Linear Logic and Linear Algebra

Steve Zdancewic

November 9, 2012

(work in progress!)

(Intuitionistic) Linear Logic

$$
\begin{array}{rcll}
A, B & ::= & 0 & \textit{additive sum unit} \\
 & \mid & 1 & \textit{multiplicative product unit} \\
 & \mid & \top & \textit{additive product unit} \\
 & \mid & \bot & \textit{multiplicative sum unit} \\
 & \mid & A \oplus B & \textit{additive sum} \\
 & \mid & A \mathbin{\&} B & \textit{additive product} \\
 & \mid & A \otimes B & \textit{multiplicative product} \\
 & \mid & A \multimap B & \textit{linear implication} \\
 & \mid & !A & \textit{exponential} \\
 & & & \\
\Gamma & ::= & A & \textit{contexts} \\
 & \mid & \Gamma \otimes \Gamma & \\
 & & & \\
 & & \Gamma \vdash A & \textit{judgments}
\end{array}
$$

Denotational (Categorical) Models

Basic idea:

- Interpret each type A as some structure $[\![A]\!]$
- Interpret each judgement $\Gamma \vdash A$ as a "morphism"

$$[\![\Gamma \vdash A]\!] : [\![\Gamma]\!] \to [\![A]\!]$$

- Interpret inference rules compositionally

Interpretations should "respect" proof equivalences, *e.g.*:

$$\left[\!\!\left[\frac{\overline{A \vdash A} \quad \overline{B \vdash B}}{A \otimes B \vdash A \otimes B} \right]\!\!\right] = [\![\overline{A \otimes B \vdash A \otimes B}]\!]$$

Many Models of Linear Logic

(Fairly?) Simple:

- Sets and Relations

$$\begin{array}{rcl}
[\![0]\!] & = & \emptyset \\
[\![1]\!] & = & \{\bullet\} \\
[\![A \oplus B]\!] & = & [\![A]\!] \uplus [\![B]\!] \\
& \ldots & \\
[\![A \vdash A]\!] & = & \{(x, x) \mid x \in [\![A]\!]\} \\
[\![A \vdash A \oplus B]\!] & = & \{(x, \mathrm{inl}\ x) \mid x \in [\![A]\!]\} \\
& \ldots &
\end{array}$$

(Fairly?) Complex:

- Coherence Spaces, Proof Nets, Game Semantics

Linear Logic and Linear Algebra

FinVect:

- Interpret a type as a *finite dimensional vector space* (over a *finite* field)
- Interpret a judgment as a *linear transformation* (*i.e.*, a matrix)

Linear Logic and Linear Algebra

FinVect:

- Interpret a type as a *finite dimensional vector space* (over a *finite* field)
- Interpret a judgment as a *linear transformation* (*i.e.*, a matrix)

Why?

- Next simplest reasonable model (after Set).
- I haven't seen this worked out in detail anywhere before.
- There are lots of interesting things that live in the category FinVect:
  - All of linear algebra: Matrix algebra, derivatives, eigenvectors, Fourier transforms, cryptography(?), *etc.*

Linear Algebra

Fields

A *field* $\mathbb{F} = (F, +, \cdot, 0, 1)$ is a structure such that:

- F is a set containing distinct elements 0 and 1.
- *Addition*: $(F, +, 0)$ abelian group, identity 0
- *Multiplication*: $(F - \{0\}, \cdot, 1)$: abelian group, identity 1
- The *distributive law* holds:

$$\forall a, b, c \in F.\ a \cdot (b + c) = a \cdot b + a \cdot c$$

- There are *no zero divisors*:

$$\forall a, b \in F.\ a \cdot b = 0 \implies a = 0 \vee b = 0$$

Vector Spaces

A vector space over $\mathbb{F}$ is just a set V with addition and scalar multiplication:

$$\forall v, w \in V.\ (v + w) \in V$$

$$\forall \alpha \in \mathbb{F}.\ \forall v \in V.\ \alpha v \in V$$

Satisfying some laws:

- Commutativity, Associativity, Unit for $+$
- $\alpha(v + w) = \alpha v + \alpha w$
- $(\alpha + \beta)v = \alpha v + \beta v$

Coordinate Systems

Pick a *coordinate system* (*i.e.* a set X) and define $[X]$, the "vector space with coordinates in X":

$$[X] \triangleq \{v \mid v : X \to \mathbb{F}\}$$

- A vector is just a function that maps each coordinate to an element of $\mathbb{F}$
  - Example: In the plane, we might pick $X = \{\text{"x"}, \text{"y"}\}$
- Vector addition and scalar multiplication are defined *pointwise*
- The *dimension* of $[X]$ is just the cardinality of X.

