Hensel's Lemma and Weierstrass Preparation for UPoPS

Alex Brandt

Department of Computer Science
University of Western Ontario, Canada

May 28, 2021

Outline

1 Notations

2 Weierstrass Preparation Theorem

3 Hensel's Lemma

Formal Power Series

- Let $\mathbb{K}$ be an algebraically closed field.

- Denote by $\mathbb{K}[[X_1, \dots, X_n]]$ the ring of formal power series with coefficients in $\mathbb{K}$ and with variables $X_1, \dots, X_n$.
  ↳ $X^e = X_1^{e_1} \cdots X_n^{e_n}$, $e = (e_1, \dots, e_n)$, $|e| = e_1 + \cdots + e_n$

- For $f \in \mathbb{K}[[X_1, \dots, X_n]]$:
  ↳ $f_{(k)} = \sum_{|e|=k} a_e X^e$ is the homogeneous part of degree k

  ↳ f is known to precision $k \in \mathbb{N}$, when $f_{(i)}$ is known for all $0 \leq i \leq k$.

  ↳ the *order* of f is $\min\{i \mid f_{(i)} \neq 0\}$, if $f \neq 0$, and as ∞ otherwise.

- $\mathcal{M} = \{f \mid \operatorname{ord}(f) \geq 1\} \subset \mathbb{K}[[X_1, \dots, X_n]]$ is the only maximal ideal.
  ↳ $\mathcal{M}^k = \{f \in \mathbb{K}[[X_1, \dots, X_n]] \mid \operatorname{ord}(f) \geq k\}$.

  ↳ $f_{(k)} \in \mathcal{M}^k \setminus \mathcal{M}^{k+1}$

UPoPS

- Denote by $\mathbb{A}[Y]$ the ring of univariate polynomials over power series (UPoPS) where, $\mathbb{A} = \mathbb{K}[[X_1, \ldots, X_n]]$.
- For $f = \sum_{i=0}^{d} a_i Y^i$, for $a_i \in \mathbb{A}$, $\deg(f, Y) = d$.
- A UPoPS is known up to precision k if each of its power series coefficients are known up to precision k.
- A UPoPS f is said to be *general (in Y) of order* j if:
  - ↳ f mod $\mathcal{M}[Y]$ has order j when viewed as a power series, or
  - ↳ for $f = \sum_{i=0}^{d} a_i Y^i$, $a_i \in \mathcal{M}$ for $0 \le i < j$

Outline

1 Notations

2 Weierstrass Preparation Theorem

3 Hensel's Lemma

A First Lemma

Lemma ("Lemma 4")

Let $f, g, h \in \mathbb{K}[[X_1, \dots, X_n]]$ *such that* $f = gh$. *Let* $f_i = f_{(i)}$, $g_i = g_{(i)}$, $h_i = h_{(i)}$. *If* $f_0 = 0$ *and* $h_0 \neq 0$, *then* g_k *is uniquely determined by* $f_1, \dots, f_k$ *and* $h_0, \dots, h_{k-1}$

Proof: Proceed by induction on k.

For $k = 0$, $f_0 = g_0 h_0 = 0$, $h_0 \neq 0$. Thus, $g_0 = 0$ and the statement holds.

Let $k > 0$, assuming hypothesis holds for $k-1$. Expand $f = gh$ mod $\mathcal{M}^{k+1}$:

$$f_1 + f_2 + \dots + f_k = g_1 h_0 + (g_1 h_1 + g_2 h_0) + \dots + (g_1 h_{k-1} + \dots + g_{k-1} h_1 + g_k h_0)$$

$$\Longrightarrow \ f_k = g_1 h_{k-1} + \dots + g_{k-1} h_1 + g_k h_0$$

recalling $h_0 \in \mathbb{K} \setminus \{0\}$, we have $g_k = \frac{1}{h_0}\left(f_k - g_1 h_{k-1} - \dots - g_{k-1} h_1\right)$ $\square$

WPT (1/3)

Theorem (Weierstrass Preparation Theorem)

Let $f = \sum_{i=0}^{d+m} a_i Y^i \in \mathbb{K}[[X_1, \ldots, X_n]][Y]$ *be general of order* d *(i.e.* d *is smallest integer s.t.* $a_d \notin \mathcal{M}$*) and* $0 \le m \in \mathbb{N}$*. Assume that* $f \not\equiv 0 \mod \mathcal{M}[Y]$*. Then, there exists a unique pair* p, α *satisfying the following:*

1. $f = p\,\alpha$,
2. α *is an invertible element of* $\mathbb{K}[[X_1, \ldots, X_n]][[Y]]$,
3. p *is a monic polynomial of degree* d,
4. *writing* $p = Y^d + b_{d-1}Y^{d-1} + \cdots b_1 Y + b_0$, *we have* $b_{d-1}, \ldots, b_0 \in \mathcal{M}$.

Proof: If $n = 0$, $f = \alpha Y^d$, $p = Y^d$, $\alpha = \sum_{i=0}^{m} a_{i+d} Y^i$.

Now assume $n > 0$. Let $\alpha = \sum_{i=0}^{m} c_i Y^i$, with $c_i \in \mathbb{K}[[X_1, \ldots, X_n]]$. From the theorem statement $p = Y^d + \sum_{i=0}^{d-1} b_i Y^i$.

We will determine $b_0, \ldots, b_{d-1}, c_0, \ldots, c_m$ modulo successive powers of $\mathcal{M}$.

