# Hensel Algorithms

Johannes Mittmann

mittmann@in.tum.de

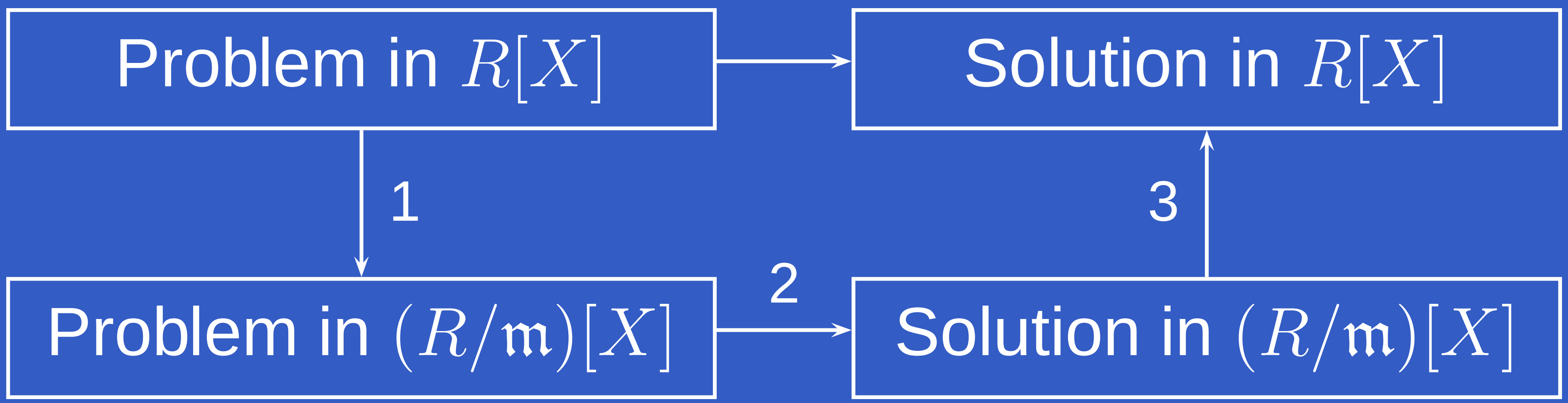
Zentrum Mathematik

Technische Universität München (TUM)

# Overview

- Introduction
- $\mathfrak{m}$-adic Completions
- One Dimensional Iteration
- Multidimensional Iteration
- Hensel's Lemma
- Sparse Hensel Algorithm

# Introduction




- *One* image problem modulo $\mathfrak{m}$
- Lift solution modulo $\mathfrak{m}^{2^k}$

# Newton's Iteration

$f : I \to \mathbb{R}$.

$$f(x) = f(a^{(k)}) + f'(a^{(k)})(x - a^{(k)}) + \mathcal{O}\left((x - a^{(k)})^2\right).$$

$$0 \approx f(a^{(k)}) + f'(a^{(k)})(a - a^{(k)}).$$

$$\boxed{a^{(k+1)} = a^{(k)} - \frac{f(a^{(k)})}{f'(a^{(k)})}}$$

# Analytical vs. $\mathfrak{m}$-adic Iteration

| | analytical | $\mathfrak{m}$-adic |
|---|---|---|
| valuation | $\lvert\cdot\rvert$ | $\lVert\cdot\rVert_{\mathfrak{m}}$ |
| basic domain | $\mathbb{Q}$ | $R$ |
| completion | $\mathbb{R}$ | $R_{\mathfrak{m}}$ |
| iteration | infinite | finite |
| convergence | depends on $a^{(0)}$ | guaranteed |

# Inverse Limit

**Definition.** $\{R_n\}$ sequence of rings with homomorphisms $\{\theta_n\}$:

$$\cdots \xleftarrow{\theta_{n-2}} R_{n-1} \xleftarrow{\theta_{n-1}} R_n \xleftarrow{\theta_n} R_{n+1} \xleftarrow{\theta_{n+1}} \cdots .$$