Canonical Basis

Canonical basis for $[X]$:

$$\{\delta_x \mid x \in X\}$$

- Here δ is Dirac's "delta" operator:

$$\delta_x \;=\; \lambda y \in X.\; \begin{cases} 1 & \text{if } y = x \\ 0 & \text{if } y \neq x \end{cases}$$

- Every vector in $[X]$ can be written as a weighted sum of basis elements.

$$\begin{bmatrix} 3 \\ 4 \end{bmatrix} = 3 \cdot \delta_x + 4 \cdot \delta_y$$

Linear Maps

A linear transformation $f : [X] \rightarrow [Y]$ is a function such that:

$$f(\alpha v + \beta w) = \alpha f(v) + \beta f(w)$$

f is completely characterized by its behavior on the set of basis vectors of $[X]$.

$$f(\delta_x) = \sum_{y \in Y} M_f[y, x] \delta_y$$

Here: $M_f[y, x]$ is a (matrix) of scalars in $\mathbb{F}$

Matrices

If $[X]$ has n coordinates and $[Y]$ has m coordinates, then any linear map $f : [X] \to [Y]$ can be represented as a matrix:

$$\begin{bmatrix} f[y_1, x_1] & f[y_1, x_2] & \cdots & f[y_1, x_n] \\ f[y_2, x_1] & f[y_2, x_2] & \cdots & f[y_2, x_n] \\ \vdots & \vdots & \ddots & \vdots \\ f[y_m, x_1] & f[y_m, x_2] & \cdots & f[y_m, x_n] \end{bmatrix}$$

For example, the 3x3 *identity* map:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} \bullet & \cdot & \cdot \\ \cdot & \bullet & \cdot \\ \cdot & \cdot & \bullet \end{bmatrix}$$

Linear Logic

Multiplicative Unit: 1

Interpret 1 as a vector space:

Multiplicative Unit: 1

Interpret 1 as a vector space:

- Coordinates: $1^\dagger = \{\bullet\}$
- $[\![1]\!] = [1^\dagger]$ $\qquad (= \{v \mid v : 1^\dagger \to \mathbb{F}\})$

Interpret the “1 introduction” inference rule as the 1x1 identity matrix:

$$[\![1 \vdash 1]\!] = [1]$$

Multiplicative Product: $A \otimes B$

Interpret $A \otimes B$ as a vector space:

Multiplicative Product: $A \otimes B$

Interpret $A \otimes B$ as a vector space:

- Coordinates: $(A \otimes B)^{\dagger} = A^{\dagger} \times B^{\dagger}$
- $[\![A \otimes B]\!] = [(A \otimes B)^{\dagger}]$

Multiplicative Product: $A \otimes B$

Interpret $A \otimes B$ as a vector space:

- Coordinates: $(A \otimes B)^\dagger = A^\dagger \times B^\dagger$
- $[\![A \otimes B]\!] = [(A \otimes B)^\dagger]$

Interpret $\otimes$ introduction:

$$\frac{\Gamma_1 \vdash A \quad \Gamma_2 \vdash B}{\Gamma_1 \otimes \Gamma_2 \vdash A \otimes B}$$

Multiplicative Product: $A \otimes B$

Interpret $A \otimes B$ as a vector space:

- Coordinates: $(A \otimes B)^{\dagger} = A^{\dagger} \times B^{\dagger}$
- $[\![A \otimes B]\!] = [(A \otimes B)^{\dagger}]$

Interpret $\otimes$ introduction:

$$\frac{\Gamma_1 \vdash A \quad \Gamma_2 \vdash B}{\Gamma_1 \otimes \Gamma_2 \vdash A \otimes B} \qquad \frac{f : [\![\Gamma_1]\!] \longrightarrow [\![A]\!] \quad g : [\![\Gamma_2]\!] \longrightarrow [\![B]\!]}{f \otimes g : [\![\Gamma_1 \otimes \Gamma_2]\!] \longrightarrow [\![A \otimes B]\!]}$$

$$(f \otimes g)[(a, b), (x, y)] = f[a, x] \cdot g[b, y]$$

Multiplicative Product: Examples

$$f \qquad \begin{bmatrix} \bullet & \cdot & \bullet \\ \cdot & \bullet & \cdot \\ \cdot & \bullet & \cdot \end{bmatrix}$$

