Factoring polynomials over function fields

Felipe Voloch

ANTS XVI

July 2024

Abstract

If K/k is a function field in one variable, we describe a general algorithm to factor one-variable polynomials with coefficients in K. The algorithm is flexible enough to find factors subject to additional restrictions, e.g., to find all roots that belong to a given finite dimensional k-subspace of K more efficiently. It also gives a deterministic polynomial time irreducibility test.

Generic Factorization Algorithm

Old algorithms follow the following pattern:

$\mathcal{O}$ int domain with quotient field K. Factor $G(T) \in K[T]$.

- Choose an appropriate maximal ideal $m \subset \mathcal{O}$.
- Factor $G(T)$ in $\mathcal{O}/m[T]$.
- Lift factorization to $\mathcal{O}/m^k[T]$ for large k.
- Recover a factorization in $K[T]$ from it.

Our algorithm - setup

- Function field K/k of characteristic p
- $G(T) \in K[T]$ monic, squarefree, of degree s.
- Finite dimensional k-vector spaces $V_i \subset K, i = 0, \ldots r-1$, together with a k-basis $\{\alpha_{ij}\}$ for each V_i, where $r < s$.

Let $\phi_0, \ldots, \phi_m \in R$ be the $\alpha_{ij}\phi^i$ in some order, $G(\phi) = 0$.

The output is either a monic factor of $G(T)$ of the form $H(T) = \sum_{i=0}^{r} b_i T^i, b_i \in V_i$ or proof it doesn't exist.

Special cases

$K = k(x), G(x, T) = \sum_{i+j \leq s} a_{ij} x^i T^j, a_{ij} \in k$. If V_i is the span of $x^j, j \leq r - i$, then $H(x, T)$ will be a factor of $G(x, T)$ of degree r in x, T.

K arbitrary, $r = 1$ is the same as finding roots of $G(T)$ in V_0.

Application: Guruswami-Sudan list decoding of algebraic geometry codes.

Hasse derivatives

$D^{(i)}, i = 0, 1, \ldots,$ are k-linear operators on K satisfying:

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

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

$D^{(i)}(\phi)$ can be computed as polynomials in ϕ if $G(\phi) = 0$.

Also $\phi_0, \ldots, \phi_m \in K$ linearly independent over k if and only if there exist integers $0 = \varepsilon_0 < \cdots < \varepsilon_m$ with $(D^{(\varepsilon_i)}(\phi_j))$ of maximal rank $m + 1$.

Our algorithm

$R = K[T]/(G(T))$, $\mathfrak{m}$ maximal ideal. Work in $R/\mathfrak{m}^q$.
Find bound Δ for ε_i.
Attempt Gaussian elimination on $M = (D^{(i)}(\phi_j))_{\substack{i=0,\ldots,D \\ j=0,\ldots,m}}$
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

Example

Linear factor of $F(x,t) \in k[x,t]$. Exists only if $D^{(2)}(\phi) = 0$ (and $D^{(p^j)}(\phi) = 0$ for $p^j \leq \deg F$ if $p > 0$) for root $F(x,\phi) = 0$.

Note $D^{(2)}(\phi) = -(F_{xx}F_t^2 - 2F_{xt}F_xF_t + F_{tt}F_x^2)/F_t^3$ evaluated at ϕ.

If that holds, linear factor is

$$t - \phi = t - D(\phi)x - (\phi - D(\phi)x) = t - ax - b$$

and both $a = D(\phi), b = \phi - D(\phi)x$ are locally constant.

THANK YOU