About different kinds of Substitutions

Matthieu Deneufchâtel

Séminaire CALIN,
18 Janvier 2011

Outline

Commutative substitution I

- Let R be a commutative ring and $\mathfrak{A}$ be a R-associative algebra with unit. If $\mathbf{X} = (X_i)_{i \in I}$ is a set of indeterminates, $R[\mathbf{X}]$ denotes the algebra of polynomials with coefficients in R.
- Let $\mathbf{x} = (x_i)_{i \in I}$ be a set of pairwise commuting elements of $\mathfrak{A}$. Then there is only one morphism of AAU $\phi : R[\mathbf{X}] \to \mathfrak{A}$ such that $\phi(X_i) = x_i$. If $u \in R[\mathbf{X}]$, we note $\phi(u) = u(\mathbf{x}) = u((x_i)_{i \in I})$.
- If $\lambda : \mathfrak{A} \to \mathfrak{A}'$ is a morphism of R-associative algebras with unit, one has

$$\lambda(u(\mathbf{x})) = u((\lambda(x_i))_{i \in I}) \tag{1}$$

for $\lambda \circ \phi : R[\mathbf{X}] \to \mathfrak{A}'$ is such that $X_i \mapsto \lambda(x_i)$.

Commutative substitution II

- Let $\mathbf{Y} = (Y_j)_{j\in J}$ be another set of indeterminates and take $\mathfrak{A} = R[\mathbf{Y}]$. If $u \in R[\mathbf{X}]$ and $(g_i)_{i\in I} \in R[\mathbf{Y}]^I$, let $u(\mathbf{g}) \in R[\mathbf{Y}]$ be the polynomial obtained by substitution of the g_i's in u.
- Let $\mathbf{y} = (y_j)_{j\in J}$ be a set of pairwise commuting elements of $\mathfrak{A}'$. Applying (1) with

$$\lambda : \begin{array}{rl} \mathfrak{A} = R[\mathbf{Y}] & \rightarrow \mathfrak{A}' \\ g_i & \mapsto g_i(\mathbf{y}) \end{array}$$

yields

$$(u(\mathbf{g}))(\mathbf{y}) = u((g_i(\mathbf{y}))_{i\in I}). \tag{2}$$

- Now if $\mathbf{f} = (f_i)_{i\in I} \in (R[(X_j)_{j\in J}])^I$ and $\mathbf{g} = (g_j)_{j\in J} \in (R[(Y_k)_{k\in K}])^J$ we denote by $f \circ g$ the family of polynomials

$$(f_i(\mathbf{g}))_{i\in I} \in (R[(Y_k)_{k\in K}])^I.$$

- Eq. (2) implies that $\circ$ is associative.

Lagrange inversion formula

Let f be an analytic complex function such that $f(0) = 0$ and $f'(0) \neq 0$. Then there exists an analytic function g such that $g(f(z)) = z$. If the Taylor series of f near 0 is

$$f(z) = f_1 z + f_2 z^2 + \dots,$$

the coefficients of (the Taylor expansion of) g (near 0) are given by

$$g_n = \frac{1}{n!} \left[\left(\frac{d}{dz}\right)^{n-1} \left(\frac{z}{f(z)}\right)^n \right] \Bigg|_{z=0} .$$

More generally, if $f(w) = z$ is analytic at the point a with $f'(a) \neq 0$, and if $w = g(z)$ with g analytic at the point $b = f(a)$, one has

$$g(z) = a + \sum_{n=1}^{\infty} \lim_{w \to a} \left(\left(\frac{d}{dw}\right)^{n-1} \left(\frac{w-a}{f(w)-b}\right)^n \right) \frac{(z-b)^n}{n!}.$$

Substitutions and Hopf algebra 1/4

$$G_{\text{uni}}^{\text{dif}} = \left\{ \phi(x) = x + \sum_{k=1}^{\infty} \phi_n x^{n+1}, \phi_n \in \mathbb{C} \right\}$$

- Formal diffeomorphisms (tangent to the unity)
- Structure of (non-abelian) group for the composition law

$$\phi(\psi(x)) = \psi(x) + \sum_{n \geq 1} \phi_n (\psi(x))^{n+1}$$

- $\text{Id}(x) = x$
- Inverse of a series can be found by the Lagrange inversion formula.