$$g \qquad \begin{bmatrix} \bullet & \cdot \\ \bullet & \bullet \end{bmatrix}$$

$f \otimes g$

$g \otimes f$

Multiplicative Product: Examples

$$f = \begin{bmatrix} \bullet & \cdot & \bullet \\ \cdot & \bullet & \cdot \\ \cdot & \bullet & \cdot \end{bmatrix} \qquad g = \begin{bmatrix} \bullet & \cdot \\ \bullet & \bullet \end{bmatrix}$$

$$f \otimes g = \begin{bmatrix} \bullet & \cdot & \cdot & \cdot & \bullet & \cdot \\ \bullet & \bullet & \cdot & \cdot & \bullet & \bullet \\ \cdot & \cdot & \bullet & \cdot & \cdot & \cdot \\ \cdot & \cdot & \bullet & \bullet & \cdot & \cdot \\ \cdot & \cdot & \bullet & \cdot & \cdot & \cdot \\ \cdot & \cdot & \bullet & \bullet & \cdot & \cdot \end{bmatrix} \qquad g \otimes f = \begin{bmatrix} \bullet & \cdot & \bullet & \cdot & \cdot & \cdot \\ \cdot & \bullet & \cdot & \cdot & \cdot & \cdot \\ \cdot & \bullet & \cdot & \cdot & \cdot & \cdot \\ \bullet & \cdot & \bullet & \bullet & \cdot & \bullet \\ \cdot & \bullet & \cdot & \cdot & \bullet & \cdot \\ \cdot & \bullet & \cdot & \cdot & \bullet & \cdot \end{bmatrix}$$

Multiplicative Product: Structural Rules

Contexts:

$$\Gamma ::= A \mid \Gamma \otimes \Gamma$$

Structural Rule:

$$\frac{\Gamma_1 \vdash A \quad \Gamma_1 \equiv \Gamma_2}{\Gamma_2 \vdash A}$$

$\Gamma_1 \equiv \Gamma_2$

- reflexivity, symmetry, transitivity
- associativity: $(\Gamma_1 \otimes \Gamma_2) \otimes \Gamma_3 \equiv \Gamma_1 \otimes (\Gamma_2 \otimes \Gamma_3)$
- unit law: $\Gamma \equiv \Gamma \otimes 1$
- commutativity: $\Gamma_1 \otimes \Gamma_2 \equiv \Gamma_2 \otimes \Gamma_1$
- $[\![\Gamma_1 \equiv \Gamma_2]\!]$ is an isomorphism

Function Composition

Function Composition

Given $f : [X] \rightarrow [Z]$ and $g : [Z] \rightarrow [Y]$, define

$$(f ; g)[y, x] = \sum_{z \in Z} g[y, z] \cdot f[z, x]$$

(a.k.a. matrix multiplication)

Function Composition

Function Composition

Given $f : [X] \to [Z]$ and $g : [Z] \to [Y]$, define

$$(f; g)[y, x] = \sum_{z \in Z} g[y, z] \cdot f[z, x]$$

(a.k.a. matrix multiplication)

Note: We *sum* over all elements of Z, so this is *not necessarily defined* if Z is infinite!

- Option 1: Allow infinite matrices but only those with "finite support" (zero almost everywhere)
- Option 2: Work with only finite matrices.

Identity and Cut

Identity:

$$\frac{}{A \vdash A}$$

$$\mathrm{id}_A[y,x] \;=\; \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

Identity and Cut

Identity:

$$\frac{}{A \vdash A}$$

$$\mathrm{id}_A[y,x] \;=\; \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

Cut:

$$\frac{\Gamma_1 \vdash A \quad A \otimes \Gamma_2 \vdash B}{\Gamma_1 \otimes \Gamma_2 \vdash B}$$

$$\frac{f : [\![\Gamma_1]\!] \longrightarrow [\![A]\!] \quad g : [\![A \otimes \Gamma_2]\!] \longrightarrow [\![B]\!]}{(f \otimes \mathrm{id}_{\Gamma_2}); g : [\![\Gamma_1 \otimes \Gamma_2]\!] \longrightarrow [\![A \otimes B]\!]}$$

Additive Sums

Interpret $A \oplus B$ as a vector space:

Additive Sums

Interpret $A \oplus B$ as a vector space:

