Genética de polinomios sobre cuerpos locales

Hayden Stainsby

Universitat Autònoma de Barcelona

STNB 30 de enero de 2014

Resumen

Tipos sobre (K, v)

(K, v) cuerpo valorado discreto, $\mathcal{O}$ anillo de valoración, $\mathfrak{m} = \pi\mathcal{O}$ ideal maximal, $\mathbb{F}_0 := \mathbb{F} = \mathcal{O}/\mathfrak{m}$ cuerpo residual

Un **tipo** sobre (K, v) es un objeto computacional capaz de representar un punto del espacio de MacLane $(\mu, \mathcal{L}) \in \mathbb{M}$

Más precisamente, un tipo es una colección de datos discretos:

$$\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r))$$

que determinan una cadena de MacLane óptima de una valoración inductiva μ de $K(x)$ y un ideal maximal $\mathcal{L}$ del anillo $\Delta(\mu)$

Vemos que los datos de $\mathbf{t}$ están estructurados en **niveles**. El número r de niveles es el **orden** del tipo

Datos de un tipo de orden cero

Un tipo de orden cero $\mathbf{t} = (\psi_0)$ está determinado por la elección de un polinomio mónico irreducible $\psi_0 \in \mathbb{F}[y]$

Contiene los siguientes datos de nivel cero:

- La valoración mínima μ_0 de $K(x)$ y su normalización $v_0 = \mu_0$
- Datos numéricos: $m_0 = 1$, $\lambda_0 = \nu_0 = 0$, $h_0 = 0$, $e_0 = 1$
- El operador **polinomio residual** 0-ésimo:

$$R_0 \colon K[x] \to \mathbb{F}_0[y], \quad g \mapsto \overline{g(y)/\pi^{v_0(g)}}$$

- $\psi_0 \in \mathbb{F}_0[y]$ mónico irreducible, de grado f_0
  $\mathbb{F}_1 = \mathbb{F}_0[y]/(\psi_0) = \mathbb{F}_0[z_0]$ extensión de $\mathbb{F}_0$ de grado f_0
  $z_0 = y \pmod{\psi_0} \in \mathbb{F}_1$

Datos de un tipo de orden positivo

Dado un tipo $\mathbf{t}' = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_{r-1}, \lambda_{r-1}, \psi_{r-1}))$ de orden $r-1 \geq 0$, podemos fabricar un tipo $\mathbf{t} = (\mathbf{t}'; (\phi_r, \lambda_r, \psi_r))$ de orden r añadiendo los siguientes datos en el nivel r-ésimo:

- Un **representante** ϕ_r de $\mathbf{t}'$. Es decir, $\phi_r \in \mathcal{O}[x]$ mónico tal, que $m_r := \deg \phi_r = e_{r-1} f_{r-1} m_{r-1}, \quad R_{r-1}(\phi_r) = \psi_{r-1}$
- El operador **polígono de Newton** $N_r = N_{v_{r-1}, \phi_r}$
- Una **pendiente** $\lambda_r = h_r/e_r$, con h_r, e_r enteros positivos coprimos

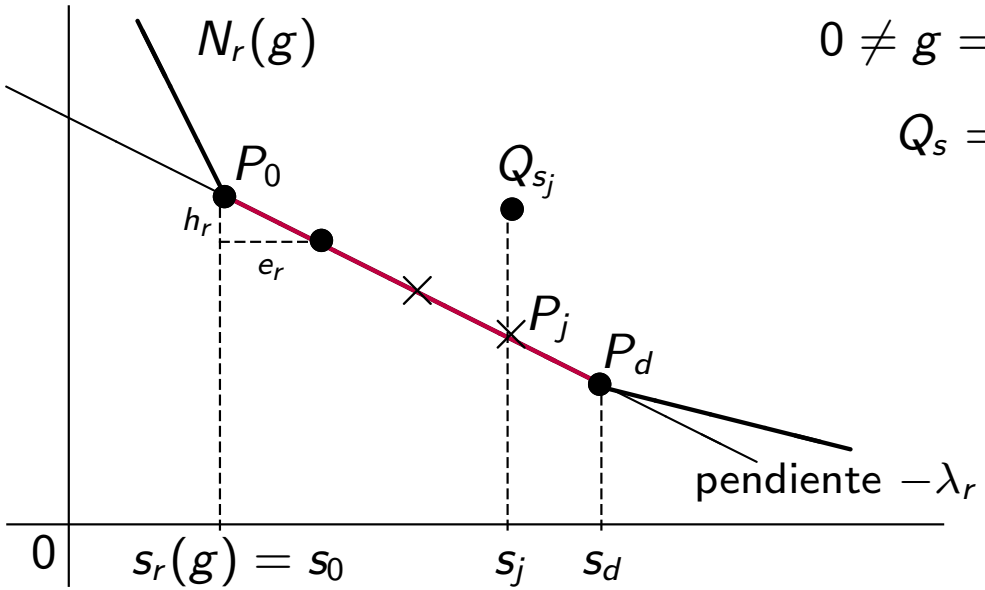
  La pendiente no-normalizada $\nu_r = h_r / e_1 \cdots e_r$
- $\mu_r = [\mu_{r-1}; (\phi_r, \nu_r)]$ y su normalización $v_r = e_1 \cdots e_r \, \mu_r$
- El operador **polinomio residual** r-ésimo

