Factorización de polinomios sobre cuerpos de funciones

Felipe Voloch

Laten

Noviembre 2021

UC
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

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 $\mathcal{O}/\mathfrak{m}[T]$.
- Levante factorization a $\mathcal{O}/\mathfrak{m}^k[T]$ para grande k.
- Recupere una factorización en $K[T]$ a partir de ella.

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.

Caso especial

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:

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

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

curva $H = 0$.

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

Derivadas de Hasse

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

$$D^{(i)} \circ D^{(j)} = \binom{i+j}{j} D^{(i+j)},$$

$$D^{(i)}(uv) = \sum_{j=0}^{i} D^{(j)}(u) D^{(i-j)}(v).$$

$D^{(i)}(\phi)$ 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. 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 $m+1$.

Nuestro algoritmo

$R = K[T]/(\mathfrak{m}^q, G(T))$. Computaciones hechas en R.
Ache una cota Δ para ε_i
Intente la eliminación gaussiana en $M = (D^{(i)}(\phi_j))_{\substack{i=0,\ldots,D \\ j=0,\ldots,m}}$
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
if M has full rank **then**
  return $G(T)$ has no factor of required form
else
  return a_j s.t. $\sum_{j=0}^m a_j D^{(i)}(\phi_j) = 0, i = 0, 1, \ldots, \Delta,\ a_0 = 1.$
end if

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

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

$$T - \phi = T - D(\phi)X - (\phi - D(\phi)X) = T - aX - b$$

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

GRACIAS