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

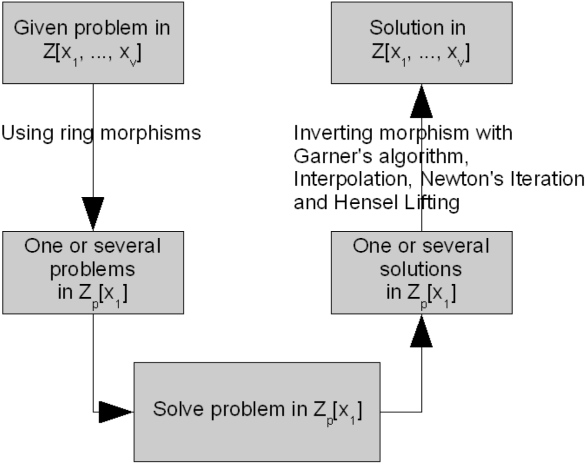
Computing with polynomials: Hensel constructions

Lukas Bulwahn

Fakultät für Informatik
TU München

March 23, 2007

Motivation and Overview



Definition 1 (ring morphism)

Let R and R' be two rings. Then a mapping $\theta : R \rightarrow R'$ is called a ring morphism 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 morphism)

Let R and R' be two rings. Then a mapping $\theta : R \to R'$ is called a ring morphism 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)

$\theta_m : Z[x_1, \ldots, x_v] \rightarrow Z_m[x_1, \ldots, x_v]$
is defined for a fixed $m \in Z$ by:

- $\theta_m(x_i) = x_i \qquad$ for $1 \leq i \leq v$
- $\theta_m(a) = rem(a, m) \qquad$ for all coefficients $a \in Z$

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

Example 2 (Modular Homomorphism)

$\theta_m : Z[x_1, \ldots, x_v] \rightarrow Z_m[x_1, \ldots, x_v]$
is defined for a fixed $m \in Z$ by:

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

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

for $a(x, y) = 2xy + 7x - y^2 + 8 \in Z[x, y]$:
$\theta_5(a) = 2xy + 2x - y^2 - 2 \in Z_5[x, y]$

Example 3 (Evaluation Homomorphism)

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

Example 3 (Evaluation Homomorphism)

$\theta_{x_i-\alpha} : D[x_1, \ldots, x_v] \to D[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_v]$
is defined for a particular indeterminate x_i and a fixed $\alpha \in D$ by:
$\theta_{x_i-\alpha}(a(x_1, \ldots, x_v)) = a(x_1, \ldots, x_{i-1}, \alpha, x_{i+1}, \ldots, x_v)$
"substitute α for x_i"

for $a(x, y) = 2xy + 7x + y^2 + 8 \in Z[x, y]$:
$\theta_{x-2}(a) = 4y + 14 + y^2 + 8 \in Z[y]$

Characterization of morphisms

Ring morphisms 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. $a - b \in R$ for all $a, b \in I$
2. $ar \in I$ for all $a \in I$ and for all $r \in R$.

Example 5 (Examples for ideals)

Example 5 (Examples for ideals)

- $< m >\subset Z = \{m \cdot r : r = 0, \pm 1, \pm 2, \ldots\}$

Example 5 (Examples for ideals)

- $< m > \subset Z = \{m \cdot r : r = 0, \pm 1, \pm 2, \ldots\}$
- $< 4 >= \{0, \pm 4, \pm 8, \pm 12, \ldots\}$

Example 5 (Examples for ideals)

- $< m > \subset Z = \{m \cdot r : r = 0, \pm 1, \pm 2, \ldots\}$
- $< 4 > = \{0, \pm 4, \pm 8, \pm 12, \ldots\}$
- $< p(x) > \subset Z[x] = \{p(x) \cdot a(x) : a(x) \in Z[x]\}$

Example 5 (Examples for ideals)

- $< m > \subset Z = \{m \cdot r : r = 0, \pm 1, \pm 2, \ldots\}$
- $< 4 >= \{0, \pm 4, \pm 8, \pm 12, \ldots\}$
- $< p(x) > \subset Z[x] = \{p(x) \cdot a(x) : a(x) \in Z[x]\}$
- $< x - 2 >= \{(x - 2) \cdot a(x) : a(x) \in Z[x]\}$

Correspondence of ideals and morphisms

We note that:

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

Correspondence of ideals and morphisms

We note that:

- Let R and R' be commutative rings. The kernel K of a morphism $\theta : R \rightarrow R'$ 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.

