

# Course "Polynomials: Their Power and How to Use Them", JASS'07

## Computing with polynomials: Hensel constructions

Lukas Bulwahn

Fakultät für Informatik  
TU München

March 28, 2007

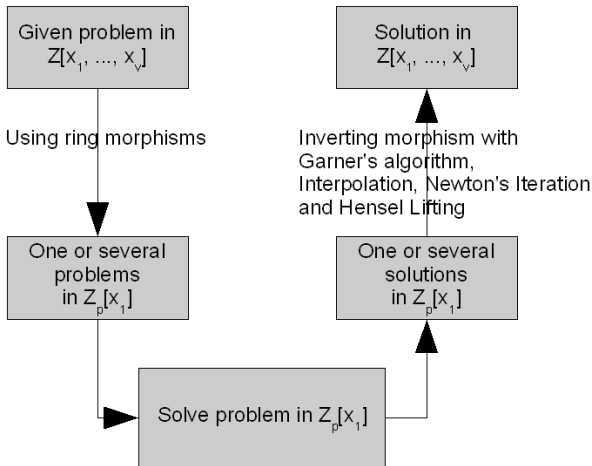
General background

Chinese Remainder Algorithm and Newton Interpolation

The Hensel lifting

Multivariate Hensel lifting

## Motivation and overview



## Definition 1 (ring homomorphism)

Let  $R$  and  $R'$  be two rings. Then a mapping  $\theta : R \rightarrow R'$  is called a **ring homomorphism** if

1.  $\theta(a + b) = \theta(a) + \theta(b)$  for all  $a, b \in R$
2.  $\theta(ab) = \theta(a)\theta(b)$  for all  $a, b \in R$
3.  $\theta(1) = 1$

## Definition 1 (ring homomorphism)

Let  $R$  and  $R'$  be two rings. Then a mapping  $\theta : R \rightarrow R'$  is called a **ring homomorphism** if

1.  $\theta(a + b) = \theta(a) + \theta(b)$  for all  $a, b \in R$
2.  $\theta(ab) = \theta(a)\theta(b)$  for all  $a, b \in R$
3.  $\theta(1) = 1$

From this definition and the ring axioms also follows:

- ▶  $\theta(0) = 0$
- ▶  $\theta(-a) = -\theta(a)$

## Example 2 (modular homomorphism)

$$\theta_m : \mathbb{Z}[x_1, \dots, x_v] \rightarrow \mathbb{Z}_m[x_1, \dots, x_v]$$

is defined for a fixed  $m \in \mathbb{Z}$  by:

- ▶  $\theta_m(x_i) = x_i$  for  $1 \leq i \leq v$
- ▶  $\theta_m(a) = \text{rem}(a, m)$  for all coefficients  $a \in \mathbb{Z}$

"replace all coefficients by their "modulo m" representation"

## Example 2 (modular homomorphism)

$$\theta_m : \mathbb{Z}[x_1, \dots, x_v] \rightarrow \mathbb{Z}_m[x_1, \dots, x_v]$$

is defined for a fixed  $m \in \mathbb{Z}$  by:

- ▶  $\theta_m(x_i) = x_i$  for  $1 \leq i \leq v$
- ▶  $\theta_m(a) = \text{rem}(a, m)$  for all coefficients  $a \in \mathbb{Z}$

"replace all coefficients by their "modulo m" representation"

for  $a(x, y) = 2xy + 7x - y^2 + 8 \in \mathbb{Z}[x, y]$ :

$$\theta_5(a) = 2xy + 2x - y^2 - 2 \in \mathbb{Z}_5[x, y]$$

### Example 3 (evaluation homomorphism)

$$\theta_{x_i-\alpha} : D[x_1, \dots, x_v] \rightarrow D[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_v]$$

is defined for a particular indeterminate  $x_i$  and a fixed  $\alpha \in D$  by:

$$\theta_{x_i-\alpha}(a(x_1, \dots, x_v)) = a(x_1, \dots, x_{i-1}, \alpha, x_{i+1}, \dots, x_v)$$

"substitute  $\alpha$  for  $x_i$ "

### Example 3 (evaluation homomorphism)

$$\theta_{x_i-\alpha} : D[x_1, \dots, x_v] \rightarrow D[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_v]$$

is defined for a particular indeterminate  $x_i$  and a fixed  $\alpha \in D$  by:

$$\theta_{x_i-\alpha}(a(x_1, \dots, x_v)) = a(x_1, \dots, x_{i-1}, \alpha, x_{i+1}, \dots, x_v)$$

"substitute  $\alpha$  for  $x_i$ "

for  $a(x, y) = 2xy + 7x + y^2 + 8 \in \mathbb{Z}[x, y]$ :

$$\theta_{x-2}(a) = 4y + 14 + y^2 + 8 \in \mathbb{Z}[y]$$

## Characterization of homomorphisms

Ring homomorphisms can be uniquely be characterized by ideals.

### Definition 4

Let  $R$  be a commutative ring. A nonempty subset  $I$  of  $R$  is called **ideal** if

1.  $a + b \in I$  for all  $a, b \in I$
2.  $-a \in I$  for all  $a \in I$
3.  $ar \in I$  for all  $a \in I$  and for **all**  $r \in R$ .