- Coordinates: $(A \oplus B)^{\dagger} = A^{\dagger} \uplus B^{\dagger}$
- $\llbracket A \oplus B \rrbracket = [(A \oplus B)^{\dagger}]$

Additive Sums

Interpret $A \oplus B$ as a vector space:

- Coordinates: $(A \oplus B)^\dagger = A^\dagger \uplus B^\dagger$
- $[\![A \oplus B]\!] = [(A \oplus B)^\dagger]$

Interpret $\oplus$ introduction:

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \oplus B} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \oplus B}$$

$$\mathrm{inl}_{A,B}[y, x] = \begin{cases} 1 & \text{if } y = \mathrm{inl}\ x \\ 0 & \text{otherwise} \end{cases}$$

Additive Sums

Booleans (over $\mathbb{F}_2$):

$$\mathbb{B} = 1 \oplus 1$$

$$\begin{bmatrix} \cdot \\ \cdot \end{bmatrix} \quad \begin{bmatrix} \bullet \\ \cdot \end{bmatrix} \quad \begin{bmatrix} \cdot \\ \bullet \end{bmatrix} \quad \begin{bmatrix} \bullet \\ \bullet \end{bmatrix}$$

$$\mathrm{inl}_{\mathbb{B},\mathbb{B}} : [\![\mathbb{B}]\!] \to [\![\mathbb{B}]\!] \oplus [\![\mathbb{B}]\!] \qquad \mathrm{inr}_{\mathbb{B},\mathbb{B}} : [\![\mathbb{B}]\!] \to [\![\mathbb{B}]\!] \oplus [\![\mathbb{B}]\!]$$

$$\begin{bmatrix} \bullet & \cdot \\ \cdot & \bullet \\ \cdot & \cdot \\ \cdot & \cdot \end{bmatrix} \qquad \begin{bmatrix} \cdot & \cdot \\ \cdot & \cdot \\ \bullet & \cdot \\ \cdot & \bullet \end{bmatrix}$$

Exponential Types

Linear Logic: Exponentials

Dereliction

$$\frac{\Gamma \otimes A \vdash B}{\Gamma \otimes !A \vdash B}$$

Weakening

$$\frac{\Gamma \otimes 1 \vdash B}{\Gamma \otimes !A \vdash B}$$

Contraction

$$\frac{\Gamma \otimes (!A \otimes !A) \vdash B}{\Gamma \otimes !A \vdash B}$$

Introduction

$$\frac{!\Gamma \vdash A}{!\Gamma \vdash !A}$$

! is a Comonad

- ! is a functor:
  - On types: for vector space $[\![A]\!]$, need a vector space $![\![A]\!]$
  - On functions: For $f : [\![A]\!] \to [\![B]\!]$, need $!f :![\![A]\!] \to ![\![B]\!]$

$$\mathrm{coreturn}_A : ![\![A]\!] \to [\![A]\!]$$

$$\mathrm{comultiply}_A : ![\![A]\!] \to !![\![A]\!]$$

- Satisfying the comonad laws.
- Plus some other operations: $m : !A \otimes !B \to !(A \otimes B)$

Exponentiating a Vector Space

Morally, we would like:

$$!A \approx 1 \oplus A \oplus A^2 \oplus A^3 \oplus \dots$$

Exponentiating a Vector Space

Morally, we would like:

$$!A \approx 1 \oplus A \oplus A^2 \oplus A^3 \oplus \dots$$

Analogy: In $\textsc{Set}$ $[\![!A]\!]$ is the set of all finite multisets whose elements are drawn from $[\![A]\!]$.

- So the *coordinates* of the vector space corresponding to $!A$ should (morally) be finite multisets drawn from A.
- Example: Write $\mathbb{B}^\dagger = \{\mathrm{inl}\ \bullet, \mathrm{inr}\ \bullet\}$ as $\{0, 1\}$

$$(!\mathbb{B})^\dagger = \{\emptyset, \{0\}, \{1\}, \{0, 0\}, \{0, 1\}, \{1, 1\}, \{0, 0, 0\}, \dots\}$$

Exponentiating a Vector Space

Morally, we would like:

$$!A \approx 1 \oplus A \oplus A^2 \oplus A^3 \oplus \dots$$

Analogy: In $\textsc{Set}$ $[\![!A]\!]$ is the set of all finite multisets whose elements are drawn from $[\![A]\!]$.