- A sequence $\{a_n\}$, $a_n \in R_n$, is *coherent*, if

$$\theta_n(a_{n+1}) = a_n \quad \forall n.$$

- Ring of coherent sequences: *inverse limit* of $\{R_n\}$,

$$\hat{R} := \lim_{\longleftarrow} R_n.$$

# $\mathfrak{m}$-adic Completion

$R$ commutative ring, $\mathfrak{m}$ ideal of $R$.
$\mathfrak{m}^{n+1} \subset \mathfrak{m}^n \implies$ canonical map

$$\theta_n : R/\mathfrak{m}^{n+1} \to R/\mathfrak{m}^n, \quad x + \mathfrak{m}^{n+1} \mapsto x + \mathfrak{m}^n.$$

**Definition.** The $\mathfrak{m}$-*adic completion* of $R$ is the inverse limit of $\{R/\mathfrak{m}^n\}$:

$$R_{\mathfrak{m}} := \varprojlim R/\mathfrak{m}^n.$$

# Examples of Completions

- $p$-adic integers:

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/(p)^n.$$

- Formal power series in $k$ variables:

$$R[[X_1, \ldots, X_k]] = \varprojlim R[X_1, \ldots, X_k]/(X_1, \ldots, X_k)^n.$$

# Correspondence $R \leftrightarrow R_{\mathfrak{m}}$

$$x \in R \iff x \in R_{\mathfrak{m}} \text{ ?}$$

Canonical map

$$\theta : R \to R_{\mathfrak{m}}, \quad x \mapsto \{x + \mathfrak{m}^n\}.$$

$$\ker \theta = \bigcap_n \mathfrak{m}^n.$$

# Krull Intersection Theorem

**Proposition** (Krull). *Let $R$ be a Noetherian ring, $\mathfrak{m}$ an ideal, $M$ a finitely-generated $R$-module, $x \in M$. Then*

$$x \in \bigcap_n \mathfrak{m}^n M \iff (1 + \mathfrak{m})x = \{0\}.$$

**Corollary.** *If $\mathfrak{m}$ is proper, then*

$$\ker \theta = \bigcap_n \mathfrak{m}^n = \{0\}$$

*and $\theta : R \longrightarrow R_{\mathfrak{m}}$ is injective.*

# One Dimensional Iteration

$R$ Noetherian commutative ring with unit, $\mathfrak{m}$ maximal ideal of $R \implies R/\mathfrak{m}$ is a field.

$f(Z) \in R[Z]$, $\alpha$ zero of $f(Z)$ in $R_{\mathfrak{m}}$.

$$\alpha^{(k)} := \alpha \pmod{\mathfrak{m}^{k+1}}.$$

**Proposition.** *Let* $\alpha \in R_{\mathfrak{m}}$ *and* $f(X) \in R_{\mathfrak{m}}[X]$*.*

$$\left.\begin{array}{c} \alpha^{(k-1)} = \alpha \\ \implies f(\alpha^{(k-1)}) = f(\alpha) \end{array}\right. \pmod{\mathfrak{m}^k}.$$

# Taylor's Formula

$$f(Z) = f(\alpha^{(k-1)}) + f'(\alpha^{(k-1)})(Z - \alpha^{(k-1)}) + \tfrac{1}{2} f''(\alpha^{(k-1)})(Z - \alpha^{(k-1)})^2 + \cdots .$$

$$0 = f(\alpha) = f(\alpha^{(k-1)}) + f'(\alpha^{(k-1)})(\alpha - \alpha^{(k-1)}) \pmod{\mathfrak{m}^{2k}}.$$

# Basic Iteration Formula

$$\begin{aligned}\alpha - \alpha^{(k-1)} &= \alpha^{(2k-1)} - \alpha^{(k-1)} \\ &= -f'(\alpha^{(k-1)})^{-1} \cdot f(\alpha^{(k-1)})\end{aligned} \pmod{\mathfrak{m}^{2k}}.$$

Basic iteration formula modulo $\mathfrak{m}^{2k}$:

$$\boxed{\begin{aligned}&\alpha^{(2k-1)} - \alpha^{(k-1)} \\ &= \left[-f'(\alpha^{(k-1)})^{-1} \mod \mathfrak{m}^k\right] \cdot \left[f(\alpha^{(k-1)}) \mod \mathfrak{m}^{2k}\right]\end{aligned}}$$