  $R_r := R_{v_{r-1}, \phi_r, \lambda_r} : K[x] \to \mathbb{F}_r[y]$
- $\psi_r \in \mathbb{F}_r[y]$ mónico irreducible, $\psi_r \neq y$, $f_r := \deg \psi_r$

  $\mathbb{F}_{r+1} = \mathbb{F}_r[y]/(\psi_r) = \mathbb{F}_r[z_r]$ extensión de $\mathbb{F}_0$ de grado $f_0 \cdots f_r$

  $z_r = y \pmod{\psi_r} \in \mathbb{F}_{r+1}$

Operador polinomio residual r-ésimo para $r > 0$



$$0 \neq g = \textstyle\sum_{0 \leq s} a_s \phi_r^s \in K[x]$$

$$Q_s = (s, v_{r-1}(a_s \phi_r^s))$$

$$c_j := \begin{cases} 0, & \text{si } Q_{s_j} \text{ por encima de } P_j, \\ z_{r-1}^{t_{r-1}(a_{s_j})} R_{r-1}(a_{s_j})(z_{r-1}) \in \mathbb{F}_r^*, & \text{si } Q_{s_j} = P_j \end{cases}$$

Para $a \in K[x]$: $t_0(a) = 0$, $t_k(a) = (s_k(a) - \ell_k v_k(a))/e_k$ si $k > 0$

$$R_r(g) := c_0 + c_1 y + \cdots + c_d y^d \in \mathbb{F}_r[y]$$

$$c_0 c_d \neq 0 \implies \deg R_r(g) = d, \quad y \nmid R_r(g)$$

Tipos y valoraciones inductivas

Para $\mathbf{t}$ tipo de orden r denotamos $\mu = \mu_{\mathbf{t}} = \mu_r$

(1) $\mu_{\mathbf{t}}$ es una valoración inductiva con cadena de MacLane

$$\mu_0 \xrightarrow{(\phi_1,\nu_1)} \mu_1 \xrightarrow{(\phi_2,\nu_2)} \cdots \longrightarrow \mu_{r-1} \xrightarrow{(\phi_r,\nu_r)} \mu_r = \mu_{\mathbf{t}}$$

(2) Diagrama conmutativo con isomorfismos verticales:

$$\begin{array}{ccccccc} \mathbb{F} = \mathbb{F}_0 & \subset & \mathbb{F}_1 & \subset & \cdots & \subset & \mathbb{F}_r \\ \| & & \downarrow \iota_1 & & \cdots & & \downarrow \iota_r \\ \mathbb{F} = \mathbb{F}_{0,\mu} & \subset & \mathbb{F}_{1,\mu} & \subset & \cdots & \subset & \mathbb{F}_{r,\mu} \end{array}$$

tales que $R_{i,\mu} = \iota_i[y] \circ R_i$ para todo i. Podemos pues identificar:
$\mathbb{F}_i = \mathbb{F}_{i,\mu}, \quad z_{i-1} = z_{i-1,\mu}, \quad \psi_{i-1} = \psi_{i-1,\mu}, \quad R_i = R_{i,\mu}$

Tipos y valoraciones inductivas

Así pues, un tipo $\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r))$ determina:

(1) Una cadena de MacLane de una valoración inductiva $\mu_{\mathbf{t}}$, que se corresponde con los datos: $(\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, -))$

(2) Un ideal maximal $\mathcal{L}_{\mathbf{t}} = \psi_r(y_r)\Delta(\mu_{\mathbf{t}})$ del anillo $\Delta(\mu_{\mathbf{t}})$, que se corresponde con los datos: ψ_r, $\mathbb{F}_{r+1}$, z_r

Lema

$\phi \in K[x]$ representante de $\mathbf{t} \iff \phi \in \mathrm{KP}(\mu_{\mathbf{t}}), \quad \mathcal{R}(\phi) = \mathcal{L}_{\mathbf{t}}$