## Example 5 (Examples for ideals)

## Example 5 (Examples for ideals)

►  $\langle m \rangle \subset \mathbb{Z} = \{m \cdot r : r = 0, \pm 1, \pm 2, \dots\}$

## Example 5 (Examples for ideals)

- ▶  $\langle m \rangle \subset \mathbb{Z} = \{m \cdot r : r = 0, \pm 1, \pm 2, \dots\}$
- ▶  $\langle 4 \rangle = \{0, \pm 4, \pm 8, \pm 12, \dots\}$

## Example 5 (Examples for ideals)

- ▶  $\langle m \rangle \subset \mathbb{Z} = \{m \cdot r : r = 0, \pm 1, \pm 2, \dots\}$
- ▶  $\langle 4 \rangle = \{0, \pm 4, \pm 8, \pm 12, \dots\}$
- ▶  $\langle p(x) \rangle \subset \mathbb{Z}[x] = \{p(x) \cdot a(x) : a(x) \in \mathbb{Z}[x]\}$

## Example 5 (Examples for ideals)

- ▶  $\langle m \rangle \subset \mathbb{Z} = \{m \cdot r : r = 0, \pm 1, \pm 2, \dots\}$
- ▶  $\langle 4 \rangle = \{0, \pm 4, \pm 8, \pm 12, \dots\}$
- ▶  $\langle p(x) \rangle \subset \mathbb{Z}[x] = \{p(x) \cdot a(x) : a(x) \in \mathbb{Z}[x]\}$
- ▶  $\langle x - 2 \rangle = \{(x - 2) \cdot a(x) : a(x) \in \mathbb{Z}[x]\}$

## Correspondence of ideals and homomorphisms

We note that:

- ▶ Let  $R$  and  $R'$  be commutative rings. The kernel  $K$  of a homomorphism  $\theta : R \rightarrow R'$  is an ideal in  $R$ .

## Correspondence of ideals and homomorphisms

We note that:

- ▶ Let  $R$  and  $R'$  be commutative rings. The kernel  $K$  of a homomorphism  $\theta : R \rightarrow R'$  is an ideal in  $R$ .
- ▶ If  $\theta_1 : R \rightarrow R'$  and  $\theta_2 : R \rightarrow R''$  have the kernel  $K$ , the two homomorphic images  $\theta_1(R)$  and  $\theta_2(R)$  are isomorphic.

## Correspondence of ideals and homomorphisms

We note that:

- ▶ Let  $R$  and  $R'$  be commutative rings. The kernel  $K$  of a homomorphism  $\theta : R \rightarrow R'$  is an ideal in  $R$ .
- ▶ If  $\theta_1 : R \rightarrow R'$  and  $\theta_2 : R \rightarrow R''$  have the kernel  $K$ , the two homomorphic images are  $\theta_1(R)$  and  $\theta_2(R)$  are isomorphic.
- ▶ Consequently, homomorphism can be constructed and notated using their ideal.

## Correspondence of ideals and homomorphisms

We note that:

- ▶ Let  $R$  and  $R'$  be commutative rings. The kernel  $K$  of a homomorphism  $\theta : R \rightarrow R'$  is an ideal in  $R$ .
- ▶ If  $\theta_1 : R \rightarrow R'$  and  $\theta_2 : R \rightarrow R''$  have the kernel  $K$ , the two homomorphic images are  $\theta_1(R)$  and  $\theta_2(R)$  are isomorphic.
- ▶ Consequently, homomorphism can be constructed and notated using their ideal.
- ▶ Congruence Arithmetic can be done **modulo  $I$**  for any ideal  $I$ .

# Correspondence of ideals and homomorphisms

## Example 6

# Correspondence of ideals and homomorphisms

## Example 6

- ▶ The homomorphism  $\theta_4$  has the kernel/ideal  $\langle 4 \rangle$ .

# Correspondence of ideals and homomorphisms

## Example 6

- ▶ The homomorphism  $\theta_4$  has the kernel/ideal  $\langle 4 \rangle$ .
- ▶ The homomorphism  $\theta_{x-2}$  has the kernel  $\langle x - 2 \rangle$ .

# Correspondence of ideals and homomorphisms

## Example 6

- ▶ The homomorphism  $\theta_4$  has the kernel/ideal  $\langle 4 \rangle$ .
- ▶ The homomorphism  $\theta_{x-2}$  has the kernel  $\langle x - 2 \rangle$ .
- ▶ Evaluation of  $p(x)$ :  $p(c) = d$  is equivalent to  $p(x) \equiv d \pmod{x - c}$ .

# Correspondence of ideals and homomorphisms

## Example 6

- ▶ The homomorphism  $\theta_4$  has the kernel/ideal  $\langle 4 \rangle$ .
- ▶ The homomorphism  $\theta_{x-2}$  has the kernel  $\langle x - 2 \rangle$ .
- ▶ Evaluation of  $p(x)$ :  $p(c) = d$  is equivalent to  $p(x) \equiv d \pmod{x - c}$ .
- ▶ From an "ideal" viewpoint, modular and evaluation homomorphisms are the same.

## Operations on ideals

- ▶ The ideal  $\langle a_1, a_2, \dots, a_n \rangle$  is defined as  $\{a_1 r_1 + \dots + a_n r_n : r_i \in R\}$   
 $a_1, \dots, a_n \in R$  is called **basis**.

## Operations on ideals

- ▶ The ideal  $\langle a_1, a_2, \dots, a_n \rangle$  is defined as

$$\{a_1 r_1 + \dots + a_n r_n : r_i \in R\}$$

$a_1, \dots, a_n \in R$  is called **basis**.

- ▶ For ideal  $I = \langle a_1, \dots, a_n \rangle$  and  $J = \langle b_1, \dots, b_m \rangle$ :

the sum of two ideals is

$$I + J = \langle I + J \rangle = \langle I, J \rangle = \langle a_1, \dots, a_n, b_1, \dots, b_m \rangle$$

the product of two ideals is  $I \cdot J = \langle I \cdot J \rangle =$

$$\langle a_1 b_1, \dots, a_1 b_m, a_2 b_1, \dots, a_2 b_m, \dots, a_n b_1, \dots, a_n b_m \rangle$$

The  $i$ -th power is recursively defined by:

$$I^1 = I \text{ and } I^i = I \cdot I^{i-1} \text{ for } i \geq 2.$$

## Example 7

- ▶  $\langle x, y \rangle$  are all polynomials  $a_1x + a_2y$  with  $a_1, a_2 \in R[x, y]$ .
- ▶  $\langle x, y \rangle \cdot \langle x, y \rangle$  are all polynomials  $a_1x^2 + a_2xy + a_3y^2$  with  $a_1, a_2, a_3 \in R[x, y]$ .
- ▶  $\langle x, y \rangle^k$  are all polynomials with terms of at least a total degree  $k$ .