Correspondence of ideals and morphisms

We note that:

- Let R and R' be commutative rings. The kernel K of a morphism $\theta : R \rightarrow R'$ 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, morphism can be constructed and notated using their ideal.

Correspondence of ideals and morphisms

We note that:

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

Correspondence of ideals and morphisms

Example 6

Correspondence of ideals and morphisms

Example 6

- The morphism θ_4 has the kernel/ideal $< 4 >$.

Correspondence of ideals and morphisms

Example 6

- The morphism θ_4 has the kernel/ideal $< 4 >$.
- The morphism θ_{x-2} has the kernel $< x - 2 >$.

Correspondence of ideals and morphisms

Example 6

- The morphism θ_4 has the kernel/ideal $< 4 >$.
- The morphism θ_{x-2} has the kernel $< x - 2 >$.
- Evaluation of p(x): $p(c) = d$ is isomorph to $d \equiv p(x)\ mod\ (x - c)$.

Correspondence of ideals and morphisms

Example 6

- The morphism θ_4 has the kernel/ideal $< 4 >$.
- The morphism θ_{x-2} has the kernel $< x - 2 >$.
- Evaluation of p(x): $p(c) = d$ is isomorph to $d \equiv p(x)\ mod\ (x - c)$.
- From an "ideal" viewpoint, modular and evalution morphisms are the same.

Operations on ideals

- The ideal $< a_1, a_2, \ldots, a_n >$ is defined as
  $\{a_1 r_1 + \cdots + a_n r_n : r_i \in R\}$
  $a_1, \ldots, a_n \in R$ is called basis.

Operations on ideals

- The ideal $< a_1, a_2, \ldots, a_n >$ is defined as
  $\{a_1 r_1 + \cdots + a_n r_n : r_i \in R\}$
  $a_1, \ldots, a_n \in R$ is called basis.
- For ideal I $= < a_1, \ldots, a_n >$ and $J =< b_1, \ldots, b_m >$:
  the sum of two ideals is $< I, J >=< a_1, \ldots, a_n, b_1, \ldots, b_m >$
  the product of two ideals is
  $I \cdot J =< a_1 b_1, \ldots, a_1 b_m, a_2 b_1, \ldots, a_2 b_m, \ldots, a_n b_1, \ldots, a_n b_m >$
  The i-th power is recursively defined by:
  $I^1 = I$ and $I^i = I \cdot I^{i-1}$ for $i \geq 2$.

Example 7

- $< x, y >$ are all polynomials $a_1x + a_2y$.
- $< x, y > \cdot < x, y >$ are all polynomials $a_1x^2 + a_2xy + a_3y^2$.
- $< x, y >^k$ are all polynomials with terms of total degree k.

General background

Chinese Remainder Algorithm and Newton Interpolation

The Hensel Lifting

Multivariate Hensel lifting

Inverting modular morphisms with Chinese Remainder Algorithm

The Chinese Remainder problem is stated as follows:
Given moduli $m_0, m_1, \ldots, m_n \in Z$ and given corresponding residues $u_i \in Z_{m_i}$, $0 \leq i \leq n$, find an integer $u \in Z$ such that $u \equiv u_i \ mod \ m_i, 0 \leq i \leq n$.

This can be uniquely solved if all moduli are pairwise prime and $a \leq u \leq a + m$ with $m = \prod_{i=0}^{n} m_i$ for any fixed integer $a \in Z$.

The Chinese Remainder Algorithm: Garner's Algorithm

The key to the algorithm:
Express the solution $u \in Z_m$ in mixed radix representation.