- So the *coordinates* of the vector space corresponding to $!A$ should (morally) be finite multisets drawn from A.
- Example: Write $\mathbb{B}^\dagger = \{\mathrm{inl}\ \bullet, \mathrm{inr}\ \bullet\}$ as $\{0, 1\}$

$$(!\mathbb{B})^\dagger = \{\emptyset, \{0\}, \{1\}, \{0, 0\}, \{0, 1\}, \{1, 1\}, \{0, 0, 0\}, \dots\}$$

Problem: This isn't finite! (But we persevere anyway. . .)

Vectors With Multisets as Coords

$$(!\mathbb{B})^{\dagger} = \{\emptyset, \{0\}, \{1\}, \{0,0\}, \{0,1\}, \{1,1\}, \{0,0,0\}, \ldots\}$$

One more observation: What would a vector with coordinates as above look like?

$$\begin{array}{rcc} v & = & \alpha_{\emptyset}\cdot\delta_{\emptyset} \\ & + & \alpha_{\{0\}}\cdot\delta_{\{0\}} \\ & + & \alpha_{\{1\}}\cdot\delta_{\{1\}} \\ & + & \alpha_{\{0,0\}}\cdot\delta_{\{0,0\}} \\ & + & \alpha_{\{0,1\}}\cdot\delta_{\{0,1\}} \\ & + & \alpha_{\{1,1\}}\cdot\delta_{\{1,1\}} \\ & + & \alpha_{\{0,0,0\}}\cdot\delta_{\{0,0,0\}} \\ & \vdots & . \end{array}$$

Multinomials

Suppose we knew that we would only ever need multisets with at most two of each element?

$$(!\mathbb{B})^\dagger = \begin{array}{ll} \{ & \emptyset, \{0\}, \{1\}, \{0,0\}, \{0,1\}, \\ & \{1,1\}, \{1,1,0\}, \{1,0,0\}, \{1,1,0,0\} \quad \} \end{array}$$

$$\begin{array}{rcr} v & = & \alpha_\emptyset \cdot \delta_\emptyset \\ & + & \alpha_{\{0\}} \cdot \delta_{\{0\}} \\ & + & \alpha_{\{1\}} \cdot \delta_{\{1\}} \\ & + & \alpha_{\{0,0\}} \cdot \delta_{\{0,0\}} \\ & + & \alpha_{\{0,1\}} \cdot \delta_{\{0,1\}} \\ & + & \alpha_{\{1,1\}} \cdot \delta_{\{1,1\}} \\ & + & \alpha_{\{1,1,0\}} \cdot \delta_{\{1,1,0\}} \\ & + & \alpha_{\{1,0,0\}} \cdot \delta_{\{1,0,0\}} \\ & + & \alpha_{\{1,1,0,0\}} \cdot \delta_{\{1,1,0,0\}} \end{array}$$

Multinomials

Suppose we knew that we would only ever need multisets with at most two of each element?

$$(!\mathbb{B})^\dagger = \begin{array}{ll} \{ & \emptyset, \{0\}, \{1\}, \{0,0\}, \{0,1\}, \\ & \{1,1\}, \{1,1,0\}, \{1,0,0\}, \{1,1,0,0\} \quad \} \end{array}$$

$$\begin{array}{rcc} v & = & \alpha_\emptyset \cdot \delta_\emptyset \\ & + & \alpha_{\{0\}} \cdot \delta_{\{0\}} \\ & + & \alpha_{\{1\}} \cdot \delta_{\{1\}} \\ & + & \alpha_{\{0,0\}} \cdot \delta_{\{0,0\}} \\ & + & \alpha_{\{0,1\}} \cdot \delta_{\{0,1\}} \\ & + & \alpha_{\{1,1\}} \cdot \delta_{\{1,1\}} \\ & + & \alpha_{\{1,1,0\}} \cdot \delta_{\{1,1,0\}} \\ & + & \alpha_{\{1,0,0\}} \cdot \delta_{\{1,0,0\}} \\ & + & \alpha_{\{1,1,0,0\}} \cdot \delta_{\{1,1,0,0\}} \end{array} \quad \Rightarrow \quad \begin{array}{rcl} v & = & \alpha_{00} \cdot \mathbf{x}_0^0 \mathbf{x}_1^0 \\ & + & \alpha_{10} \cdot \mathbf{x}_0^1 \mathbf{x}_1^0 \\ & + & \alpha_{01} \cdot \mathbf{x}_0^0 \mathbf{x}_1^1 \\ & + & \alpha_{20} \cdot \mathbf{x}_0^2 \mathbf{x}_1^0 \\ & + & \alpha_{11} \cdot \mathbf{x}_0^1 \mathbf{x}_1^1 \\ & + & \alpha_{02} \cdot \mathbf{x}_0^0 \mathbf{x}_1^2 \\ & + & \alpha_{21} \cdot \mathbf{x}_0^2 \mathbf{x}_1^1 \\ & + & \alpha_{12} \cdot \mathbf{x}_0^1 \mathbf{x}_1^2 \\ & + & \alpha_{22} \cdot \mathbf{x}_0^2 \mathbf{x}_1^2 \end{array}$$