General background

Chinese Remainder Algorithm and Newton Interpolation

The Hensel lifting

Multivariate Hensel lifting

# Inverting modular homomorphisms with Chinese Remainder Algorithm

The **Chinese Remainder problem** is stated as follows:

Given pairwise comaximal ideals  $I_0, I_1, \dots, I_n$  and given corresponding residues  $s_i \in \mathbb{Z}/I_i$ ,  $0 \leq i \leq n$ , find an integer  $u \in \mathbb{Z}/\prod_{i=0}^n I_i$  such that

$$u \equiv s_i \pmod{I_i}, 0 \leq i \leq n.$$

## The Chinese Remainder Algorithm: Garner's Algorithm

The key to the algorithm:

Express the solution  $u \in \mathbb{Z} / \prod_{i=0}^n l_i$  in mixed radix representation.

### Definition 8 (mixed radix representation)

A element  $u \in \mathbb{Z} / \prod_{i=0}^n l_i$  is in **mixed radix representation** when it is in the form

$$u^{(1)} + \Delta u^{(1)} + \Delta u^{(2)} + \dots + \Delta u^{(n)}$$

where  $u^{(1)} = u_0 \in \mathbb{Z} / l_0$   
 and  $\Delta u^{(k)} \in \prod_{i=0}^{k-1} l_i / \prod_{i=0}^k l_i$  for  $1 \leq k \leq d$   
 and  $n$  is the number of equations.

We define  $u^{(k+1)} = u^{(1)} + \Delta u^{(1)} + \dots + \Delta u^{(k)}$ .

## Mixed radix representation

So, for ideals  $I_i = \langle m_i \rangle$ , the elements  $\Delta u^{(k)}$  can be represented in the following form:

$$\Delta u^{(k)} = u_k \cdot \prod_{i=0}^{k-1} m_i$$

where  $u_k \in Z_{m_k}$  for  $0 \leq k \leq n$ .

Therefore,  $u$  can be written as:

$$u = u_0 + u_1 \cdot m_0 + u_2 \cdot (m_0 m_1) + \cdots + u_n \cdot \left( \prod_{i=0}^{n-1} m_i \right)$$

## Mixed radix representation

So, for ideals  $I_i = \langle m_i \rangle$ , the elements  $\Delta u^{(k)}$  can be represented in the following form:

$$\Delta u^{(k)} = u_k \cdot \prod_{i=0}^{k-1} m_i$$

where  $u_k \in Z_{m_k}$  for  $0 \leq k \leq n$ .

Therefore,  $u$  can be written as:

$$u = u_0 + u_1 \cdot m_0 + u_2 \cdot (m_0 m_1) + \cdots + u_n \cdot \left( \prod_{i=0}^{n-1} m_i \right)$$

### Example 9

$$m_0 = 3; m_1 = 5; m = 3 \cdot 5 = 15$$

$$5 = (-1) + 2 \cdot 3$$

Any number from -7 to 7 can be represented in this form.

## From modulo equations to mixed radix form

Iteration over  $i = 0 \dots n$ :

- ▶ For  $i = 0$ :  $u = s_0 \bmod m_0$   
Choose  $u_0 = s_0$ .

## From modulo equations to mixed radix form

Iteration over  $i = 0 \dots n$ :

- ▶ For  $i = 0$ :  $u = s_0 \bmod m_0$

Choose  $u_0 = s_0$ .

- ▶ For  $i = k$ :  $u_0, \dots, u_{k-1}$  are known.

Solve

$$u_0 + u_1(m_0) + u_2(m_0 m_1) + \dots + u_k(\prod_{i=0}^{k-1} m_i) \equiv s_k \bmod m_k$$

## From modulo equations to mixed radix form

Iteration over  $i = 0 \dots n$ :

- ▶ For  $i = 0$ :  $u = s_0 \bmod m_0$

Choose  $u_0 = s_0$ .

- ▶ For  $i = k$ :  $u_0, \dots, u_{k-1}$  are known.

Solve

$$u_0 + u_1(m_0) + u_2(m_0 m_1) + \dots + u_k(\prod_{i=0}^{k-1} m_i) \equiv s_k \bmod m_k$$

## From modulo equations to mixed radix form

Iteration over  $i = 0 \dots n$ :

- ▶ For  $i = 0$ :  $u = s_0 \bmod m_0$

Choose  $u_0 = s_0$ .

- ▶ For  $i = k$ :  $u_0, \dots, u_{k-1}$  are known.

Solve

$$u_0 + u_1(m_0) + u_2(m_0m_1) + \dots + u_k(\prod_{i=0}^{k-1} m_i) \equiv s_k \bmod m_k$$

$$\implies u_k \equiv$$

$$\left( s_k - \left( u_0 + \dots + u_{k-1} \left( \prod_{i=0}^{k-2} m_i \right) \right) \right) \left( \prod_{i=0}^{k-1} m_i \right)^{-1} \bmod m_k$$

## From modulo equations to mixed radix form

Iteration over  $i = 0 \dots n$ :

- ▶ For  $i = 0$ :  $u = s_0 \bmod m_0$

Choose  $u_0 = s_0$ .

- ▶ For  $i = k$ :  $u_0, \dots, u_{k-1}$  are known.