# Linear Iteration

$$\alpha^{(k)} - \alpha^{(k-1)}$$

$$= \left[-f'(\alpha^{(k-1)})^{-1} \mod \mathfrak{m}\right] \cdot \left[f(\alpha^{(k-1)}) \mod \mathfrak{m}^{k+1}\right]$$

$$= -f'(\alpha^{(0)})^{-1} \cdot f(\alpha^{(k-1)}) \pmod{\mathfrak{m}^{k+1}}.$$

Linear iteration formula:

$$\boxed{\alpha^{(k)} - \alpha^{(k-1)} = -f'(\alpha^{(0)})^{-1} \cdot f(\alpha^{(k-1)}) \pmod{\mathfrak{m}^{k+1}}}$$

# Hensel Lifting

**Proposition.** *Let $R$ be an integral domain, $\mathfrak{m}$ an ideal of $R$ and $f(Z) \in R[Z]$.*
*If*

$$f(\alpha^{(0)}) = 0 \pmod{\mathfrak{m}}$$

*such that $f'(\alpha^{(0)})^{-1}$ exists in $R/\mathfrak{m}$,*
*then there is a unique $\alpha \in R_{\mathfrak{m}}$ such that*

$$f(\alpha) = 0$$

*and $\alpha = \alpha^{(0)} \pmod{\mathfrak{m}}$.*

# Optimization: Principal Ideals

$\mathfrak{m} = (p)$.

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots, \qquad a_0 = \alpha^{(0)}.$$

$$\begin{aligned} a_k p^k &= \alpha^{(k)} - \alpha^{(k-1)} \\ &= -f(\alpha^{(k-1)}) f'(\alpha^{(0)})^{-1} \pmod{\mathfrak{m}^{k+1}}. \end{aligned}$$

$$\boxed{a_k = -\left[\frac{f(\alpha^{(k-1)})}{p^k}\right] f'(\alpha^{(0)})^{-1} \pmod{p}}$$

# Quadratic Iteration $\bmod \mathfrak{m}^{2k}$

$$g(Z) = bZ - 1,$$

$$b = f'(\alpha),\ \beta^{(k)} := b^{-1} \pmod{\mathfrak{m}^{k+1}}.$$

$$\beta^{(2k-1)} - \beta^{(k-1)} = (1 - b \cdot \beta^{(k-1)}) \cdot b^{-1},$$

$$\beta^{(2k-1)} - \beta^{(k-1)} = (1 - b \cdot \beta^{(k-1)}) \cdot \beta^{(k-1)}.$$

$$\boxed{\begin{aligned} \alpha^{(2k-1)} - \alpha^{(k-1)} &= -f(\alpha^{(k-1)}) \cdot \beta^{(k-1)}, \\ \beta^{(2k-1)} - \beta^{(k-1)} &= (1 - f'(\alpha^{(2k-1)}) \cdot \beta^{(k-1)}) \cdot \beta^{(k-1)} \end{aligned}}$$

# Division Elimination

$f(Z)$ square-free.

$$f'(Z)A(Z) - f(Z)B(Z) = 1.$$

$$f'(\alpha^{(k-1)})A(\alpha^{(k-1)}) = 1 \pmod{\mathfrak{m}^k}.$$

$$\alpha^{(2k-1)} - \alpha^{(k-1)}$$
$$= \left[A(\alpha^{(k-1)}) \mod \mathfrak{m}^k\right] \cdot \left[-f(\alpha^{(k-1)}) \mod \mathfrak{m}^{2k}\right]$$

# Multidimensional Iteration

$$\vec{f} = (f_1, \ldots, f_m) : R^n_{\mathfrak{m}} \rightarrow R^m_{\mathfrak{m}},\ \vec{x} = (x_1, \ldots, x_n).$$

$$\vec{f}(\vec{Z}) = \vec{f}(\vec{x}) + \mathbf{J}(\vec{x}) \cdot (\vec{Z} - \vec{x}) + \cdots ,$$

$$\mathbf{J}(\vec{x}) = \frac{\partial \vec{f}}{\partial \vec{Z}}(\vec{x}) = \begin{pmatrix} \frac{\partial f_1}{\partial Z_1}(\vec{x}) & \frac{\partial f_1}{\partial Z_2}(\vec{x}) & \cdots & \frac{\partial f_1}{\partial Z_n}(\vec{x}) \\ \frac{\partial f_2}{\partial Z_1}(\vec{x}) & \frac{\partial f_2}{\partial Z_2}(\vec{x}) & \cdots & \frac{\partial f_2}{\partial Z_n}(\vec{x}) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial Z_1}(\vec{x}) & \frac{\partial f_m}{\partial Z_2}(\vec{x}) & \cdots & \frac{\partial f_m}{\partial Z_n}(\vec{x}) \end{pmatrix}.$$