Definition 8 (mixed radix representation)

$$u = v_0 + v_1 \cdot m_0 + v_2 \cdot (m_0 m_1) + \cdots + v_n \cdot (\prod_{i=0}^{n-1} m_i)$$

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

The Chinese Remainder Algorithm: Garner's Algorithm

The key to the algorithm:
Express the solution $u \in Z_m$ in mixed radix representation.

Definition 8 (mixed radix representation)

$$u = v_0 + v_1 \cdot m_0 + v_2 \cdot (m_0 m_1) + \cdots + v_n \cdot (\prod_{i=0}^{n-1} m_i)$$

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

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 $i = 0 \cdots n$:

- For $i = 0$: $u = u_0 \ mod \ m_0$
  Choose $v_0 = u_0$.

From modulo equations to mixed radix form

Iteration over $i = 0 \cdots n$:

- For $i = 0$: $u = u_0 \ mod \ m_0$
  Choose $v_0 = u_0$.
- For $i = k$: $v_1, \ldots, v_{k-1}$ are known.
  Solve
  $v_0 + v_1(m_0) + v_2(m_0 m_1) + \cdots + v_k(\prod_{i=0}^{k-1} m_i) \equiv u_k \ mod \ m_k$

From modulo equations to mixed radix form

Iteration over $i = 0 \cdots n$:

- For $i = 0$: $u = u_0 \ mod \ m_0$
  Choose $v_0 = u_0$.
- For $i = k$: $v_1, \ldots, v_{k-1}$ are known.
  Solve
  $v_0 + v_1(m_0) + v_2(m_0 m_1) + \cdots + v_k(\prod_{i=0}^{k-1} m_i) \equiv u_k \ mod \ m_k$

From modulo equations to mixed radix form

Iteration over $i = 0 \cdots n$:

- For $i = 0$: $u = u_0 \ mod \ m_0$
  Choose $v_0 = u_0$.
- For $i = k$: $v_1, \ldots, v_{k-1}$ are known.
  Solve
  $v_0 + v_1(m_0) + v_2(m_0 m_1) + \cdots + v_k(\prod_{i=0}^{k-1} m_i) \equiv u_k \ mod \ m_k$
  $\Longrightarrow v_k \equiv$
  $\left(u_k - \left(v_0 + \cdots + v_{k-1}\left(\prod_{i=0}^{k-2} m_i\right)\right)\right)\left(\prod_{i=0}^{k-1} m_i\right)^{-1} \ mod \ m_k$

From modulo equations to mixed radix form

Iteration over $i = 0 \cdots n$:

- For $i = 0$: $u = u_0 \ mod \ m_0$
  Choose $v_0 = u_0$.
- For $i = k$: $v_1, \ldots, v_{k-1}$ are known.
  Solve
  $v_0 + v_1(m_0) + v_2(m_0 m_1) + \cdots + v_k(\prod_{i=0}^{k-1} m_i) \equiv u_k \ mod \ m_k$
  $\Longrightarrow v_k \equiv$
  $\left(u_k - \left(v_0 + \cdots + v_{k-1}\left(\prod_{i=0}^{k-2} m_i\right)\right)\right)\left(\prod_{i=0}^{k-1} m_i\right)^{-1} \ mod \ m_k$

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

Inverting evaluation morphisms with Newton Interpolation

The polynomial interpolation problem is stated as follows:
Let D be a domain of polynomials over a coefficient field Z_p. Given moduli $x - \alpha_0, x - \alpha_1, \ldots, x - \alpha_n$ where $\alpha_i \in Z_p, 0 \leq i \leq n$ and given corresponding residues $u_i \in D, 0 \leq i \leq n$, find a polynomial $u(x) \in D[x]$ such that $u(x) \equiv u_i \ mod \ x - \alpha_i, 0 \leq i \leq n$.

Inverting evaluation morphisms with Newton Interpolation

The polynomial interpolation problem is stated as follows:
Let D be a domain of polynomials over a coefficient field Z_p. Given moduli $x - \alpha_0, x - \alpha_1, \dots, x - \alpha_n$ where $\alpha_i \in Z_p, 0 \le i \le n$ and given corresponding residues $u_i \in D, 0 \le i \le n$, find a polynomial $u(x) \in D[x]$ such that $u(x) \equiv u_i \ mod \ x - \alpha_i, 0 \le i \le n$.