Solve

$$u_0 + u_1(m_0) + u_2(m_0m_1) + \dots + u_k(\prod_{i=0}^{k-1} m_i) \equiv s_k \bmod m_k$$

$$\implies u_k \equiv$$

$$\left( s_k - \left( u_0 + \dots + u_{k-1} \left( \prod_{i=0}^{k-2} m_i \right) \right) \right) \left( \prod_{i=0}^{k-1} m_i \right)^{-1} \bmod m_k$$

From mixed radix representation to standard representation by evaluation with Horner scheme.

## Uniqueness of the Chinese Remainder problem

The Chinese Remainder Problem can be uniquely solved and can be transferred from the domain  $\mathbb{Z} / \prod_{i=0}^n l_i$  to  $\mathbb{Z}$  if all moduli  $m_0, \dots, m_n$  are pairwise prime and  $a \leq u \leq a + m$  with  $m = \prod_{i=0}^n m_i$  for any fixed integer  $a \in \mathbb{Z}$ .

## Inverting evaluation homomorphisms with Newton Interpolation

The **polynomial interpolation problem** is stated as follows:

Let  $D$  be a domain of polynomials over a coefficient field  $R$ . Given ideals  $\langle x - \alpha_0 \rangle, \langle x - \alpha_1 \rangle, \dots, \langle x - \alpha_n \rangle$  where  $\alpha_i \in R, 0 \leq i \leq n$  and given corresponding residues  $s_i \in D, 0 \leq i \leq n$ , find a polynomial  $u(x) \in D[x]$  such that

$$u(x) \equiv s_i \pmod{x - \alpha_i}, 0 \leq i \leq n.$$

## Inverting evaluation homomorphisms with Newton Interpolation

The **polynomial interpolation problem** is stated as follows:

Let  $D$  be a domain of polynomials over a coefficient field  $R$ . Given ideals  $\langle x - \alpha_0 \rangle, \langle x - \alpha_1 \rangle, \dots, \langle x - \alpha_n \rangle$  where  $\alpha_i \in R, 0 \leq i \leq n$  and given corresponding residues  $s_i \in D, 0 \leq i \leq n$ , find a polynomial  $u(x) \in D[x]$  such that

$$u(x) \equiv s_i \pmod{x - \alpha_i}, 0 \leq i \leq n.$$

$\alpha_1, \dots, \alpha_n$  are also called interpolation points.

## Inverting evaluation homomorphisms with Newton Interpolation

The **polynomial interpolation problem** is stated as follows:

Let  $D$  be a domain of polynomials over a coefficient field  $R$ . Given ideals  $\langle x - \alpha_0 \rangle, \langle x - \alpha_1 \rangle, \dots, \langle x - \alpha_n \rangle$  where  $\alpha_i \in R, 0 \leq i \leq n$  and given corresponding residues  $s_i \in D, 0 \leq i \leq n$ , find a polynomial  $u(x) \in D[x]$  such that

$$u(x) \equiv s_i \pmod{x - \alpha_i}, 0 \leq i \leq n.$$

$\alpha_1, \dots, \alpha_n$  are also called interpolation points.

The polynomial interpolation problem can be uniquely solved with Newton interpolation if  $\deg(u(x)) \leq n$  with  $n + 1$  distinct interpolation points.

General background

Chinese Remainder Algorithm and Newton Interpolation

**The Hensel lifting**

Multivariate Hensel lifting

## The factorization problem

We consider the following problem:

Given a polynomial  $a(x)$ , we look for two polynomials  $u(x)$ ,  $w(x)$  such that

$$a(x) = u(x) \cdot w(x)$$

## The factorization problem

We consider the following problem:

Given a polynomial  $a(x)$ , we look for two polynomials  $u(x)$ ,  $w(x)$  such that

$$a(x) = u(x) \cdot w(x)$$

Reformulated, we are looking for a root of the function

$$F(u, w) = a(x) - u(x)w(x)$$

Assume, we found a solution  $u^{(1)}$  and  $w^{(1)}$  in  $R/I$ .

We now invert a homomorphism  $\theta_I : R \rightarrow R/I$  lifting two polynomials  $u$  and  $v$  as solution by an iterative method.

## The factorization problem

We consider the following problem:

Given a polynomial  $a(x)$ , we look for two polynomials  $u(x)$ ,  $w(x)$  such that

$$a(x) = u(x) \cdot w(x)$$

Reformulated, we are looking for a root of the function

$$F(u, w) = a(x) - u(x)w(x)$$

Assume, we found a solution  $u^{(1)}$  and  $w^{(1)}$  in  $R/I$ .

We now invert a homomorphism  $\theta_I : R \rightarrow R/I$  lifting two polynomials  $u$  and  $v$  as solution by an iterative method.

This iterative method is called the Hensel construction.

## Ideal-adic representation

### Definition 10

Let  $I$  be an given ideal. A polynomial  $u$  is in **ideal-adic representation** when it is in the form

$$u^{(1)} + \Delta u^{(1)} + \Delta u^{(2)} + \dots + \Delta u^{(d)}$$

where  $u^{(1)} \in R/I$   
and  $\Delta u^{(k)} \in I^k/I^{k+1}$  for  $1 \leq k \leq d$   
and  $d$  is maximal total degree of  $u$  with respect to  $I$ .

We define  $u^{(k+1)} = u^{(1)} + \Delta u^{(1)} + \dots + \Delta u^{(k)}$ .

## Ideal-adic approximation

### Definition 11

Let  $I \subset R$  be an ideal. For a given polynomial  $a \in R$ , a polynomial  $b \in R$  is an **order  $k$  ideal-adic approximation to  $a$**  with respect to  $I$  if

$$a \equiv b \pmod{I^k}$$

The **error** approximating  $a$  by  $b$  is  $a - b \in I^k$ .

### Example 12

The polynomial  $u^{(k)}$  is an order  $k$  ideal-adic approximation to the polynomial  $u$ .