Substitutions and Hopf algebra 1/4

$$G_{\text{uni}}^{\text{dif}} = \left\{ \phi(x) = x + \sum_{k=1}^{\infty} \phi_n x^{n+1}, \phi_n \in \mathbb{C} \right\}$$

- Formal diffeomorphisms (tangent to the unity)
- Structure of (non-abelian) group for the composition law

$$\phi(\psi(x)) = \psi(x) + \sum_{n \geq 1} \phi_n (\psi(x))^{n+1}$$

- $\text{Id}(x) = x$
- Inverse of a series can be found by the Lagrange inversion formula.

$\mathbb{C}(G_{\text{uni}}^{\text{dif}})$: functions $G_{\text{uni}}^{\text{dif}} \rightarrow \mathbb{C}$ which are in the algebra generated by some basic elements (i.e. are "polynomial" *w.r.t.* these elements). For example, one can choose the functions

$$a_n : \phi \mapsto \frac{1}{(n+1)!} \frac{d^{n+1}\phi(0)}{dx^{n+1}} = \phi_n, \ n \geq 1.$$

Substitutions and Hopf algebra 2/4

The group structure of $G_{\text{uni}}^{\text{dif}}$ induces a Hopf algebra structure on $\mathbb{C}(G_{\text{uni}}^{\text{dif}})$:

- product : $\langle \mu(a_n \otimes a_m) | \phi \circ \psi \rangle = a_n(\phi) a_m(\psi)$;
- coproduct : $\langle \Delta^{\text{dif}} a_n | \phi \otimes \psi \rangle = a_n(\phi \circ \psi)$;

Let $A(x) = \sum_{k=0}^{\infty} a_k x^{k+1}$ be the generating series of the a_k's ($a_0 = 1$).

Then one has

$$\Delta^{\text{dif}} A(x) = \sum_{n=0}^{\infty} \Delta^{\text{dif}} a_n \, x^n = \langle z^{-1} \rangle A(z) \otimes \frac{1}{z - A(x)}$$

where

$$\langle z^{-1} \rangle f$$

denotes the coefficient of z^{-1} in f.

Substitutions and Hopf algebra 3/4

Proof

Note first that

$$\langle A(x)|\phi\rangle = \sum_{n=0}^{\infty}\langle a_n|\phi\rangle x^{n+1} = \phi(x) \text{ and } \langle A^m(x)|\phi\rangle = \phi^m(x).$$

Substitutions and Hopf algebra 3/4

Proof

Note first that

$$\langle A(x)|\phi\rangle = \sum_{n=0}^{\infty}\langle a_n|\phi\rangle x^{n+1} = \phi(x) \text{ and } \langle A^m(x)|\phi\rangle = \phi^m(x).$$

Then

$$\begin{aligned}\langle\Delta^{\mathrm{Dif}}A(x)|\phi\otimes\psi\rangle &= \sum_{n=0}^{\infty}\langle\Delta^{\mathrm{Dif}}a_n|\phi\otimes\psi\rangle = \sum_{n=0}^{\infty} a_n(\phi\circ\psi)x^{n+1} \\ &= \langle z^{-1}\rangle\frac{\phi(z)}{z-\psi(x)} = \langle z^{-1}\rangle\left(\langle A(z)|\phi\rangle\langle\frac{1}{z-A(x)}|\psi\rangle\right)\end{aligned}$$

Substitutions and Hopf algebra 3/4

Proof

Note first that

$$\langle A(x)|\phi\rangle = \sum_{n=0}^{\infty}\langle a_n|\phi\rangle x^{n+1} = \phi(x) \text{ and } \langle A^m(x)|\phi\rangle = \phi^m(x).$$

Then

$$\begin{aligned}\langle \Delta^{\mathrm{Dif}} A(x)|\phi\otimes\psi\rangle &= \sum_{n=0}^{\infty}\langle \Delta^{\mathrm{Dif}} a_n|\phi\otimes\psi\rangle = \sum_{n=0}^{\infty} a_n(\phi\circ\psi)x^{n+1}\\ &= \langle z^{-1}\rangle\frac{\phi(z)}{z-\psi(x)} = \langle z^{-1}\rangle\left(\langle A(z)|\phi\rangle\langle\frac{1}{z-A(x)}|\psi\rangle\right)\\ &= \langle z^{-1}\rangle\langle A(z)\otimes\frac{1}{z-A(x)}|\phi\otimes\psi\rangle,\end{aligned}$$

$$\text{with } \frac{1}{z-A(x)} = \sum_{n=0}^{\infty} A(x)^n z^{-n-1}.$$

Substitutions and Hopf algebra 4/4

Link with the *Faà di Bruno bi-algebra*

$\mathbb{C}(G_{\text{uni}}^{\text{dif}})$ is the co-ordinate ring ([Brouder, Fabretti, Krattenthaler]) of the group $G_{\text{uni}}^{\text{dif}}$. The Faà di Bruno bi-algebra is the co-ordinate ring of the semigroup

$$\left\{ \phi(x) = \sum_{n=1}^{\infty} \phi_n \frac{x^n}{n!},\ \phi_n \in \mathbb{C} \right\}$$

with ϕ_1 not necessarily equal to 1.