# Linear Iteration

Basic iteration formula:

$$\vec{\alpha}^{(2k-1)} - \vec{\alpha}^{(k-1)} = -\mathbf{J}(\vec{\alpha}^{(k-1)})^{-1} \cdot \vec{f}(\vec{\alpha}^{(k-1)}) \pmod{\mathfrak{m}^{2k}}$$

Linear iteration formula:

$$\vec{\alpha}^{(k)} - \vec{\alpha}^{(k-1)} = -\mathbf{J}(\vec{\alpha}^{(0)})^{-1} \cdot \vec{f}(\vec{\alpha}^{(k-1)}) \pmod{\mathfrak{m}^{k+1}}$$

# Multivariate Hensel Lifting

**Proposition.** *Let $R$ be an integral domain with an ideal $\mathfrak{m}$. Let $\vec{f} \in R[Z_1, \ldots, Z_n]^n$ and denote its Jacobian w. r. t. the $Z_i$ by $\mathbf{J}$. If*

$$\vec{f}(\vec{\alpha}^{(0)}) = 0 \pmod{\mathfrak{m}}$$

*such that $\det \mathbf{J}(\vec{\alpha}^{(0)})$ has an inverse in $R/\mathfrak{m}$, then there exists a unique $\vec{\alpha} \in R_{\mathfrak{m}}^n$ such that*

$$\vec{f}(\vec{\alpha}) = 0$$

*and $\vec{\alpha} = \vec{\alpha}^{(0)} \pmod{\mathfrak{m}}$.*

# Quadratic Iteration $\bmod \mathfrak{m}^{2k}$

$$\Upsilon^{(k-1)} \cdot \mathbf{J}(\vec{\alpha}^{(k-1)}) = \mathbf{1} \pmod{\mathfrak{m}^k}.$$

$$\boxed{\begin{aligned} \vec{\alpha}^{(2k-1)} - \vec{\alpha}^{(k-1)} &= -\Upsilon^{(k-1)} \cdot \vec{f}(\vec{\alpha}^{(k-1)}), \\ \Upsilon^{(2k-1)} - \Upsilon^{(k-1)} &= (\mathbf{1} - \Upsilon^{(k-1)} \cdot \mathbf{J}(\vec{\alpha}^{(2k-1)})) \cdot \Upsilon^{(k-1)} \end{aligned}}$$

Synopsis:

- Linear iteration: slow convergence
- Quadratic iteration: repeated matrix inversion or double iteration

# Hensel's Lemma

**Lemma** (Hensel)**.** *Let* $R$ *be an integral domain,* $F(Z) \in R[Z]$ *monic and* $\mathfrak{m}$ *an ideal of* $R$*. If there exist relatively prime* $G(Z), H(Z) \in (R/\mathfrak{m})[Z]$ *such that*

$$F(Z) = G(Z)H(Z) \pmod{\mathfrak{m}},$$

*then there exist* $\hat{G}(Z), \hat{H}(Z) \in R_{\mathfrak{m}}[Z]$ *such that*

$$G(Z) = \hat{G}(Z), \quad H(Z) = \hat{H}(Z) \pmod{\mathfrak{m}}$$

*and* $F(Z) = \hat{G}(Z)\hat{H}(Z)$ *over* $R_{\mathfrak{m}}$*.*

# Proof of Hensel's Lemma

$$F(Z) = Z^d + f_1 Z^{d-1} + \cdots + f_d,$$

$$G(Z) = Z^r + g_1^{(0)} Z^{r-1} + \cdots + g_r^{(0)},$$

$$H(Z) = Z^s + h_1^{(0)} Z^{s-1} + \cdots + h_s^{(0)},$$

$$f_i \in R, \quad g_i^{(0)}, h_i^{(0)} \in R/\mathfrak{m}, \quad d = r + s.$$

$$\hat{G}(Z) = Z^r + g_1 Z^{r-1} + \cdots + g_r,$$

$$\hat{H}(Z) = Z^s + h_1 Z^{s-1} + \cdots + h_s.$$

# Coefficient Equations

*Coefficient equations* of $\hat{G}(Z)\hat{H}(Z) = F(Z)$:

$$
\begin{aligned}
g_1 + h_1 &= f_1, \\
g_2 + g_1 h_1 + h_2 &= f_2, \\
&\vdots \\
g_r h_{s-1} + g_{r-1} h_s &= f_{d-1}, \\
g_r h_s &= f_d.
\end{aligned}
$$