Tipos y puntos del espacio de MacLane

Definición

t es óptimo si $m_1 < \cdots < m_r$
t es fuertemente óptimo si además $e_r f_r > 1$
Convenimos que los tipos de orden $r = 0$ son fuertemente óptimos

Estas condiciones se traducen en que la cadena de MacLane de $\mu_{\mathbf{t}}$ sea óptima y en que además el ideal maximal $\mathcal{L}_{\mathbf{t}}$ sea fuerte

Si denotamos por $\mathcal{T}$ el conjunto de los tipos sobre (K, v) y por $\mathcal{T}^{\text{str}} \subset \mathcal{T}$ el subconjunto de los tipos fuertemente óptimos, obtenemos una **aplicación de MacLane**:

$$\text{ml}\colon \mathcal{T}^{\text{str}} \longrightarrow \mathbb{M}, \qquad \mathbf{t} \mapsto (\mu_{\mathbf{t}}, \mathcal{L}_{\mathbf{t}})$$

Es fácil ver que esta aplicación es exhaustiva. Estudiemos sus fibras.

Equivalencia de tipos

Definición

Consideremos dos tipos fuertemente óptimos de orden r:
$\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r))$
$\mathbf{t}' = (\psi_0'; (\phi_1', \lambda_1', \psi_1'); \ldots; (\phi_r', \lambda_r', \psi_r'))$
Decimos que $\mathbf{t} \equiv \mathbf{t}'$ son equivalentes si $\psi_0' = \psi_0$ y para $1 \leq i \leq r$:

(a) $\phi_i' = \phi_i + a_i, \ \deg a_i < m_i, \ \mu_i(a_i) \geq \mu_i(\phi_i)$

(b) $\lambda_i' = \lambda_i$

(c) $\psi_i'(y) = \psi_i(y - \eta_i)$, donde

$$\eta_i = \begin{cases} 0, & \text{si } \mu_i(a_i) > \mu_i(\phi_i) \quad (\text{i.e. } \phi_i' \sim_{\mu_i} \phi_i) \\ R_i(a_i) \in \mathbb{F}_i^*, & \text{si } \mu_i(a_i) = \mu_i(\phi_i) \quad (\text{i.e. } \phi_i' \not\sim_{\mu_i} \phi_i) \end{cases}$$

Proposición

$\mathbf{t} \equiv \mathbf{t}' \iff \mathrm{ml}(\mathbf{t}) = \mathrm{ml}(\mathbf{t}')$

Tipos y polinomios primos

Denotamos por $\mathbb{T} = \mathcal{T}^{\mathsf{str}}/\equiv$ el conjunto cociente y por $[\mathbf{t}] \subset \mathcal{T}^{\mathsf{str}}$ la clase de equivalencia de $\mathbf{t}$

Obtenemos aplicaciones biyectivas

$$\mathbb{T} \xrightarrow{\mathsf{ml}} \mathbb{M} \xrightarrow{\mathsf{ok}} (\mathbb{P}/\approx)$$

La composición assigna a cada $\mathbf{t} \in \mathcal{T}^{\mathsf{str}}$ la clase de equivalencia de Okutsu $[\phi]$ de qualquier representante ϕ de $\mathbf{t}$.

Además, $[\phi] \cap \mathcal{O}[x]$ coincide con el conjunto $\mathrm{Rep}(\mathbf{t})$ de todos los representantes de $\mathbf{t}$

Construcción de tipos

Proposición

Sea $\mathbf{t}$ un tipo de orden $r \geq 1$ y consideremos

$$m_{r+1} := e_r f_r m_r, \quad V_r = v_{r-1}(\phi_r), \quad V_{r+1} := e_r f_r (e_r V_r + h_r)$$

Dados $0 \neq \varphi \in \mathbb{F}_r[y]$ con $\deg \varphi < f_r$, y un entero $b \geq V_{r+1}$, podemos construir un polinomio $g \in \mathcal{O}[x]$ tal, que

$$\deg g < m_{r+1}, \quad v_r(g) = b, \quad y^{\lfloor s_r(g)/e_r \rfloor} R_r(g) = \varphi$$

Si tomamos $\varphi = \psi_r - y^{f_r}$, $b = V_{r+1}$, el polinomio g así construido nos proporciona un representante de $\mathbf{t}$: $\phi = \phi_r^{e_r f_r} + g$