## The iteration step of the Hensel construction

- ▶ Assume, we already have a pair of order  $k$  approximations  $u^{(k)}$  and  $w^{(k)}$ , so  $F(u^{(k)}, w^{(k)}) \equiv 0 \pmod{I^k}$ .

## The iteration step of the Hensel construction

- ▶ Assume, we already have a pair of order  $k$  approximations  $u^{(k)}$  and  $w^{(k)}$ , so  $F(u^{(k)}, w^{(k)}) \equiv 0 \pmod{I^k}$ .
- ▶ We want to get  $k+1$  order approximations  $u^{(k+1)} = u^{(k)} + \Delta u^{(k)}$  and  $w^{(k+1)} = w^{(k)} + \Delta w^{(k)}$

## The iteration step of the Hensel construction

- ▶ Assume, we already have a pair of order  $k$  approximations  $u^{(k)}$  and  $w^{(k)}$ , so  $F(u^{(k)}, w^{(k)}) \equiv 0 \pmod{I^k}$ .
- ▶ We want to get  $k+1$  order approximations  $u^{(k+1)} = u^{(k)} + \Delta u^{(k)}$  and  $w^{(k+1)} = w^{(k)} + \Delta w^{(k)}$
- ▶ So  $F(u^{(k)} + \Delta u^{(k)}, w^{(k)} + \Delta w^{(k)}) \equiv 0 \pmod{I^{k+1}}$

## The iteration step of the Hensel construction

- ▶ Assume, we already have a pair of order  $k$  approximations  $u^{(k)}$  and  $w^{(k)}$ , so  $F(u^{(k)}, w^{(k)}) \equiv 0 \pmod{I^k}$ .
- ▶ We want to get  $k+1$  order approximations  $u^{(k+1)} = u^{(k)} + \Delta u^{(k)}$  and  $w^{(k+1)} = w^{(k)} + \Delta w^{(k)}$
- ▶ So  $F(u^{(k)} + \Delta u^{(k)}, w^{(k)} + \Delta w^{(k)}) \equiv 0 \pmod{I^{k+1}}$
- ▶  $F(u^{(k)}, w^{(k)}) + \frac{\delta F}{\delta u}(u^{(k)}, w^{(k)})\Delta u^{(k)} + \frac{\delta F}{\delta w}(u^{(k)}, w^{(k)})\Delta w^{(k)} \equiv 0 \pmod{I^{k+1}}$

## The iteration step of the Hensel construction

- ▶ Assume, we already have a pair of order  $k$  approximations  $u^{(k)}$  and  $w^{(k)}$ , so  $F(u^{(k)}, w^{(k)}) \equiv 0 \pmod{I^k}$ .
- ▶ We want to get  $k+1$  order approximations  $u^{(k+1)} = u^{(k)} + \Delta u^{(k)}$  and  $w^{(k+1)} = w^{(k)} + \Delta w^{(k)}$
- ▶ So  $F(u^{(k)} + \Delta u^{(k)}, w^{(k)} + \Delta w^{(k)}) \equiv 0 \pmod{I^{k+1}}$
- ▶  $F(u^{(k)}, w^{(k)}) + \frac{\delta F}{\delta u}(u^{(k)}, w^{(k)})\Delta u^{(k)} + \frac{\delta F}{\delta w}(u^{(k)}, w^{(k)})\Delta w^{(k)} \equiv 0 \pmod{I^{k+1}}$
- ▶ With  $F(u, w) = a - uw$ , we get:  
 $F(u^{(k)}, w^{(k)}) - w^{(k)}\Delta u^{(k)} - u^{(k)}\Delta w^{(k)} \equiv 0 \pmod{I^{k+1}}$

## The iteration step of the Hensel construction

- ▶ Assume, we already have a pair of order  $k$  approximations  $u^{(k)}$  and  $w^{(k)}$ , so  $F(u^{(k)}, w^{(k)}) \equiv 0 \pmod{I^k}$ .
- ▶ We want to get  $k+1$  order approximations  $u^{(k+1)} = u^{(k)} + \Delta u^{(k)}$  and  $w^{(k+1)} = w^{(k)} + \Delta w^{(k)}$
- ▶ So  $F(u^{(k)} + \Delta u^{(k)}, w^{(k)} + \Delta w^{(k)}) \equiv 0 \pmod{I^{k+1}}$
- ▶  $F(u^{(k)}, w^{(k)}) + \frac{\delta F}{\delta u}(u^{(k)}, w^{(k)})\Delta u^{(k)} + \frac{\delta F}{\delta w}(u^{(k)}, w^{(k)})\Delta w^{(k)} \equiv 0 \pmod{I^{k+1}}$
- ▶ With  $F(u, w) = a - uw$ , we get:  
 $F(u^{(k)}, w^{(k)}) - w^{(k)}\Delta u^{(k)} - u^{(k)}\Delta w^{(k)} \equiv 0 \pmod{I^{k+1}}$
- ▶ Finally, we have:  
 $w^{(k)}\Delta u^{(k)} + u^{(k)}\Delta w^{(k)} \equiv F(u^{(k)}, w^{(k)}) \pmod{I^{k+1}}$

## Univariate Hensel lifting

Problem:

Inverting modular homomorphism  $\theta_p : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$

Given polynomials  $a(x) \in \mathbb{Z}[x]$  and  $u^{(1)}(x), w^{(1)}(x) \in \mathbb{Z}_p[x]$  such that

$$a(x) \equiv u_0(x)w_0(x) \pmod{p}$$

calculate  $u(x), w(x) \in \mathbb{Z}_{p^t}[x]$  such that

$$\begin{aligned} F(u, w) &= a(x) - uw = 0 \\ \text{and } u(x) &\equiv u^{(1)}(x) \pmod{p} \\ \text{and } w(x) &\equiv w^{(1)}(x) \pmod{p} \end{aligned}$$

## p-adic representation and approximation

### Definition 13

Let  $I = \langle p \rangle$  be an ideal and let  $R = \mathbb{Z}[x]$ .

