$\frac{(p^n,T;C)\Downarrow_R e_n}{(!p,T;C)\Downarrow_R \Sigma_{n\in\mathbb{N}} e_n}$$

$$\frac{(x(\vec{y_1}),\ldots,x(\vec{y_{i-1}}),x(\vec{y_{i+1}}),\ldots,x(\vec{y_n}),T[\vec{y_i}/\vec{\vec{z}}];C)\Downarrow_R e_i \qquad 1\leq i\leq n}{(\overline{x}(\vec{z}),x(\vec{y_1}),\ldots,x(\vec{y_n}),T;C)\Downarrow_R \Sigma_{i\leq n} e_i}\ x\notin FN(T)$$

Examples of notions of testing

- R is the two-point Boolean lattice $(\{\top, \bot\}, \bigvee, \bot, \wedge, \top)$. $\Downarrow_R$ is may-testing — does a reduction path to the empty configuration exist?
- R is the semiring of natural numbers $(\mathbb{N}^\infty, \Sigma, 0, \times, 1)$ — How many different reduction paths exist?
- R is a probability or log semiring, e.g. $(\mathbb{R}^\infty, \Sigma, 0, \times, 1)$ What is the probability of a successful reduction?
- R is an exotic semiring, e.g. $(\mathbb{N}^\infty, \bigwedge, \infty, +, 0)$ or $(\mathbb{R}^\infty, \bigvee, 0, +, 0)$. What is the cost of the least/most expensive path?

Each Σ-semiring induces a contextual equivalence $\sim_R$.

Expressiveness

We can express:

- Sums — $p(\vec{y}) + q(\vec{y}) = \nu a.a^{+}(\vec{y})|!(\nu\vec{y}.a^{-}(\vec{\overline{y}})|p)|!\nu\vec{y}.a^{-}(\vec{\overline{y}})|q)$ — note that this is idempotent iff R is a *dioid*.
- Units — $0{\sim_R}\nu a.a^{+}()$ and $1{\sim_R}!0$ — note that $1 \not\sim_R 0$ in general.
- Unguarded bound input — e.g. $\nu y.x(\overline{y})|p$ — cf. the synchronous π-calculus.
- Non-linear solos — e.g $x(y) = \nu a.x(a^{+})|!(\nu b.a^{-}(b^{+})|y(b^{-}))$.
- Differential/Resource λ-calculus — Milner's encoding of λ in π readily extends to *bags* of applicands.
- Guarded prefixing (π-calculus style) — we may delay communication on b by binding it to a channel communicated on a. Note that if a and b are the same channel, this requires recursive types.

Multiset Objects

In a commutative-monoid-enriched SMC, say that multiset object for A is a (commutative) bialgebra $(!A, \mu_A : !A \otimes !A \to !A, e_A : I \to !A, \delta_A : !A \to !A \otimes !A, \iota_A : !A \to I)$ with maps $\epsilon_A : A \to !A$ and $\eta_A : !A \to A$ such that:

(i) $\epsilon_A; \eta_A : A \to A = id_A$

(ii) $e_A; \eta_A : I \to A = 0$ and $\epsilon_A; \iota_A : A \to I = 0$

(iii) $\epsilon_A; \delta_A : A \to !A \otimes !A = \epsilon_A \otimes e_A + e_A \otimes \epsilon_A$ and $\mu_A; \eta_A : !A \otimes !A \to A = \eta_A \otimes \iota_A + \iota_A \otimes \eta_A$

Categorical Model

To model our type theory, we require:

- a *compact closed category* $(\mathcal{C}, I, \otimes)$, which is
- Σ-monoid-enriched, and
- a self-dual functor $! : \mathcal{C} \longrightarrow \mathcal{C}$, with natural commutative monoid structure, and a nat. trans. $\epsilon : I \longrightarrow !$ making $(!A, \mu_A, e_A, \mu^*_{A^*}, e^*_{A^*}, \epsilon_A, \epsilon^*_{A^*})$ a multiset object for A.

Note that if $\mathcal{C}$ is Σ-monoid enriched, then $\mathcal{C}(I, I)$ is a Σ-semiring (R_I) and $\mathcal{C}$ is R_I Σ-semimodule enriched.

Examples

For any Σ-semiring R, the following (symmetric monoidal) categories are equivalent:

- The category of R-weighted relations (objects are sets and morphisms from A to B are maps from $A \times B$ to R, composed by setting $f;g(a,c) = \Sigma\{f(a,b).g(b,c) \mid b \in B\}$).
- The Kleisli category of the monad R^{-} on the category of sets and functions.
- The symmetric monoidal category of free R Σ-semimodules and countably additive functions.
- The symmetric monoidal category of all R Σ-semimodules (by Zorn's lemma).

Every object is self-dual, and for any set A, the set $!A$ of finite multisets over A is a multiset object over A.

Multiset Objects as Limits/Colimits

Let N be the (symmetric monoidal) category in which objects are natural numbers and morphisms are permutations.

- If $!A$ is a limit and a colimit for the diagram $J_A : N \to \mathcal{C}$ sending n to $A^{\otimes n}$ and each permutation to the corresponding isomorphism, then it is a multiset object.
- Given any multiset object $!A$, we have maps $p_n : !A \to A^{\otimes n}$ and $i_n : A^{\otimes n} \to !A$. If $\Sigma_{n \in \omega} p_n ; i_n$ is the identity on $!A$, then $!A$ is a limit/colimit for J_A.
- Any such object is the free monoid/cofree comonoid - so we have a (degenerate) model of linear logic, which is also a differential category.

Constructing models

We can construct a limit/colimit for J_A as the infinite biproduct of tensor powers $\bigoplus_{i\in\omega} A^i$. We can obtain these from free constructions:

- R-semimodule enrichment — take the category of objects of $\mathcal{C}$ in which morphisms from A to B are functions from $\mathcal{C}(A, B)$ to R.
- Countable biproducts —take the category of indexed families of objects of $\mathcal{C}$ and *matrices* of morphisms.
- Tensor powers — take the Karoubi envelope $\mathcal{K}(\mathcal{C})$ (we need R_I to have *natural number division*) — we can use the idempotent $\frac{\Sigma\{J_A(\pi) \mid \pi\in perm(n)\}}{n!}$ to build tensor powers of A.

Denotational Semantics

- Types are interpreted as functors — in particular $\mu X.(T_1, \ldots, T_n)$ as an invariant for $!\llbracket T_1 \rrbracket \otimes \ldots \otimes !\llbracket T_n \rrbracket$ (a fixed point in our indexed families construction).
- Terms interpret as morphisms — solos as unit morphisms, parallel compositions as the tensor product, and restriction as the canonical trace operator (composition with the counit).

Full abstraction

Theorem Any instance of our categorical model is sound ($p \Downarrow_R e \iff [\![p]\!]_R = e$).
Theorem R-semimodule interpretation is fully abstract ($p {\sim_R} q \iff [\![p]\!]_R = [\![q]\!]_R$).

Conclusions

- R-semimodules are just the biproduct completion of the one-object category R — what about starting with more interesting structure (e.g. games) and how do we represent it syntactically.
- What about a richer typing system — e.g. linear types.
- How much of our construction can be carried out in categories which don't have all infinite sums (e.g. Hilbert Spaces)?