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

Inverting evaluation morphisms with Newton Interpolation

The polynomial interpolation problem is stated as follows:
Let D be a domain of polynomials over a coefficient field Z_p. Given moduli $x - \alpha_0, x - \alpha_1, \ldots, x - \alpha_n$ where $\alpha_i \in Z_p, 0 \leq i \leq n$ and given corresponding residues $u_i \in D, 0 \leq i \leq n$, find a polynomial $u(x) \in D[x]$ such that $u(x) \equiv u_i \ mod \ x - \alpha_i, 0 \leq i \leq n$.

$\alpha_1, \ldots, \alpha_n$ 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.

Inverting morphisms with Garner's algorithm and Newton interpolation

Problem: To invert a morphism for a polynomial with v invariants and maximal degree d, we would need to solve $O((d+1)^{v-1})$ image problems.

Instead of solving exponential many problems, we would like to solve one problem in $Z_p[x]$ and "lift" it to $Z_p[x_1, \ldots, x_v]$.

p-adic representation and approximation

Definition 10

A polynomial $u(x)$ is in its polynomial p-adic representation when it is in the form $u(x) = u_0(x) + u_1(x)p + u_2(x)p^2 + \cdots + u_n(x)p^n$.

Definition 11

Let $a(x) \in Z[x]$ be a given polynomial. A polynomial $b(x) \in Z[x]$ is called an order n p-adic approximation to a(x) if
$a(x) \equiv b(x)\ mod\ p^n$
The error in approximating a(x) by b(x) is $a(x) - b(x) \in Z[x]$.

Example 12

$u(x) = 27x^2 + 11x + 7$
in polynomial p-adic representation for $p = 5$:
$u(x) = (2x^2 + x + 2) + (2x + 1) \cdot 5 + x^2 \cdot 5^2$

The 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 $u^{(0)}$ and $w^{(0)}$ in $Z_p[x_1]$.
We now invert a homomorphism $\theta_{I,p} : Z[x_1, \ldots, x_v] \rightarrow Z_p[x_1]$ 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 $u^{(0)}$ and $w^{(0)}$ in $Z_p[x_1]$.
We now invert a homomorphism $\theta_{I,p} : Z[x_1, \ldots, x_v] \rightarrow Z_p[x_1]$ lifting two polynomials u and v as solution by an iterative method.
This iterative method is called the Hensel Construction.

The Iteration Step of the Hensel Construction

- Assume, we already have a pair of approximations $u^{(k)}$ and $w^{(k)}$.
- Solve $F(u^{(k)} + \Delta u^{(k)}, w^{(k)} + \Delta w^{(k)}) \approx 0$
- Leads to $\frac{\delta F}{\delta u}(u^{(k)}, w^{(k)})\Delta u^{(k)} + \frac{\delta F}{\delta w}(u^{(k)}, w^{(k)})\Delta w^{(k)} = -F(u^{(k)}, w^{(k)})$
- Get better approximations $u^{(k+1)} = u^{(k)} + \Delta u^{(k)}$ and $w^{(k+1)} = w^{(k)} + \Delta w^{(k)}$

Univariate Hensel Lifting

Problem:
Inverting modular homomorphism $\theta_p : Z[x] \rightarrow Z_p[x]$

Given polynomials $a(x) \in Z[x]$ and $u_0(x), w_0(x) \in Z_p[x]$ such that

$$a(x) \equiv u_0(x)w_0(x) \ mod \ p$$

calculate $u(x), w(x) \in Z[x]$ such that

$$F(u, v) = a(x) - uw = 0$$
$$\text{and } u(x) \equiv u_0(x) \ mod \ p$$
$$\text{and } w(x) \equiv w_0(x) \ mod \ p$$

The Iteration Step of the Hensel lifting

- We have order k approximations to $u(x)$ and $w(x)$, called $u^{(k)}$ and $w^{(k)}$.
- 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 $a(x) \in Z[x]$ is monic and $u^{(1)}$ and $w^{(1)}$ are monic and relative prime, then there are uniquely determined monic polynomials factors $u^{(k)}$ and $w^{(k)}$ for any $k \geq 1$.

