
REPORT: HENSEL LIFTING AND NEWTON ITERATION IN VALUTATION RINGS

Instructor: Amit Kumar Sinhababu and Sumanta Ghosh

SOHAM CHATTERJEE

SOHAMCHATTERJEE999@GMAIL.COM

WEBSITE: SOHAMCH08.GITHUB.IO

CONTENTS

CHAPTER 1	INTRODUCTION	PAGE 2
CHAPTER 2	HENSEL LIFTING	PAGE 3
2.1	Conditions related to Hensel's Lemma	3
2.2	Hensel's Lemma	4
CHAPTER 3	NEWTON ITERATION	PAGE 6
CHAPTER 4	SOLVING DIFFERENTIAL EQUATIONS	PAGE 7
CHAPTER 5	FINDING SHORT VECTORS IN MODULES	PAGE 8
CHAPTER 6	FACTORIZATION OF POLYNOMIALS	PAGE 9

Chapter 1

Introduction

Chapter 2

Hensel Lifting

The hensel method described here will lift an approximate factorization of a polynomial over a Hensel Ring R with valuation v where the factors are relatively prime. We will show a linear convergence and a quadratic convergence behavior for the liftings.

Note:-

From the valuation v over R we naturally get a valuation v over the polynomial ring $R[x]$ by defining

$$\forall f \in R[x], \text{ let } f = \sum_{i=0}^n f_i x^i, \text{ then } v\left(\sum_{i=0}^n f_i x^i\right) = \max_i \{v(f_i)\}$$

2.1 Conditions related to Hensel's Lemma

We will define 5 conditinos. First suppose we have:

- (1) $f \in R[x]$
- (2) $f_0, \dots, f_m \in R[x] \quad \mathcal{F} = \{f_i : 0 \leq i \leq m\}$
- (3) $f_0^*, \dots, f_m^* \in R[x] \quad \mathcal{F}^* = \{f_i^* : 0 \leq i \leq m\}$
- (4) $s_0, \dots, s_m \in R[x] \quad \mathcal{S} = \{s_i : 0 \leq i \leq m\}$
- (5) $s_0^*, \dots, s_m^* \in R[x] \quad \mathcal{S}^* = \{s_i^* : 0 \leq i \leq m\}$
- (6) $z \in R$
- (7) $\alpha, \delta, \epsilon \in \mathbb{R}$
- (8) $\delta^* \in \mathbb{R}$
- (9) $\gamma = \max\{\delta, \alpha\epsilon\}$

As you can see the set \mathcal{F}^* basically represents the lift of \mathcal{F} but here since we are saying the conditions in more generality we are not assuming any relations among them and we define some conditions involving them.

- $H_1(m, f, \mathcal{F}, \mathcal{S}, \epsilon) := v\left(f - \prod_{i=0}^m f_i\right) \leq \epsilon < 1$
- $H_2(m, f, \mathcal{F}, \mathcal{S}, z, \delta) := v\left(\sum_{i=0}^m s_i \prod_{j \neq i} f_j - z\right) < \text{leq} \delta < 1$
- $H_3(m, f, \mathcal{F}, \mathcal{S}, z, \alpha, \delta, \epsilon) :=$
 - (1) f_1, \dots, f_m are monic
 - (2) $\deg\left(\prod_{i=0}^m f_i\right) \leq \deg f$
 - (3) $\deg s_i \leq \deg f_i \quad \forall i \in [m]$
 - (4) $\alpha\delta \leq 1, \alpha\epsilon^2 \leq 1$
 - (5) $1 \leq \alpha v(z)$

- $H_4(m, f, \mathcal{F}, \mathcal{F}^*, \mathcal{S}, \mathcal{S}^*, \alpha, \delta, \epsilon) :=$
 - (1) $v(f_i^* - f_i) \leq \alpha\epsilon$ $\forall 0 \leq i \leq m$
 - (2) $v(s_i^* - s_i) \leq \alpha\epsilon$ $\forall 0 \leq i \leq m$
 - (3) $\deg f_i^* = \deg f_i$ $\forall i \in [m]$
 - (4) $\deg s_i < \deg f_i \implies \deg s_i^* < \deg f_i^*$ $\forall i \in [m]$

- $H_5(m, f, \mathcal{F}, \mathcal{F}^*, \mathcal{S}, \mathcal{S}^*, \alpha, \delta, \epsilon, \delta^*) :=$ Let $p \in [m]$. Then suppose