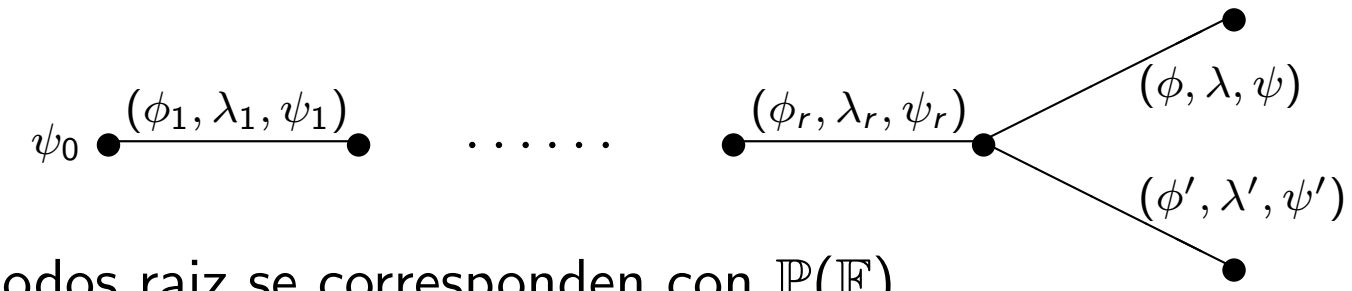
Como λ_{r+1}, ψ_{r+1} pueden ser escogidos libremente, podemos construir tipos con invariantes h_i, e_i, f_i y orden r prescritos. Podemos construir polinomios primos con profudidad e invariantes de MacLane-Okutsu prescritos, dando lugar a extensiones de cuerpos locales con propiedades aritméticas prescritas.

Estructura de árbol en el conjunto de tipos

Podemos representar un tipo como un árbol no ramificado.

Cada nodo se corresponde con el tipo obtenido recogiendo los datos de las aristas del camino que une el nodo con el nodo inicial

Podemos dotar el conjunto $\mathcal{T}$ de una estructura de árbol



Los nodos raiz se corresponden con $\mathbb{P}(\mathbb{F})$

Induce estructuras naturales de árbol en el subconjunto $\mathcal{T}^{\text{str}}$ y en el cociente $\mathbb{T} = \mathcal{T}^{\text{str}} / \equiv$
La aplicación $\mathcal{T}^{\text{str}} \longrightarrow \mathbb{T}$ conserva la longitud de los caminos

Representaciones OM de polinomios primos

Definición

Una **representación OM** de $F \in \mathbb{P}$ es un par $[\mathbf{t}_F, \phi]$, donde

- $\mathbf{t}_F \in \mathcal{T}^{\mathrm{str}}$ y la biyección canónica $\mathbb{T} \to \mathbb{P}/\approx$ envia $[\mathbf{t}_F] \mapsto [F]$
- ϕ es un representante de $\mathbf{t}_F$

Los datos discretos de $\mathbf{t}_F$ son una especie de secuencia de ADN compartida por todos los individuos en la clase $[F]$

$\phi \in [F] \cap \mathcal{O}[x]$ es una "buena" aproximación de F. La **calidad** de la aproximación se mide por el número racional positivo

$$v(\phi(\theta)) = \delta_0(F) + \lambda/e(F), \qquad \lambda \in \mathbb{Z}_{>0}$$

donde $F(\theta) = 0$ y $-\lambda =$ mínima pendiente de $N^-_{r+1}(F) := N^-_{v_r,\phi}(F)$

En la práctica, identificamos la representación OM con el tipo $(\mathbf{t}_F; (\phi, \lambda, \psi))$, donde $\psi = R_{r+1}(F) := R_{v_r,\phi,\lambda}(F)$

Factorizaciones OM

Definición

Sea $g \in \mathcal{O}[x]$ mónico con factores primos $g = G_1 \cdots G_s$ en $\mathcal{O}_v[x]$
Una **factorización de Okutsu** de g es una expresión $g \approx P_1 \cdots P_s$, con $P_1, \ldots, P_s \in \mathbb{P} \cap \mathcal{O}[x]$ tales que $P_j \approx G_j$ para todo $1 \leq j \leq s$, a menos de la ordenación de los factores

Si los G_j son todos equivalentes a P, entonces $g \approx P^s$ es una factorización de Okutsu que no distingue los factores de g

Definición

$P_j \in [G_j]$ es una aproximación de Montes a G_j como factor de g si

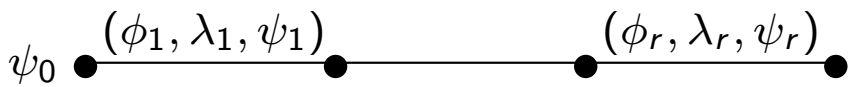
$$v(P_j(\theta_j)) > v(P_j(\theta_k)), \quad \forall\, k \neq j \qquad (G_k(\theta_k) = 0,\ \forall k)$$