Multinomials

Suppose we knew that we would only ever need multisets with at most two of each element?

$$(!\mathbb{B})^\dagger = \left\{ \begin{array}{l} \emptyset, \{0\}, \{1\}, \{0,0\}, \{0,1\}, \\ \{1,1\}, \{1,1,0\}, \{1,0,0\}, \{1,1,0,0\} \end{array} \right\}$$

$$\begin{array}{rcc c rcl c rcl}
v & = & \alpha_{\emptyset}\cdot\delta_{\emptyset} & & v & = & \alpha_{00}\cdot\mathbf{x}_0^0\mathbf{x}_1^0 & & v & = & \alpha_{00}\cdot\mathbf{1} \\
 & + & \alpha_{\{0\}}\cdot\delta_{\{0\}} & & & + & \alpha_{10}\cdot\mathbf{x}_0^1\mathbf{x}_1^0 & & & + & \alpha_{10}\cdot\mathbf{x}_0 \\
 & + & \alpha_{\{1\}}\cdot\delta_{\{1\}} & & & + & \alpha_{01}\cdot\mathbf{x}_0^0\mathbf{x}_1^1 & & & + & \alpha_{01}\cdot\mathbf{x}_1 \\
 & + & \alpha_{\{0,0\}}\cdot\delta_{\{0,0\}} & & & + & \alpha_{20}\cdot\mathbf{x}_0^2\mathbf{x}_1^0 & & & + & \alpha_{20}\cdot\mathbf{x}_0^2 \\
 & + & \alpha_{\{0,1\}}\cdot\delta_{\{0,1\}} & \Rightarrow & & + & \alpha_{11}\cdot\mathbf{x}_0^1\mathbf{x}_1^1 & \Rightarrow & & + & \alpha_{11}\cdot\mathbf{x}_0\mathbf{x}_1 \\
 & + & \alpha_{\{1,1\}}\cdot\delta_{\{1,1\}} & & & + & \alpha_{02}\cdot\mathbf{x}_0^0\mathbf{x}_1^2 & & & + & \alpha_{02}\cdot\mathbf{x}_1^2 \\
 & + & \alpha_{\{1,1,0\}}\cdot\delta_{\{1,1,0\}} & & & + & \alpha_{21}\cdot\mathbf{x}_0^2\mathbf{x}_1^1 & & & + & \alpha_{21}\cdot\mathbf{x}_0^2\mathbf{x}_1 \\
 & + & \alpha_{\{1,0,0\}}\cdot\delta_{\{1,0,0\}} & & & + & \alpha_{12}\cdot\mathbf{x}_0^1\mathbf{x}_1^2 & & & + & \alpha_{12}\cdot\mathbf{x}_0\mathbf{x}_1^2 \\
 & + & \alpha_{\{1,1,0,0\}}\cdot\delta_{\{1,1,0,0\}} & & & + & \alpha_{22}\cdot\mathbf{x}_0^2\mathbf{x}_1^2 & & & + & \alpha_{22}\cdot\mathbf{x}_0^2\mathbf{x}_1^2
\end{array}$$

Multinomials

Suppose we knew that we would only ever need multisets with at most two of each element?

$$(!\mathbb{B})^{\dagger} = \begin{array}{ll} \{ & \emptyset, \{0\}, \{1\}, \{0,0\}, \{0,1\}, \\ & \{1,1\}, \{1,1,0\}, \{1,0,0\}, \{1,1,0,0\} \quad \} \end{array}$$