A polynomial  $u(x)$  is in its polynomial p-adic representation when it is in the form

$$u^{(1)} + \Delta u^{(1)} + \Delta u^{(2)} + \dots + \Delta u^{(d)}$$

where  $u^{(1)} \in R/I$

and  $\Delta u^{(k)} \in I^k/I^{k+1}$  for  $1 \leq k \leq d$

and  $d$  is maximal total degree of  $u$  with respect to  $I$ .

We define  $u^{(k+1)} = u^{(1)} + \Delta u^{(1)} + \dots + \Delta u^{(k)}$ .

## More specific view at the p-adic representation

$u^{(1)} \in R/I$  is a polynomial with coefficients in  $\mathbb{Z}/p$ .

and the elements  $\Delta u^{(k)}$  can be represented in the following form:

$$\Delta u^{(k)} = u_k(x) \cdot p^k$$

where  $u_k \in \mathbb{Z}_p[x]$  for  $0 \leq k \leq n$ .

Therefore,  $u$  can be written as:

$$u(x) = u_0(x) + u_1(x)p + u_2(x)p^2 + \cdots + u_n(x)p^n.$$

## order $n$ $p$ -adic approximation

### Definition 14

Let  $a(x) \in \mathbb{Z}[x]$  be a given polynomial. A polynomial  $b(x) \in \mathbb{Z}[x]$  is called an **order  $n$   $p$ -adic approximation to  $a(x)$**  if

$$a(x) \equiv b(x) \pmod{p^n}$$

The **error** in approximating  $a(x)$  by  $b(x)$  is  $a(x) - b(x) \in \mathbb{Z}[x]$ .

### Example 15

$$u(x) = 27x^2 + 11x + 7$$

in polynomial p-adic representation for  $p = 5$ :

$$u(x) = (2x^2 + x + 2) + (2x + 1) \cdot 5 + x^2 \cdot 5^2$$

## The iteration step of the Hensel lifting

- ▶ We have order  $k$  approximations to  $u(x)$  and  $w(x)$ , called  $u^{(k)}$  and  $w^{(k)}$ .
- ▶ Remember that
$$w^{(k)}\Delta u^{(k)} + u^{(k)}\Delta w^{(k)} \equiv F(u^{(k)}, w^{(k)}) \pmod{I^{k+1}}$$
- ▶ Solve  $w_0(x)u_k(x) + u_0(x)w_k(x) = \theta_p \left( \frac{a(x) - u^{(k)}w^{(k)}}{p^k} \right)$  with Extended Euclidean Algorithm
- ▶ Define  $u^{(k+1)} = u^{(k)} + u_k(x)p^k$  and  $w^{(k+1)} = w^{(k)} + w_k(x)p^k$  and repeat iteration.

## Uniqueness of the Hensel construction

If  $a(x) \in \mathbb{Z}[x]$  is monic and  $u^{(1)}$  and  $w^{(1)}$  are monic and relative prime, then there are uniquely determined monic polynomial factors  $u^{(k)}$  and  $w^{(k)}$  for any  $k \geq 1$ .

## Uniqueness of the Hensel construction

If  $a(x) \in \mathbb{Z}[x]$  is monic and  $u^{(1)}$  and  $w^{(1)}$  are monic and relative prime, then there are uniquely determined monic polynomial factors  $u^{(k)}$  and  $w^{(k)}$  for any  $k \geq 1$ .

For a non-monic polynomial  $a(x)$ , some pre- and postprocessing has to be done.

## Example for univariate Hensel lifting

- ▶ Factorizing  $a(x) = x^3 + 10x^2 - 432x + 5040$  with  $p = 5$

## Example for univariate Hensel lifting

- ▶ Factorizing  $a(x) = x^3 + 10x^2 - 432x + 5040$  with  $p = 5$
- ▶ Applying  $\theta_5(a(x)) = x^3 - 2x = x(x^2 - 2) = u^{(1)} \cdot w^{(1)}$

## Example for univariate Hensel lifting

- ▶ Factorizing  $a(x) = x^3 + 10x^2 - 432x + 5040$  with  $p = 5$
- ▶ Applying  $\theta_5(a(x)) = x^3 - 2x = x(x^2 - 2) = u^{(1)} \cdot w^{(1)}$
- ▶ First iteration of Hensel construction

## Example for univariate Hensel lifting

- ▶ Factorizing  $a(x) = x^3 + 10x^2 - 432x + 5040$  with  $p = 5$
- ▶ Applying  $\theta_5(a(x)) = x^3 - 2x = x(x^2 - 2) = u^{(1)} \cdot w^{(1)}$
- ▶ First iteration of Hensel construction
  - ▶ Calculate  $\theta_5\left(\frac{a(x) - u^{(1)}w^{(1)}}{5}\right) = 2x^2 - x - 2$

## Example for univariate Hensel lifting

- ▶ Factorizing  $a(x) = x^3 + 10x^2 - 432x + 5040$  with  $p = 5$
- ▶ Applying  $\theta_5(a(x)) = x^3 - 2x = x(x^2 - 2) = u^{(1)} \cdot w^{(1)}$
- ▶ First iteration of Hensel construction
  - ▶ Calculate  $\theta_5\left(\frac{a(x) - u^{(1)}w^{(1)}}{5}\right) = 2x^2 - x - 2$
  - ▶ Solve  $(x^2 - 2)u_1(x) + xw_1(x) = 2x^2 - x - 2$

