Factorización de polinomios sobre cuerpos de funciones

Felipe Voloch

Laten

Noviembre 2021

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

Resumo

Si K/k es un cuerpo de funciones en una variable, describimos un algoritmo general para factorizar polinomios en una variable con coeficientes en K. El algoritmo es lo suficientemente flexible para encontrar factores sujetos a restricciones adicionales, por ejemplo, para encontrar todas las raíces que pertenecen a un dado k-subespacio de dimensión finita de K más eficientemente. También proporciona una prueba de irreductibilidad determinista en tiempo polinomial.

Algoritmo de Factorizacion Generico

Zassenhaus
Pohst
vor [illegible] [illegible]

Los algoritmos antiguos siguen el siguiente modelo:

$\mathcal{O}$ dominio con cuerpo de fracciones K. Factore $G(T) \in K[T]$.

- Escoje un ideal maximal appropriado $\mathfrak{m} \subset \mathcal{O}$.
- Factore $G(T)$ in $\mathcal{O}/\mathfrak{m}[T]$. $\longleftarrow$ probabilistico
- Levante factorization a $\mathcal{O}/\mathfrak{m}^k[T]$ para grande k.
- Recupere una factorización en $K[T]$ a partir de ella.

LLL

$\mathbb{Z}[T]$

$\mathcal{O}[T]$

Nuestro algoritmo - inicio

- Cuerpo de funciones K/k of characteristic $p > 0$
- $G(T) \in K[T]$ monico, separable, de grado s.
- k-espacios vectoriales de dimension finita
  $V_i \subset K, i = 0, \ldots r-1$, con una k-basis $\{\alpha_{ij}\}$ para cada
  $V_i, r < s$.

La salida es un factor monico de $G(T)$ de la forma

$H(T) = \sum_{i=0}^{r} b_i T^i$, $b_i \in V_i$ o prueba de que no existe.

$H \mid G$

Caso especial

Criterio Wronskiano

$k \subset \mathbb{C}$

$y_0, y_1, \dots, y_n$ funciones son linealmente dependientes sobre $\mathbb{C}$ $\iff$ $\det\left(\frac{d^i y_j}{dx^i}\right) = 0$

Caso especial más importante:

$G(X,T) \in \mathbb{F}_q[X,T]$ polinomio en dos variables, $K = \mathbb{F}_q(X)$,

deg $G = s$. Factor de G de grado r:

$H(X,T) = \sum_{i=0}^{r} b_i(X) T^i$, $b_i \in \mathbb{F}_q[X]$, deg $b_i \leq r - i$. $= V_i$

Relación de dependencia linear entre los $X^i T^j$, $i + j \leq r$ en la

curva $H = 0$.

$H(X,T) = 0$

Si $G(X,T) = 0$, $\boxed{dT/dX = -G_X/G_T}$, etc.

$\frac{dT}{dX}$

$d^2T/dX^2, \dots$

Derivadas de Hasse

$D^{(1)} =$ una derivación como $\frac{d}{dx}$

$D^{(i)}, i \geq 0$, k-operadores lineares en K satisfaciendo:

$i!\, D^{(i)} = D^i$

$$\left\{ \begin{aligned} D^{(i)} \circ D^{(j)} &= \binom{i+j}{j} D^{(i+j)}, \\ D^{(i)}(uv) &= \sum_{j=0}^{i} D^{(j)}(u) D^{(i-j)}(v). \end{aligned} \right.$$

" $D^{(i)} = \frac{D^i}{i!}$ "

$D^{(i)}(\phi)$ pueden seer computados como polinomios en ϕ si $G(\phi) = 0$. Sean $\phi_0, \ldots, \phi_m \in R$ los $\alpha_{ij}\phi^i$ en alguna orden.

α_{ij}

Los $\phi_0, \ldots, \phi_m \in K$ son linearmente independentes sobre k si e solo si existen inteiros $0 = \varepsilon_0 < \cdots < \varepsilon_m$ con $(D^{(\varepsilon_i)}(\phi_j))$ de rango maximal $m+1$.

$\det (D^{\varepsilon_i} \phi_j) \neq 0$

Nuestro algoritmo

ϕ imagen T $\quad$ $G(\phi)=0$ $\quad$ $K[T]/(G(T))$

$R = K[T]/(\mathfrak{m}^q, G(T))$. Computaciones hechas en R. $\quad$ $q > \Delta$ $\quad$ q una potencia dep

Ache una cota Δ para ε_i

Intente la eliminación gaussiana en $M = (D^{(i)}(\phi_j))_{\substack{i=0,\dots,\Delta \\ j=0,\dots,m}}$

if Some pivot $P(T)$ is not invertible **then**

  Replace $G(T)$ by $D(T) = \gcd(G(T), P(T))$ and $G(T)/D(T)$

end if $\quad$ $P(T)$

if M has full rank **then**

  return $G(T)$ has no factor of required form

else

  return a_j s.t. $\sum_{j=0}^m a_j D^{(i)}(\phi_j) = 0, i = 0, 1, \dots, \Delta,\ a_0 = 1.$

end if

$D^{(i)}$ $\quad$ $i < q$ $\quad$ $D^{(i)}(t^q) = 0$ si $i < q$

Teorema

El algoritmo acima retorna, en tiempo polinomial determinista en p, s, Δ un certificado de que $G(T)$ no tiene un factor de la forma requerida, o una descomposición de R como suma directa de anillos R' tales que, para cada sumando R', el algoritmo genera elementos u_{ij} de R' que son constantes en cada sumando de la descomposicin de R' en anillos locales y a partir de los cuales se puede construir un factor de $G(T)$ de la forma requerida o un certificado de que no hay tal factor. En particular, el algoritmo proporciona una prueba de irreductibilidad absoluta en tiempo polinomial en la caracterśtica p para p polinomialmente acotado en s, Δ.

Ejemplo

$F(x,\phi) = 0$

Factor linear de $F(X,T) \in k[x,t]$. Existe solo si $D^{(2)}(\phi) = 0$ (i

$D^{(p^j)}(\phi) = 0$ para $p^j \leq \deg F$) para una raiz $F(X,\phi) = 0$.

Note $D^{(2)}(\phi) = -(F_{XX}F_T^2 - 2F_{XT}F_XF_T + F_{TT}F_T^2)/F_T^3$ evaluada at ϕ.

Si eso vale, factor linear es

$$0 = T - \phi = T - D(\phi)X - (\phi - D(\phi)X) = \boxed{T - aX - b}$$

0

ambos $a = D(\phi)$, $b = \phi - D(\phi)x$ son localmente constante.

$D(a) = D^{(2)}\phi = 0$ $\quad D(b) = D(\phi) - \cancel{D(\phi)} - D^{(2)}\phi\, x = 0$

GRACIAS

$$R = \mathcal{O}[T] \big/ \left(m^q, G(T)\right) \qquad D^{(i)}: R \to R$$

n grande

$$R_n = \mathcal{O}[T] \big/ \left(m^n, G(T)\right) \qquad \mathcal{O} = \mathbb{F}_q\{x\}$$

$$m = (\cancel{x} - a)$$

$$D^{(i)} : R_n \to R_{n-i}$$