Lecture 10

Note Title 3/12/2012

3/12/2012

Notes on Hensel Lifting

(for other stuff see notes for lecture 8)

Goals of Hensel Lifting

Given Ideal $I \subseteq R \subseteq R[x]$, $f, g, h \in R[x]$ & integer t

s.t. $f \equiv g \cdot h \pmod{I}$

(1) Existence: Prove $\exists\ g_1, h_1$ s.t.

$$f \equiv g_1 \cdot h_1 \pmod{I^t}$$

(2) Construction: find g_1, h_1

(3) Uniqueness: Prove g_1, h_1 "essentially" unique

Caveats

No uniqueness?

Reason 1:

$$f = (x-1+r_1)(x-1+r_2) \qquad r_1, r_2 \in J$$

$$g = (x-1)$$

$$h = (x-1)$$

Should $g_1 = x-1+r_1$?

$= x-1+r_2$?

(More seriously ... this is impediment even to existence. No example 😊)

Reason 2: $U \in I^{t/2}$

$\Rightarrow g_2 = g_1(1+u)$; $h_2 = h_1(1-u)$

are also solutions. So best to hope for is uniqueness up to such equivalence.

The real Lemma

Hensel Lemma

Let $I \subseteq R \subseteq R[x]$ be an Ideal;

$f, g, h, a, b \in R[x]$ be s.t.

(1) $f = g \cdot h \pmod{I}$

(2) $ag + bh = 1 \pmod{I}$

Then $\forall t \ \exists \ g_1, h_1, a_1, b_1$ s.t.

(1') $f = g_1 \cdot h_1 \pmod{I^{2t}}$

(2') $a_1 g_1 + b_1 h_1 = 1 \pmod{I^{2t}}$

(3') $g_1 = g \pmod{I}$; $h_1 = h \pmod{I}$

Furthermore if g_2, h_2 satisfy (1'), (2'), (3')

then $\exists \ u \in I^t$ s.t.

$g_2 = g_1(1+u) \pmod{I^{2t}}$

$h_2 = h_1(1-u) \pmod{I^{2t}}$

Proofs

Existence of a_1, b_1, g_1, h_1 by induction on t. Say a_0, b_0, g_0, h_0 satisfy (1'), (2''), (3') for $t_0 = t/2$.

g_1, h_1: Let $f = g_0 h_0 + q$ $\quad q \in I^t$

& $a_0 g_0 + b_0 h_0 = 1 + r_0$ $\quad r_0 \in I^t$

$$g_1 \triangleq g_0 + b_0 q$$
$$h_1 \triangleq h_0 + a_0 q$$

$$g_1 h_1 = g_0 h_0 + (a_0 g_0 + b_0 h_0) q + a_0 b_0 q^2$$

$$= g_0 h_0 + q + r_0 q + a_0 b_0 q^2$$

($r_0 q \in I^{2t}$, $a_0 b_0 q^2 \in I^{2t}$)

$$= f \pmod{I^{2t}} \checkmark (1')$$

Note (3') automatically satisfied.

Now let $a_0 g_1 + b_0 h_1 = 1 + r_1$

$r_1 \in I^t$

(must be since $g_0 = g_1 \pmod{I^t}$ & $h_0 = h_1 \pmod{I^t}$)

$$a_1 \triangleq a_0 (1 - r_1)$$
$$b_1 \triangleq b_0 (1 - r_1)$$

$$a_1 \cdot g_1 + b_1 h_1 = 1 - r_1^2 = 1 \pmod{I^{2t}}$$

$r_1^2 \in I^{2t}$

Uniqueness

Let g_2, h_2 be solutions satisfying (1'), (3') also

$g_2 = g_1 + \alpha$; $h_2 = h_1 + \beta$

Let ℓ be largest integer s.t.

$\alpha, \beta \in I^\ell$

Case 1: $\ell \geq t$

Since $g_2 h_2 = g_1 h_1 \pmod{I^{2t}}$

we have $\alpha h_1 + \beta g_1 = 0 \pmod{I^{2t}}$

$\Rightarrow \alpha b_1 h_1 = -\beta b_1 g_1 \pmod{I^{2t}}$

$\Rightarrow \alpha (1 - a_1 g_1) = -\beta b_1 g_1 \pmod{I^{2t}}$

$\Rightarrow \alpha = (\alpha a_1 - \beta b_1) g_1 \pmod{I^{2t}}$

Similarly

$\beta = (\beta b_1 - \alpha a_1) h_1 \pmod{I^{2t}}$

Thus $v = \alpha a_1 - \beta b_1$ satisfies uniqueness condition

Case 2: $\ell < t$

still define α, β, υ as above

$$g_2 = g_1 + \alpha \qquad h_2 = h_1 + \beta$$

$$\upsilon = \alpha a_1 - \beta b_1$$

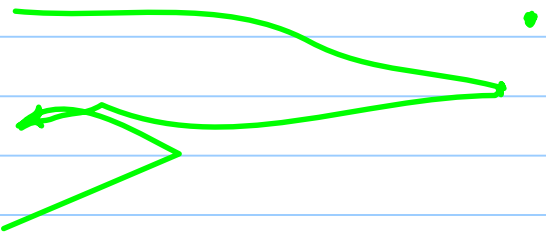
$$g_1 \upsilon = \alpha a_1 g_1 - \beta b_1 g_1$$

$$= \alpha \cdot 1 - \alpha b_1 h_1 - \beta b_1 g_1 \pmod{I^{2\ell}}$$

$$= \alpha - b_1 (\alpha h_1 + \beta g_1)$$

$$= \alpha \pmod{I^{2\ell}}$$

$$g_2 h_2 = g_1 h_1 (1 - \upsilon^2) \pmod{I^{2\ell}}$$



$g_0 h_0 \longrightarrow g_0 (1+v_0)(1+v_1)$

$h_0 (1-v_0)(1-v_1)$

$g_0 h_0 (1-v_0^2)$