- $\mathcal{I}_p = \{I_0, I_1, \dots, I_p\}$ be a partition of $\{0, \dots, m\}$ with $0 \in I_0$.
- $\overline{\mathcal{F}}_p^m = \{\overline{f}_i : i \in [p]\} \subseteq R[x]$ be a set of monic polynomials

Then define:

$$F_i = \prod_{j \in I_i} f_j, \quad F_i^* = \prod_{j \in I_i} f_j^*, \quad \mathfrak{s}_i^* = \sum_{j \in I_i} s_j \frac{F_i^*}{f_j^*}$$

So now we denote:

$$\mathcal{F} = \{F_i : 0 \leq i \leq p\}, \quad \mathcal{F}^* = \{F_i^* : 0 \leq i \leq p\}, \quad \mathcal{S} = \{\mathfrak{s}_i^* : 0 \leq i \leq p\}$$

Assume:

1. $v(\overline{f}_i - F_i) \leq \alpha\epsilon \forall i \in [p]$
2. $\alpha v(s_i) \leq 1 \forall 0 \leq i \leq m$
3. $\alpha\delta < 1, \alpha^2\delta \leq 1$
4. $\alpha^2\epsilon < 1, \alpha^3\epsilon \leq 1$

Then the following are equivalent:

- (i) $\exists \overline{f}_0, \overline{s}_0, \dots, \overline{s}_p \in R[x]$ denote

$$\overline{\mathcal{F}} = \{\overline{f}_i : 0 \leq i \leq p\}, \quad \overline{\mathcal{S}} = \{\overline{s}_i : 0 \leq i \leq p\}$$

then the following conditions are true:

- (a) $H_1(p, f, \overline{\mathcal{F}}, \overline{\mathcal{S}}, \epsilon^*)$
- (b) $H_2(p, f, \overline{\mathcal{F}}, \overline{\mathcal{S}}, z, \delta^*)$
- (c) $H_3(p, f, \overline{\mathcal{F}}, \overline{\mathcal{S}}, z, \alpha^*, \delta^*, \epsilon^*)$
- (d) $H_4(p, f, \mathcal{F}, \mathcal{F}^*, \mathcal{S}, \mathcal{S}^*, z, \alpha^*, \delta^*, \epsilon^*)$

where $\alpha^* = \alpha, \epsilon^* = \alpha\epsilon\gamma$

- (ii) $\exists \overline{f}_0 \in R[x]$ such that $H_1(p, f, \overline{\mathcal{F}}, \overline{\mathcal{S}}, \epsilon^*)$ is true

- (iii) $\forall i \in [p]$ we have $v(\overline{f}_i - F_i^*) \leq \epsilon^*$.

The first 3 conditions here together imply that: From H_1 we get that $f_0 \cdots f_m$ is a good approximation of factorization of f with ϵ -precision, $H_2 \implies z$ plays a similar role to the gcd of f_0, \dots, f_m and it shows the generalized bezout's identity for gcd for multiple elements.

H_4 shows the connection between the lifts f_i^*, s_i^* and f_i, s_i .

H_5 basically states that the lifts are unique in the sense that one can group some of the f_i^* 's to form F_0, \dots, F_p and change F_i to \overline{f}_i with precision ϵ^* and still one will have the factorization of f with precision ϵ^* . H_5 is very important for the factorization algorithm in chapter 6.

Now we will state the Hensel's Lemma and will later give the algorithm to obtain the lifts.

2.2 Hensel's Lemma

Theorem 2.2.1 Hensel's Lemma

Assume that we have $f \in R[x]$, $\mathcal{F} = \{f_0, \dots, f_m\} \subseteq R[x]$, $\mathcal{S} = \{s_0, \dots, s_m\} \subseteq R[x]$, $z \in R$ and $\alpha, \delta, \epsilon \in \mathbb{R}$ which satisfy:

1. $H_1(m, f, \mathcal{F}, \mathcal{S}, \epsilon)$
2. $H_2(m, f, \mathcal{F}, \mathcal{S}, z, \delta)$
3. $H_3(m, f, \mathcal{F}, \mathcal{S}, z, \alpha, \delta, \epsilon)$

Then we can compute efficiently

$$\mathcal{F}^* = \{f_i^* : 0 \leq i \leq m\} \quad \text{and} \quad T = \{t_0, \dots, t_m\}$$

such that

(i) **Linear Case:**

Chapter 3

Newton Iteration

Chapter 4

Solving Differential Equations

Chapter 5

Finding Short Vectors in Modules

Chapter 6

Factorization of Polynomials