Substitutions and Hopf algebra 4/4

Link with the *Faà di Bruno bi-algebra*

$\mathbb{C}(G_{\text{uni}}^{\text{dif}})$ is the co-ordinate ring ([Brouder, Fabretti, Krattenthaler]) of the group $G_{\text{uni}}^{\text{dif}}$. The Faà di Bruno bi-algebra is the co-ordinate ring of the semigroup

$$\left\{\phi(x) = \sum_{n=1}^{\infty} \phi_n \frac{x^n}{n!},\ \phi_n \in \mathbb{C}\right\}$$

with ϕ_1 not necessarily equal to 1.
Using the procedure described for $\mathbb{C}(G_{\text{uni}}^{\text{dif}})$, one identifies the Faà di Bruno bi-algebra with $\mathbb{C}\left[u_1, u_2, \ldots\right]$, $\deg(u_n) = n-1$, with coproduct

$$\Delta u_n = \sum_{k=1}^{n} u_k \otimes \sum_{\substack{\alpha \vdash k \\ \sum_{i=1}^{n} i\alpha_i = n}} \frac{n!}{\alpha_1! \ldots \alpha_n!} \frac{u_1^{\alpha_1} \ldots u_n^{\alpha_n}}{1!^{\alpha_1} \ldots n!^{\alpha_n}}$$

and counit $\epsilon(u_n) = \delta_{n,0}$.

Series with coefficient in the Boolean semiring

Let $\mathfrak{B} = \{0, 1\}$ be the Boolean semiring and let L be a language over the alphabet A.

Characteristic series of the language L : the sum $\underline{L} = \sum_{w \in L} w (\in \mathfrak{B}\langle\langle A \rangle\rangle)$.

If S is a series with coefficients $\alpha_w \in \mathfrak{B}$, S is the characteristic series of the language $\mathfrak{L} = \mathtt{Supp}(\alpha)$.

Series with coefficient in the Boolean semiring

Let $\mathfrak{B} = \{0, 1\}$ be the Boolean semiring and let L be a language over the alphabet A.

Characteristic series of the language L : the sum $\underline{L} = \sum_{w \in L} w (\in \mathfrak{B}\langle\langle A \rangle\rangle)$.

If S is a series with coefficients $\alpha_w \in \mathfrak{B}$, S is the characteristic series of the language $\mathfrak{L} = \mathtt{Supp}(\alpha)$.

The usual operations on languages are represented on their characteristic series as follows :

- $\underline{L \cup M} = \underline{L} + \underline{M}$;
- $\underline{L \cap M} = \underline{L} \odot \underline{M}$ where $\odot$ denotes the Hadamard product of series;
- $\underline{L \cdot M} = \underline{L} \cdot \underline{M}$ where in the point in the *lhs* denotes the concatenation and in the *rhs* the Cauchy (or concatenation) product of two series.

Let A and B be two languages and $f : A \to \mathfrak{P}(B^*)$. f is called a substitution.
f can be extended as a morphism of monoids from (A^*, conc) to $(\mathfrak{P}(B^*), \text{conc})$ and then as a sum-preserving application from $\mathfrak{P}(A^*)$ to $\mathfrak{P}(B^*)$ denoted by $\overline{f}$:

$$\forall (L_i)_{i\in I} \in \mathfrak{P}(A^*),\ f(\sum_{i\in I} L_i) = \sum_{i\in I} f(L_i)$$

These substitutions are composable : if $f : A \to \mathfrak{P}(B^*)$ and $g : B \to \mathfrak{P}(C^*)$, one defines $g \circ f : A \to \mathfrak{P}(C^*)$ as the composition

$$\overline{g} \circ f : A \to \mathfrak{P}(B^*) \to \mathfrak{P}(C^*).$$

Let A be a finite alphabet and R a commutative ring with a unit.