## Example for univariate Hensel lifting

- ▶ Factorizing  $a(x) = x^3 + 10x^2 - 432x + 5040$  with  $p = 5$
- ▶ Applying  $\theta_5(a(x)) = x^3 - 2x = x(x^2 - 2) = u^{(1)} \cdot w^{(1)}$
- ▶ First iteration of Hensel construction
  - ▶ Calculate  $\theta_5\left(\frac{a(x) - u^{(1)}w^{(1)}}{5}\right) = 2x^2 - x - 2$
  - ▶ Solve  $(x^2 - 2)u_1(x) + xw_1(x) = 2x^2 - x - 2$
  - ▶  $u_1(x) = 1; w_1(x) = x - 1$

## Example for univariate Hensel lifting

- ▶ Factorizing  $a(x) = x^3 + 10x^2 - 432x + 5040$  with  $p = 5$
- ▶ Applying  $\theta_5(a(x)) = x^3 - 2x = x(x^2 - 2) = u^{(1)} \cdot w^{(1)}$
- ▶ First iteration of Hensel construction
  - ▶ Calculate  $\theta_5\left(\frac{a(x) - u^{(1)}w^{(1)}}{5}\right) = 2x^2 - x - 2$
  - ▶ Solve  $(x^2 - 2)u_1(x) + xw_1(x) = 2x^2 - x - 2$
  - ▶  $u_1(x) = 1; w_1(x) = x - 1$
  - ▶  $u^{(2)} = u^{(1)} + u_1(x) \cdot p = x + 5$   
 $w^{(2)} = w^{(1)} + w_1(x) \cdot p = x^2 + 5x - 7$

## Example for univariate Hensel lifting

- ▶ Factorizing  $a(x) = x^3 + 10x^2 - 432x + 5040$  with  $p = 5$
- ▶ Applying  $\theta_5(a(x)) = x^3 - 2x = x(x^2 - 2) = u^{(1)} \cdot w^{(1)}$
- ▶ First iteration of Hensel construction
  - ▶ Calculate  $\theta_5\left(\frac{a(x) - u^{(1)}w^{(1)}}{5}\right) = 2x^2 - x - 2$
  - ▶ Solve  $(x^2 - 2)u_1(x) + xw_1(x) = 2x^2 - x - 2$
  - ▶  $u_1(x) = 1; w_1(x) = x - 1$
  - ▶  $u^{(2)} = u^{(1)} + u_1(x) \cdot p = x + 5$   
 $w^{(2)} = w^{(1)} + w_1(x) \cdot p = x^2 + 5x - 7$
- ▶ Next iterations:

## Example for univariate Hensel lifting

- ▶ Factorizing  $a(x) = x^3 + 10x^2 - 432x + 5040$  with  $p = 5$
- ▶ Applying  $\theta_5(a(x)) = x^3 - 2x = x(x^2 - 2) = u^{(1)} \cdot w^{(1)}$
- ▶ First iteration of Hensel construction
  - ▶ Calculate  $\theta_5\left(\frac{a(x) - u^{(1)}w^{(1)}}{5}\right) = 2x^2 - x - 2$
  - ▶ Solve  $(x^2 - 2)u_1(x) + xw_1(x) = 2x^2 - x - 2$
  - ▶  $u_1(x) = 1; w_1(x) = x - 1$
  - ▶  $u^{(2)} = u^{(1)} + u_1(x) \cdot p = x + 5$   
 $w^{(2)} = w^{(1)} + w_1(x) \cdot p = x^2 + 5x - 7$
- ▶ Next iterations:

## Example for univariate Hensel lifting

- ▶ Factorizing  $a(x) = x^3 + 10x^2 - 432x + 5040$  with  $p = 5$
- ▶ Applying  $\theta_5(a(x)) = x^3 - 2x = x(x^2 - 2) = u^{(1)} \cdot w^{(1)}$
- ▶ First iteration of Hensel construction
  - ▶ Calculate  $\theta_5\left(\frac{a(x) - u^{(1)}w^{(1)}}{5}\right) = 2x^2 - x - 2$
  - ▶ Solve  $(x^2 - 2)u_1(x) + xw_1(x) = 2x^2 - x - 2$
  - ▶  $u_1(x) = 1; w_1(x) = x - 1$
  - ▶  $u^{(2)} = u^{(1)} + u_1(x) \cdot p = x + 5$   
 $w^{(2)} = w^{(1)} + w_1(x) \cdot p = x^2 + 5x - 7$
- ▶ Next iterations:

Iter	$u_k$	$w_k$	$u^{(k)}(x)$	$w^{(k)}(x)$	$e(x)$
0	-	-	$x$	$x^2 - 2$	$10x^2 - 430x + 5040$
1	1	$x - 1$	$x + 5$	$x^2 + 5x - 7$	$-450x + 5075$
2	1	$-x + 2$	$x + 30$	$x^2 - 20x + 43$	$125x + 3750$
3	0	1	$x + 30$	$x^2 - 20x + 168$	0

General background

Chinese Remainder Algorithm and Newton Interpolation

The Hensel lifting

**Multivariate Hensel lifting**

## Multivariate Hensel lifting

Problem:

Inverting multivariate evaluation homomorphism

$$\theta_I : \mathbb{Z}[x_1, \dots, x_v] \rightarrow \mathbb{Z}[x_1]$$

Given polynomials  $a(x) \in \mathbb{Z}[x_1, \dots, x_v]$  and

$u^{(1)}(x_1), w^{(1)}(x_1) \in R/I$  such that

$$a(x_1) \equiv u^{(1)}(x_1)w^{(1)}(x_1) \pmod{I}$$

calculate  $u(x_1, \dots, x_v), w(x_1, \dots, x_v) \in R[x_1, \dots, x_v]$  such that

$$F(u, w) = a(x) - uw = 0$$

$$\text{and } u(x_1, \dots, x_v) \equiv u^{(1)}(x_1) \pmod{I}$$

$$\text{and } w(x_1, \dots, x_v) \equiv w^{(1)}(x_1) \pmod{I}$$

## Multivariate Hensel lifting

Problem:

Inverting multivariate evaluation homomorphism

$$\theta_I : \mathbb{Z}[x_1, \dots, x_v] \rightarrow \mathbb{Z}[x_1]$$

Given polynomials  $a(x) \in \mathbb{Z}[x_1, \dots, x_v]$  and

$u^{(1)}(x_1), w^{(1)}(x_1) \in R/I$  such that

$$a(x_1) \equiv u^{(1)}(x_1)w^{(1)}(x_1) \pmod{I}$$

calculate  $u(x_1, \dots, x_v), w(x_1, \dots, x_v) \in R[x_1, \dots, x_v]$  such that

$$F(u, w) = a(x) - uw = 0$$

$$\text{and } u(x_1, \dots, x_v) \equiv u^{(1)}(x_1) \pmod{I}$$

$$\text{and } w(x_1, \dots, x_v) \equiv w^{(1)}(x_1) \pmod{I}$$

The ideal  $I$  has the form  $\langle x_2 - \alpha_2, \dots, x_v - \alpha_v \rangle$ .

## Ideal-adic representation

Analogously to p-adic representation, we can define a ideal-adic representation for an ideal  $I$ .

### Definition 16

Let  $I = \langle x_2 - \alpha_2, x_3 - \alpha_3, \dots, x_v - \alpha_v \rangle$  be an given ideal. A polynomial  $u(x_1, \dots, x_v)$  is in **ideal-adic representation** when it is in the form

$$u^{(1)} + \Delta u^{(1)} + \Delta u^{(2)} + \dots + \Delta u^{(d)}$$

$$\text{where } u^{(1)} \in R/I$$

$$\text{and } \Delta u^{(k)} \in I^k/I^{k+1} \text{ for } 1 \leq k \leq d$$

and  $d$  is maximal total degree of  $u$  with respect to  $I$ .

We define  $u^{(k+1)} = u^{(1)} + \Delta u^{(1)} + \dots + \Delta u^{(k)}$ .

## More specific view at the ideal-adic representation

The term  $u^{(1)}$  is  $u(x_1, \alpha_2, \alpha_3, \dots, \alpha_v)$ .

A term  $\Delta u^{(k)} \in I^k$  is a sum of all terms with total degree of  $k$  with respect to  $I$ , so it has the form

$$\underbrace{\sum_{i_1=2}^v \sum_{i_2=i_1}^v \cdots \sum_{i_k=i_{k-1}}^v}_{k \text{ sums}} \underbrace{u_i^{(k)}(x_1)}_{\text{coefficient}} \underbrace{(x_{i_1} - \alpha_{i_1}) \cdot (x_{i_2} - \alpha_{i_2}) \cdot \cdots \cdot (x_{i_k} - \alpha_{i_k})}_{k \text{ factors}}$$

where  $2 \leq i_1 \leq \dots \leq i_k \leq v$

and  $i$  is a vector with  $k$  entries of indices  $= (i_1, i_2, \dots, i_k)$

## Ideal-adic approximation

### Definition 17

Let  $I$  be an ideal in  $\mathbb{Z}[x_1, \dots, x_v]$ . For a given polynomial  $a \in \mathbb{Z}[x_1, \dots, x_v]$ , a polynomial  $b \in \mathbb{Z}[x_1, \dots, x_v]$  is an **order  $k$  ideal-adic approximation to  $a$**  with respect to  $I$  if

$$a \equiv b \pmod{I^k}$$

The **error** is approximating  $a$  by  $b$  is  $a - b \in I^k$ .

### Example 18

The polynomial  $u^{(k)}$  is an order  $k$  ideal-adic approximation to the polynomial  $u$ .

## Iteration step for multivariate Hensel construction

From an  $k$  order ideal-adic approximation  $u^{(k)}$  and  $w^{(k)}$ , we calculate an  $k+1$  order ideal-adic  $u^{(k+1)}$  and  $w^{(k+1)}$  approximation.

- ▶ The update formula

$$w^{(k)} \Delta u^{(k)} + u^{(k)} \Delta w^{(k)} = (a(x_1, \dots, x_v) - u^{(k)} w^{(k)}) \bmod I^{k+1}$$

- ▶ Represent  $a(x_1, \dots, x_v) - u^{(k)} w^{(k)} =$

$$\sum_{i_1=2}^v \sum_{i_2=i_1}^v \cdots \sum_{i_k=i_{k-1}}^v c_i^{(k)}(x_1) (x_{i_1} - \alpha_{i_1}) \cdot \cdots \cdot (x_{i_k} - \alpha_{i_k})$$

- ▶ Separate and simplify equation to

$$w^{(1)} u_i(x_1) + u^{(1)} w_i(x_1) = c_i(x_1)$$

- ▶ Solve with Extended Euclidean Algorithm

# Outlook

We did not discuss

- ▶ Leading Coefficient Problem in the univariate Hensel Construction
- ▶ Bad performance because of the Bad-Zero Problem
- ▶ Using sparseness of solution to improve Hensel Construction
- ▶ Quadratic Iteration, also known as Zassenhaus Construction



Keith O. Geddes, Stephen R. Czapor, and George Labahn.

*Algorithms for computer algebra.*

Kluwer Academic Publishers, Norwell, MA, USA, 1992.



Alfonso Miola and David Y. Y. Yun.

Computational aspects of Hensel-type univariate polynomial greatest common divisor algorithms.

8(3):46–54, August 1974.



D. Y. Y. Yun.

*The Hensel Lemma in algebraic manipulation.*

PhD thesis, M.I.T. , Reprint Garland Publ. NY, 1980, 1974.



Richard Zippel.

Newton's iteration and the sparse hensel algorithm (extended abstract).

In *SYMSAC '81: Proceedings of the fourth ACM symposium on Symbolic and algebraic computation*, pages 68–72, New York, NY, USA, 1981. ACM Press.