# Sylvester Matrix

Jacobian $\hat{=}$ Sylvester matrix:

$$\det \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ h_1 & 1 & & 0 & g_1 & 1 & & 0 \\ h_2 & h_1 & \cdots & 0 & g_2 & g_1 & \cdots & 0 \\ \vdots & & & & \vdots & & & \vdots \\ 0 & 0 & \cdots & h_s & 0 & 0 & \cdots & g_r \end{pmatrix}$$

$$= \operatorname{res}_Z(G(Z), H(Z)). \qquad \square$$

# Sparse Hensel Algorithm

$K$ field, $R = K[X_1, \dots, X_v]$.

$$f_1(\Xi_1, \dots, \Xi_m) = p_1(X_1, \dots, X_v),$$
$$\vdots$$
$$f_n(\Xi_1, \dots, \Xi_m) = p_n(X_1, \dots, X_v),$$

$m \le n, \quad \Xi_i, p_i \in R, \quad \deg_{X_j} \Xi_i \le d_i$.

Oracle: solution modulo $(X_1 - x_1, \dots, X_v - x_v)$.

# The $k^{\text{th}}$ Stage

$$f_1(\Xi_1, \ldots, \Xi_m) = p_1(X_1, \ldots, X_k),$$

$$\vdots$$

$$f_n(\Xi_1, \ldots, \Xi_m) = p_n(X_1, \ldots, X_k).$$

Random ideal: $(X_k - x_k)$.

$$\Xi_i = c_{i1}\vec{X}^{\vec{e}_{i1}} + c_{i2}\vec{X}^{\vec{e}_{i2}} + \cdots + c_{it_i}\vec{X}^{\vec{e}_{it_i}} \pmod{(X_k - x_k)},$$

$t_i = \#\{$non-zero terms$\}$, $\quad \vec{X} = (X_1, \ldots, X_{k-1})$.

# Sparsity Assumption

New indeterminates: $\Lambda_{ij}, \quad 1 \leq j \leq t_i$.

$$f_j(\Lambda_{11}\vec{X}^{\vec{e}_{11}} + \cdots + \Lambda_{1t_i}\vec{X}^{\vec{e}_{1t_i}}, \ldots,$$
$$\Lambda_{m1}\vec{X}^{\vec{e}_{m1}} + \cdots + \Lambda_{mt_m}\vec{X}^{\vec{e}_{mt_m}}) = p_j(X_1, \ldots, X_{k-1}; X_k).$$

$$g_1(\Lambda_{11}, \ldots, \Lambda_{mt_m}) = q_1(X_k),$$
$$\vdots$$
$$g_N(\Lambda_{11}, \ldots, \Lambda_{mt_m}) = q_N(X_k).$$

# Hensel Lifting

$$\Lambda_{ij} = c_{ij} \pmod{(X_k - x_k)}.$$

$$\begin{aligned}\Lambda_{ij} &= c_{ij} + c_{ij}^{(1)}(X_k - x_k) + c_{ij}^{(2)}(X_k - x_k)^2 + \cdots \\ &= d_{ij}^{(0)} + d_{ij}^{(1)} X_k + d_{ij}^{(2)} X_k^2 + \cdots \;.\end{aligned}$$

$$\begin{aligned}\Xi_i =& (d_{i1}^{(0)} + d_{i1}^{(1)} X_k + \cdots)\vec{X}^{\vec{e}_{i1}} + \cdots + \\ & (d_{it_i}^{(0)} + d_{it_i}^{(1)} X_k + \cdots)\vec{X}^{\vec{e}_{it_i}}.\end{aligned}$$

# Costs

$$\Pr(\text{imprecise evaluation point}) \leq \frac{v(v-1)dT}{B}.$$

$$B > \frac{v(v-1)dT^2}{\epsilon}.$$