$$\begin{array}{rcc c rcl c rcl}
v & = & \alpha_{\emptyset} \cdot \delta_{\emptyset} & & v & = & \alpha_{00} \cdot \mathbf{x}_0^0 \mathbf{x}_1^0 & & v & = & \alpha_{00} \cdot \mathbf{1} \\
 & + & \alpha_{\{0\}} \cdot \delta_{\{0\}} & & & + & \alpha_{10} \cdot \mathbf{x}_0^1 \mathbf{x}_1^0 & & & + & \alpha_{10} \cdot \mathbf{x}_0 \\
 & + & \alpha_{\{1\}} \cdot \delta_{\{1\}} & & & + & \alpha_{01} \cdot \mathbf{x}_0^0 \mathbf{x}_1^1 & & & + & \alpha_{01} \cdot \mathbf{x}_1 \\
 & + & \alpha_{\{0,0\}} \cdot \delta_{\{0,0\}} & & & + & \alpha_{20} \cdot \mathbf{x}_0^2 \mathbf{x}_1^0 & & & + & \alpha_{20} \cdot \mathbf{x}_0^2 \\
 & + & \alpha_{\{0,1\}} \cdot \delta_{\{0,1\}} & \Rightarrow & & + & \alpha_{11} \cdot \mathbf{x}_0^1 \mathbf{x}_1^1 & \Rightarrow & & + & \alpha_{11} \cdot \mathbf{x}_0 \mathbf{x}_1 \\
 & + & \alpha_{\{1,1\}} \cdot \delta_{\{1,1\}} & & & + & \alpha_{02} \cdot \mathbf{x}_0^0 \mathbf{x}_1^2 & & & + & \alpha_{02} \cdot \mathbf{x}_1^2 \\
 & + & \alpha_{\{1,1,0\}} \cdot \delta_{\{1,1,0\}} & & & + & \alpha_{21} \cdot \mathbf{x}_0^2 \mathbf{x}_1^1 & & & + & \alpha_{21} \cdot \mathbf{x}_0^2 \mathbf{x}_1 \\
 & + & \alpha_{\{1,0,0\}} \cdot \delta_{\{1,0,0\}} & & & + & \alpha_{12} \cdot \mathbf{x}_0^1 \mathbf{x}_1^2 & & & + & \alpha_{12} \cdot \mathbf{x}_0 \mathbf{x}_1^2 \\
 & + & \alpha_{\{1,1,0,0\}} \cdot \delta_{\{1,1,0,0\}} & & & + & \alpha_{22} \cdot \mathbf{x}_0^2 \mathbf{x}_1^2 & & & + & \alpha_{22} \cdot \mathbf{x}_0^2 \mathbf{x}_1^2
\end{array}$$

Upshot: A vector whose coordinates are multisets over *A* can be thought of as a *multinomial* with one variable for each element of *A*.

Finite Fields

A field $\mathbb{F}$ is finite if $|F|$ is finite.

Some beautiful theorems:

- Every finite field $\mathbb{F}_q$ with q elements has $q = p^k$, where p is a prime.
- For every element $\alpha \in \mathbb{F}_q$ we have:
  - $\underbrace{\alpha + \alpha + \ldots + \alpha}_{\text{p times}} = 0$
  - $\alpha^q = \alpha$

Finite Fields

A field $\mathbb{F}$ is finite if $|F|$ is finite.

Some beautiful theorems:

- Every finite field $\mathbb{F}_q$ with q elements has $q = p^k$, where p is a prime.
- For every element $\alpha \in \mathbb{F}_q$ we have:
  - $\underbrace{\alpha + \alpha + \ldots + \alpha}_{\text{p times}} = 0$
  - $\alpha^q = \alpha$

Consequence:

When working with multinomials whose variables range over elements of $\mathbb{F}$, we have $\mathbf{x}^q = \mathbf{x}$.
For example, in $\mathbb{F}_2$:

$$(\mathbf{x} + \mathbf{1})^2 \quad = \quad \mathbf{x}^2 + 2\mathbf{x} + \mathbf{1} \quad = \quad \mathbf{x}^2 + 1 \quad = \quad \mathbf{x} + 1$$

Definition of !

- A multiset $\{0, 0, 1\}$ corresponds to a *term* $\mathbf{x}_0^2\mathbf{x}_1$ of the multinomial.
- The set of these terms form a basis.
  $f : [A] \to [B]$ acts on each $\mathbf{x}_a$ by:

$$\mathbf{x}_a \xmapsto{f} \sum_{b \in B} f[b, a] \cdot \mathbf{y}_b$$

Definition of !