Substitution

A substitution is a morphism of algebras from $R\langle\langle A\rangle\rangle$ to $R\langle\langle A\rangle\rangle$ such that $\phi(A) \subseteq R_{\geq 1}\langle\langle A\rangle\rangle$.

- Let $\phi : A \to R_{\geq 1}\langle\langle A\rangle\rangle$ be a substitution.
- We extend ϕ as a morphism of monoids from $(A^*, \bullet)$ to $(R_{\geq 1}\langle\langle A\rangle\rangle, \times)$ where $\times$ denotes the Cauchy product : if $w = a_1 \cdots a_n$,

$$\phi(w) = \phi(a_1) \times \cdots \times \phi(a_n).$$

- Since A^* is a basis of $R\langle A\rangle$, we can extend ϕ as an application from $R\langle A\rangle$ to $R_{\geq 1}\langle\langle A\rangle\rangle$ by linearity :

$$\phi(S) = \phi(\sum_{w\in A^*} \langle S|w\rangle w) = \sum_{w\in A^*} \langle S|w\rangle \phi(w).$$

Question : Does the last relation hold for $S \in R\langle\langle A\rangle\rangle$?

The family $(\langle S|w\rangle\phi(w))_{w\in A^*}$ is summable. Indeed, $\forall v \in A^*$, the support of $(\langle S|w\rangle\langle\phi(w)|v\rangle)_{w\in A^*}$ is finite :

- $\phi(a) \in R_{\geq 1}\langle\langle A\rangle\rangle$. Hence, $\forall w \in A^*$,

$$\phi(w) \in R_{\geq |w|}\langle\langle A\rangle\rangle.$$

- Therefore, $\mathrm{Supp}\left((\langle S|w\rangle\langle\phi(w)|v\rangle)_{w\in A^*}\right) \subseteq A^{\leq |v|}$ which is finite in the case of a finite alphabet.

Substitution

If $S \in R\langle\langle A\rangle\rangle$,

$$\phi(S) = \sum_{w\in A^*} \langle S|w\rangle\phi(w) = \sum_{v\in A^*}\left(\sum_{w\in A^*} \langle S|w\rangle\langle\phi(w)|v\rangle\right) v.$$

Infinite alphabet

- Let Y be an infinite alphabet (common in Physics and Geometry). **Example :** we define $\phi : Y \to R_{\geq 1}\langle\langle Y\rangle\rangle$ by $\phi(y_i) = y_1$, $\forall i \in \mathbb{N}$.
- We extend ϕ to Y^* as a morphism of monoids.
- We extend ϕ by linearity to $R\langle Y\rangle$.
- Is it possible to extend it to $R\langle\langle Y\rangle\rangle$?

One has to be able to substitute the characteristic series of Y, namely $\sum_{y\in Y} y$. Hence, $(\phi(y))_{y\in Y}$ has to be summable.

Exercise

$$\phi \text{ is a substitution} \Leftrightarrow \forall w \in Y^*, \left|\mathrm{Supp}\begin{pmatrix} Y \to R \\ y \mapsto \langle \phi(y) | w\rangle \end{pmatrix}\right| < \infty$$

Statistics on graphs

Let $\mathfrak{C}$ be a class of graphs stable under taking connected components ($\forall \Gamma \in \mathfrak{C}, \forall \Gamma_i$ connected component of $\Gamma, \Gamma_i \in \mathfrak{C}$). An integer-valued statistics c is a map $\mathfrak{C} \to \mathbb{N}^d$.

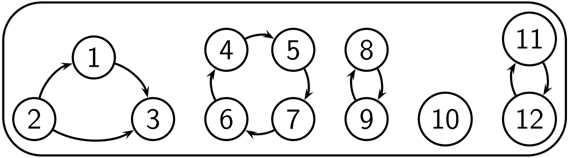
Very often, one represents this statistics by $c(\Gamma) = L_1^{c(\Gamma)_1} \dots L_d^{c(\Gamma)_d}$.

- $c^1(\Gamma) = x^n y^k$;
- $c^2(\Gamma) = x^k L_1^{\alpha_1} \dots L_n^{\alpha_n}$.

- $n =$ number of vertices,
- $k =$ number of connected components,
- $\alpha_i =$ number of i-blocks.

Example :

If $\Gamma =$



$c^2(\Gamma) = y^5 L_1 L_2^2 L_3 L_4$.