Uniqueness of the Hensel Construction

If $a(x) \in Z[x]$ is monic and $u^{(1)}$ and $w^{(1)}$ are monic and relative prime, then there are uniquely determined monic polynomials 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 $p = 5$
- Applying $\theta_5(a(x)) = x^3 - 2x = x(x^2 - 2) = u^{(1)} \cdot w^{(1)}$
- First iteration of Hensel construction
  - Calculate $\theta_5(\frac{a(x) - u^{(1)} w(1)}{5}) = 2x^2 - x - 2$
  - Solve $(x^2 - 2)u_1(x) + xw_1(x) = 2x^2 - x - 2$
  - $u_1(x) = 1; w_1(x) = x - 1$
  - $u^{(2)} = u^{(1)} + u_1(x) \cdot p = x + 5$
    $w^{(2)} = w^{(1)} + w_1(x) \cdot p = x^2 + 5 - 7$
- 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
$\theta_I : Z[x_1, \dots, x_v] \to Z[x_1]$

Given polynomials $a(x) \in Z[x_1, \dots, x_v]$ and
$u^{(1)}(x), w^{(1)}(x) \in Z_{p^t}[x_1]$ such that

$$a(x) \equiv u_0(x)w_0(x) \ mod \ I$$

calculate $u(x_1, \dots, x_v), w(x_1, \dots, x_v) \in Z_{p^t}[x_1, \dots, x_v]$ such that

$$a(x) - uw \equiv 0 \ mod \ p^t$$
$$\text{and } u(x_1, \dots, x_v) \equiv u^{(1)}(x_1) \ mod \ < I, p^t >$$
$$\text{and } w(x_1, \dots, x_v) \equiv w^{(1)}(x_1) \ mod \ < I, p^t >$$

Multivariate Hensel lifting

Problem:
Inverting multivariate evaluation homomorphism
$\theta_I : Z[x_1, \ldots, x_v] \to Z[x_1]$

Given polynomials $a(x) \in Z[x_1, \ldots, x_v]$ and
$u^{(1)}(x), w^{(1)}(x) \in Z_{p^t}[x_1]$ such that

$$a(x) \equiv u_0(x)w_0(x) \ mod \ I$$

calculate $u(x_1, \ldots, x_v), w(x_1, \ldots, x_v) \in Z_{p^t}[x_1, \ldots, x_v]$ such that

$$a(x) - uw \equiv 0 \ mod \ p^t$$
$$\text{and } u(x_1, \ldots, x_v) \equiv u^{(1)}(x_1) \ mod \ < I, p^t >$$
$$\text{and } w(x_1, \ldots, x_v) \equiv w^{(1)}(x_1) \ mod \ < I, p^t >$$

The ideal I has the form $< x_2 - \alpha_2, \ldots, x_v - \alpha_v >$.

Ideal-adic representation

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

Definition 13

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

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

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

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

More specific view at the Ideal-adic Representation

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

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

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

where $2 \leq i_1, \ldots, i_k \leq v$
and i is a vector with k entries of indices $= (i_1, i_2, \ldots, i_k)$

Ideal-adic approximation

Definition 14

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

$$a \equiv b \ mod \ I^k$$

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

Example 15

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 $w^{(k)}\Delta u^{(k)} + u^{(k)}\Delta w^{(k)} = (a(x_1, \ldots, x_v) - u^{(k)}w^{(k)}) \ mod \ < I^k + 1, p^t >$
- Represent $a(x_1, \ldots, x_v) - u^{(k)}w^{(k)} = \sum_{i_1=2}^{v} \sum_{i_2=i_1}^{v} \cdots \sum_{i_k=i_{k-1}}^{v} c_i^{(k)}(x_1)(x_{i_1} - \alpha_{i_1}) \cdot \ \cdots \ \cdot (x_{i_k} - \alpha_{i_k})$
- Separate and simplify equation to $w^{(1)}u_i(x_1) + u^{(1)}w_i(x_1) = c_i(x_1) \ mod \ p^t$
- 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.