WPT (2/3)

$$f = \sum_{i=0}^{d+m} a_i Y^i \qquad p = Y^d + \sum_{i=0}^{d-1} b_i Y^i \qquad \alpha = \sum_{i=0}^{m} c_i Y^i$$

Equating coefficients in $f = p\alpha$ gives:

$$\begin{array}{rcl}
a_0 & = & b_0 c_0 \\
a_1 & = & b_0 c_1 + b_1 c_0 \\
 & \vdots & \\
a_{d-1} & = & b_0 c_{d-1} + b_1 c_{d-2} + \cdots + b_{d-2} c_1 + b_{d-1} c_0 \\
\hline
a_d & = & b_0 c_d + b_1 c_{d-1} + \cdots + b_{d-1} c_1 + c_0 \\
 & \vdots & \\
a_{d+m-1} & = & b_{d-1} c_m + c_{m-1} \\
a_{d+m} & = & c_m
\end{array}$$

The first d equations define p, the remaining $m+1$ equations define α.

Since α is a unit, $c_0 \notin \mathcal{M}$. By definition, $a_0, \ldots, a_{d-1}$ are all 0 mod $\mathcal{M}$. and thus $b_0, \ldots, b_{d-1}$ are also all 0 mod $\mathcal{M}$.

WPT (3/3)

All $a_0, \ldots, a_{d+m}$ are sufficiently known as they are the input.
Inductively assume all $b_0, \ldots, b_{d-1}, c_0, \ldots, c_m$ are known mod $\mathcal{M}^k$.
We now determine them mod $\mathcal{M}^{k+1}$. Rearranging prev. equations gives:

$$
\begin{array}{rclrcl}
a_0 & = & b_0 c_0 & c_m & = & a_{d+m} \\
a_1 - b_0 c_1 & = & b_1 c_0 & c_{m-1} & = & a_{d+m-1} - b_{d-1} c_m \\
a_2 - b_0 c_2 - b_1 c_1 & = & b_2 c_0 & c_{m-2} & = & a_{d+m-2} - b_{d-2} c_m - b_{d-1} c_{m-1} \\
& \vdots & & & \vdots & \\
a_{d-1} - b_0 c_{d-1} - \cdots - b_{d-2} c_1 & = & b_{d-1} c_0 & c_0 & = & a_d - b_0 c_d - \cdots - b_{d-1} c_1
\end{array}
$$

Recall $c_0 \notin \mathcal{M}$. By Lemma 4 and $a_0 = b_0 c_0$, we determine b_0 mod $\mathcal{M}^{k+1}$

Since $b_0 \in \mathcal{M}$, knowing c_1 mod $\mathcal{M}^k$ is sufficient to know $b_0 c_1$ mod $\mathcal{M}^{k+1}$.
Then, $a_1 - b_0 c_1$ is known mod $\mathcal{M}^{k+1}$ and we determine b_1 mod $\mathcal{M}^{k+1}$ by Lemma 4. This follows for $b_2, \ldots, b_{d-1}$.

Since $b_i \in \mathcal{M}$ for $0 \leq i < d$, all products $b_i c_j$ now known mod $\mathcal{M}^{k+1}$.
Determining $c_0, \ldots, c_m$ mod $\mathcal{M}^{k+1}$ follows with simple poly. arithmetic. $\square$

Outline

1 Notations

2 Weierstrass Preparation Theorem

3 Hensel's Lemma

Hensel's Lemma

Theorem (Hensel's Lemma)

Let $f = Y^d + \sum_{i=0}^{d-1} a_i Y^i$ *be a monic polynomial with* $a_i \in \mathbb{K}[[X_1, \ldots, X_n]]$*.*
Let $\bar{f} = f(0, \ldots, 0, Y) = (Y - c_1)^{d_1}(Y - c_2)^{d_2} \cdots (Y - c_r)^{d_r}$*,*
for $c_1, \ldots, c_r \in \mathbb{K}$ *and positive integers* $d_1, \ldots, d_r$*. Then, there exists* $f_1, \ldots, f_r \in \mathbb{K}[[X_1, \ldots, X_n]][Y]$*, all monic in Y, such that:*

1. $f = f_1 \cdots f_r$,
2. $\deg(f_i, Y) = d_i$ *for* $1 \le i \le r$*, and*
3. $\bar{f}_i = (Y - c_i)_i^d$ *for* $1 \le i \le r$*.*

We proceed by induction on r. For $r = 1$, $d_1 = d$ and we have $f_1 = f$, where f_1 has all the required properties.

Now assume $r > 1$. A change of coordinates in Y, sends c_r to 0 as g:

$$\begin{aligned} g(X_1, \ldots, X_n, Y) &= f(X_1, \ldots, X_n, Y + c_r) \\ &= (Y + c_r)^d + a_{d-1}(Y + c_r)^{d-1} + \cdots + a_0 \end{aligned}$$

Hensel's Lemma (2/2)

$$\begin{aligned} g(X_1, \ldots, X_n, Y) &= f(X_1, \ldots, X_n, Y + c_r) \\ &= (Y + c_r)^d + a_{d-1}(Y + c_r)^{d-1} + \cdots + a_0 \end{aligned}$$

By construction, g is general of order d_r and WPT can be applied to obtain $g = p\,\alpha$ with p being of degree d_r and $\bar{p} = Y^{d_r}$.

Reversing the change of coordinates we set $f_r = p(Y - c_r)$ and $f^* = \alpha(Y - c_r)$, and we have $f = f^* f_r$.

f_r is a monic polynomial of degree d_r in Y with $\bar{f_r} = (Y - c_r)^{d_r}$.

We have $\bar{f^*} = (Y - c_1)^{d_1}(Y - c_2)^{d_2} \cdots (Y - c_{r-1})^{d_{r-1}}$. The inductive hypothesis applied to f^* implies the existence of $f_1, \ldots, f_{r-1}$.

$\square$

Sources

On the Complexity and Parallel Implementation of Hensel's Lemma and Weierstrass Preparation