Exponential formula

How to memorize it ?

$$\mathrm{EGF}(ALL) = \exp\left(\mathrm{EGF}(CONNECTED)\right).$$

More formally, if:

- $\mathfrak{C}$ is a class of graphs stable under relabelling and taking connected components,
- $\mathfrak{C}_{[1..n]}$ denotes the class obtained by renaming the vertices with integers from 1 to n,
- $\mathfrak{C}^c_{[1..n]}$ the connected graphs of $\mathfrak{C}_{[1..n]}$,

$$\sum_{n\geq 0} c\left(\mathfrak{C}_{[1..n]}\right)\frac{z^n}{n!} = \exp\left(\sum_{n\geq 1} c\left(\mathfrak{C}^c_{[1..n]}\right)\frac{z^n}{n!}\right),$$

where $c(\mathfrak{C}) = \sum_{\Gamma\in\mathfrak{C}} c(\Gamma)$.

Substitution of formal power series

Let $f = \sum_{i \geq 1} f_i \frac{z^i}{i!}$ (zero constant term), and $g = \sum_{j \geq 0} g_j \frac{z^j}{j!}$.

$g \circ f = \sum_{j \geq 0} g_j \frac{f^j}{j!}$. Is there a simple expression of f^j in terms of the f_j's?

$$\mathrm{EGF}(f^j) = \sum_{k \geq 0} f^k \frac{y^k}{k!} = \exp\left(y \sum_{i \geq 1} f_i \frac{z^i}{i!} \right) \tag{3}$$

Ideally, we would like something like

$$f^j = \sum_{m \geq 0} P_k(f_1, \ldots, f_*) \frac{z^m}{m!}.$$

for some polynomials P_k.

Substitution of formal power series

Let $f = \sum_{i \geq 1} f_i \frac{z^i}{i!}$ (zero constant term), and $g = \sum_{j \geq 0} g_j \frac{z^j}{j!}$.

$g \circ f = \sum_{j \geq 0} g_j \frac{f^j}{j!}$. Is there a simple expression of f^j in terms of the f_j's?

$$\mathrm{EGF}(f^j) = \sum_{k \geq 0} f^k \frac{y^k}{k!} = \exp\left(y \sum_{i \geq 1} f_i \frac{z^i}{i!} \right) \tag{3}$$

Ideally, we would like something like

$$f^j = \sum_{m \geq 0} P_k(f_1, \ldots, f_*) \frac{z^m}{m!}.$$

for some polynomials P_k.

Idea : Find a class of "good" class of graphs with the statistics c^2 and use the exponential formula.

Equivalence relation graphs I

Interesting properties :

- Their connected components are complete;
- There is only one connected graph with n vertices.

$\mathfrak{C}_{eq}$ = class of equivalence relation graphs.

$$\text{Therefore, } \sum_{n\geq 1} c(\mathfrak{C}^c_{\mathrm{eq},[1..n]})\frac{z^n}{n!} = y\sum_{n\geq 1} L_n\frac{z^n}{n!}.$$

But

$$\sum_{n\geq 0}\frac{z^n}{n!}\sum_{\Gamma\in\mathfrak{C}_{\mathrm{eq},[1..n]}} c(\Gamma) = \sum_{n\geq 0}\frac{z^n}{n!}\sum_{k=0}^{n} y^k \sum_{\substack{\|\alpha\|=n\\ |\alpha|=k}} \mathrm{numpart}(\alpha)\mathbb{L}^\alpha$$

with $|\alpha| = \sum_{i=1}\alpha_i$ and $\|\alpha\| = \sum_i i\alpha_i$.

Equivalence relation graphs II

$$\sum_{\substack{\|\alpha\|=n\\|\alpha|=k}} \mathrm{numpart}(\alpha)\mathbb{L}^{\alpha} = B_{n,k}(L_1,\ldots,L_{n-k+1}),$$

One has,

$$\exp(yf) = 1 + \sum_{n=1}^{\infty}\sum_{k=1}^{n} B_{n,k}(f_1,\ldots,f_{n-k+1})\frac{y^k z^n}{n!}.$$

Therefore

$$f^j = \sum_{n\geq j} B_{n,j}(f_1,\ldots,f_{n-j+1})\frac{z^n}{n!}.$$

Cf. Faà di Bruno's formula :

$$\frac{d^n}{dx^n}g(f(x)) = \sum_{k=0}^{\infty} h_n\frac{z^n}{n!} \text{ with } h_n = \sum_{k=1}^{n} g_k B_{n,k}(f_1,\ldots,f_{n-k+1})$$