Una **factorización OM** de g es una factorización de Okutsu $g \approx P_1 \cdots P_s$ tal que cada P_j es una aproximación de Montes a G_j como factor de g

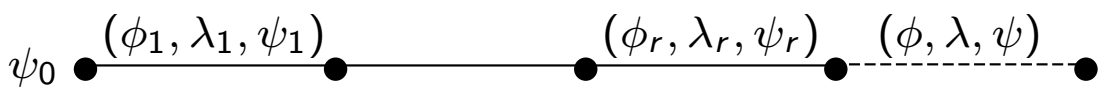
Árbol genómico de un polinomio primo

Dado $F \in \mathbb{P}$, consideremos $\mathbf{t}_F \in \mathcal{T}^{\mathrm{str}}$ tal, que la aplicación biyectiva $\mathbb{T} \to \mathbb{P}/\approx$ envia $[\mathbf{t}_F] \mapsto [F]$

El **árbol genómico** de F es el subárbol $\mathbb{T}(F) \subset \mathbb{T}$ formado por el camino que une $[\mathbf{t}_F]$ con su nodo-raiz.



Una representación OM de F, dada por un tipo $\mathbf{t} = (\mathbf{t}_F; (\phi, \lambda, \psi))$, se representa mediante un árbol



La arista punteada nos recuerda que el tipo $\mathbf{t}$ no es (jamás) fuertemente óptimo, con lo que no da lugar a un elemento de $\mathbb{T}$

Representación OM de un polinomio libre de cuadrados

Sea $f \in \mathcal{O}[x]$ un polinomio libre de cuadrados con factores primos $f = F_1 \cdots F_t$ en $\mathcal{O}_v[x]$

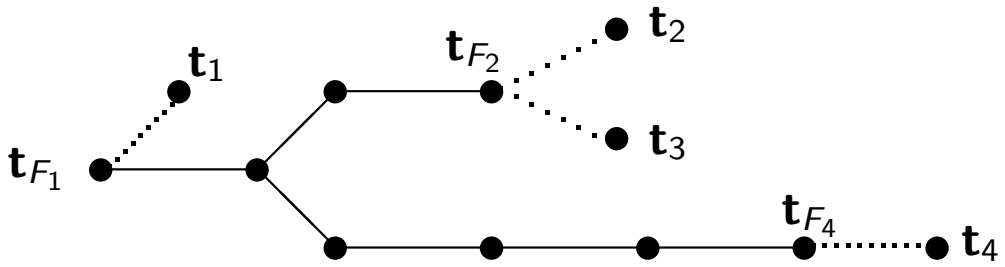
El **árbol genómico** de f es $\mathbb{T}(f) = \mathbb{T}(F_1) \cup \cdots \cup \mathbb{T}(F_t)$

Definición

Una **representación OM** de f es una familia $[\mathbf{t}_{F_j}, \phi_{F_j}]$ de representaciones OM de cada factor primo F_j, con la propiedad que $f \approx \phi_{F_1} \cdots \phi_{F_t}$ es una factorización OM de f.

Si completamos cada representación OM en un tipo $\mathbf{t}_j = \left(\mathbf{t}_{F_j}; (\phi_{F_j}, \lambda_{F_j}, \psi_{F_j})\right)$, entonces podemos asociar a cada representación OM un árbol de tipos. Por ejemplo:

Árbol de una representación OM



En este ejemplo, $f = F_1 \cdots F_4$, con $F_2 \approx F_3$

Las hojas de este árbol se corresponden con los factores primos de f y el tipo determinado por el camino que une la hoja con el nodo raiz es una representación OM de este factor

Si suprimimos los nodos hoja del árbol y las aristas punteadas, nos queda el árbol genómico de f

La estructura de este árbol es útil para ciertas cuestiones donde necesitemos conocer con precisión la información genética que comparten dos factores. Por ejemplo, para calcular $v(\mathrm{Res}(F_i, F_j))$

Objetivos

(I) Calcular una representación OM de un polinomio dado f, libre de cuadrados

Tendremos la información genética de cada factor primo y una primera "buena" aproximación a cada uno de los factores

(II) A partir de una representación OM de un factor primo F de f, obtener una aproximación a F con una calidad prefijada

Nos proporcionará un algoritmo de factorización v-ádico

Estas tareas son llevadas a cabo por el **Algoritmo de Montes** y el **Algoritmo SFL** (Single-factor lifting), respectivamente

Muchas gracias por vuestra atención.