- A multiset $\{0, 0, 1\}$ corresponds to a *term* $\mathbf{x}_0^2\mathbf{x}_1$ of the multinomial.
- The set of these terms form a basis.
  $f : [A] \to [B]$ acts on each $\mathbf{x}_a$ by:

$$\mathbf{x}_a \xmapsto{f} \sum_{b \in B} f[b, a] \cdot \mathbf{y}_b$$

So $!f$ acts on a term like $\mathbf{x}_0^2\mathbf{x}_1$ by:

$$\mathbf{x}_0^2\mathbf{x}_1 \xmapsto{!f} (\sum_{b \in B} f[b, 0] \cdot \mathbf{y}_b) \times (\sum_{b \in B} f[b, 0] \cdot \mathbf{y}_b) \times (\sum_{b \in B} f[b, 1] \cdot \mathbf{y}_b)$$

This is multinomial multiplication, modulo $\mathbf{y}^q = \mathbf{y}$.

Example in $\mathbb{F}_2$

Let $f : \llbracket 1 \oplus 1 \oplus 1 \rrbracket \longrightarrow \llbracket 1 \oplus 1 \oplus 1 \rrbracket$ be:

$$\begin{bmatrix} \bullet & \cdot & \bullet \\ \cdot & \bullet & \cdot \\ \cdot & \bullet & \cdot \end{bmatrix}$$

Then $!f :!\llbracket 1 \oplus 1 \oplus 1 \rrbracket \longrightarrow !\llbracket 1 \oplus 1 \oplus 1 \rrbracket$ is:

$$\begin{bmatrix} \bullet & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \bullet & \cdot & \cdot & \bullet & \cdot & \cdot & \cdot \\ \cdot & \cdot & \bullet & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot \\ \cdot & \cdot & \bullet & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \bullet & \cdot & \cdot & \bullet & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

Theorem (Functoriality of !)

For any $f : [\![A]\!] \rightarrow [\![B]\!]$ *and* $g : [\![B]\!] \rightarrow [\![C]\!]$*:*

$$!(f;g) = (!f);(!g) \quad : \; ![\![A]\!] \rightarrow ![\![C]\!]$$

Back to the Comonad: Coreturn

Let $M(a)$ be the multiplicity of a in the multiset M.

$$\mathrm{coreturn}_A : ![\![A]\!] \to [\![A]\!]$$

$$\mathrm{coreturn}_A[a, M] = M(a)$$

Example: $\mathrm{coreturn}_{\mathbb{B}} :![\![\mathbb{B}]\!] \to \mathbb{B}$ over $\mathbb{F}_2$

$$\begin{bmatrix} \cdot & \bullet & \cdot & \bullet \\ \cdot & \cdot & \bullet & \bullet \end{bmatrix}$$

More generally: The n^{th} column of the matrix is just n written in base q

Comultiply

$\mathrm{comultiply}_{\mathbb{B}} : ![\![\mathbb{B}]\!] \rightarrow !![\![\mathbb{B}]\!]$

$$\begin{bmatrix}
\bullet & \cdot & \cdot & \cdot \\
\bullet & \cdot & \cdot & \cdot \\
\cdot & \bullet & \cdot & \bullet \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \bullet & \bullet \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \bullet \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \bullet \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot
\end{bmatrix}$$

Dimensionality

$$
\begin{aligned}
\dim\,[0] &= 0 \\
\dim\,[\top] &= 0 \\
\dim\,[1] &= 1 \\
\dim\,[\bot] &= 1 \\
\dim\,[A \oplus B] &= \dim\,[A] + \dim\,[B] \\
\dim\,[A \,\&\, B] &= \dim\,[A] + \dim\,[B] \\
\dim\,[A \otimes B] &= \dim\,[A] \times \dim\,[B] \\
\dim\,[A \multimap B] &= \dim\,[A] \times \dim\,[B] \\
\dim\,[!A] &= ??
\end{aligned}
$$

Dimensionality

$$
\begin{aligned}
\dim[0] &= 0\\
\dim[\top] &= 0\\
\dim[1] &= 1\\
\dim[\bot] &= 1\\
\dim[A \oplus B] &= \dim[A] + \dim[B]\\
\dim[A \,\&\, B] &= \dim[A] + \dim[B]\\
\dim[A \otimes B] &= \dim[A] \times \dim[B]\\
\dim[A \multimap B] &= \dim[A] \times \dim[B]\\
\dim[!A] &= q^{\dim[A]}
\end{aligned}
$$

Conclusions

The category of finite dimensional vector spaces over finite fields is a model of linear logic.

- Very pretty mathematics!
- Connects lambda calculus and linear algebra!
- What are the implications of picking a particular $\mathbb{F}_q$?
- I'm working on an implementation...
- Applications?