if $f(a_n) = 0$ then $a_{n+1} = a_n$

A MULTIVARIABLE HENSEL'S LEMMA

KEITH CONRAD

1. Introduction

Hensel's lemma in $\mathbf{Z}_p[X]$ is the following result about refining an approximate solution of $f(X) = 0$ to an exact solution.

by Newton's method

$\alpha_{n+1} = \alpha_n - f(\alpha_n)/f'(\alpha_n)$,

$\alpha_0 = a$

$\alpha = \lim_n \alpha_n$

Theorem 1.1. *If $f(X) \in \mathbf{Z}_p[X]$ and some $a \in \mathbf{Z}_p$ satisfies*

$$|f(a)|_p < |f'(a)|_p^2 \Rightarrow \frac{f}{f'} < f'$$

then for a unique $\alpha \in \mathbf{Z}_p$, $f(\alpha) = 0$ and $|\alpha - a|_p < |f'(a)|_p$. More precisely, $|\alpha - a|_p = |f(a)/f'(a)|_p < |f'(a)|_p$ and $|f'(\alpha)|_p = |f'(a)|_p \neq 0$, so α is a simple root of $f(X)$.

In particular, if $|f(a)|_p < 1$ and $|f'(a)|_p = 1$ then there is a unique $\alpha \in \mathbf{Z}_p$ such that $f(\alpha) = 0$ and $|\alpha - a|_p < 1$.

Our goal here is to generalize Theorem 1.1 and its proof to a result about zeros of multivariable p-adic polynomial equations. To do this we will want to measure the size of a vector in $\mathbf{Q}_p^d$ (more often, $\mathbf{Z}_p^d$). For $\mathbf{a} = (a_1, \ldots, a_d)$ in $\mathbf{Q}_p^d$, its *norm* is

$$\|\mathbf{a}\|_p = \max_i |a_i|_p. \tag{1.1}$$

In real analysis it is common to take as the norm (length) of a vector in $\mathbf{R}^d$ the square root of the sum of the squares of the coordinates. That type of norm has no special features in p-adic analysis due to the lack of positivity in the p-adics, so the simpler (1.1) is the standard choice of norm on $\mathbf{Q}_p^d$.

2. An easy generalization

For $f(X_1, \ldots, X_d) \in \mathbf{Z}_p[X_1, \ldots, X_d]$ its derivative is its gradient $(\nabla f)(X_1, \ldots, X_d) = (\partial f/\partial X_1, \ldots, \partial f/\partial X_d)$, which is the vector of partial derivatives of f.

1 polynomial
d variables

Theorem 2.1. *If $f(X_1, \ldots, X_d) \in \mathbf{Z}_p[X_1, \ldots, X_d]$ and some $\mathbf{a} \in \mathbf{Z}_p^d$ satisfies*

$$|f(\mathbf{a})|_p < \|(\nabla f)(\mathbf{a})\|_p^2$$

then there is an $\boldsymbol{\alpha} \in \mathbf{Z}_p^d$ such that $f(\boldsymbol{\alpha}) = 0$ and $\|\boldsymbol{\alpha} - \mathbf{a}\|_p < \|(\nabla f)(\mathbf{a})\|_p$.

In particular, if

$$|f(\mathbf{a})|_p < 1 \quad \text{and} \quad \|(\nabla f)(\mathbf{a})\|_p = 1$$

then there is an $\boldsymbol{\alpha} \in \mathbf{Z}_p^d$ such that $f(\boldsymbol{\alpha}) = 0$ and $\alpha_i \equiv a_i \bmod p$ for $i = 1, \ldots, d$.

Proof. We will pick a coordinate in $(\nabla f)(\mathbf{a})$ at which the maximum in $\|(\nabla f)(\mathbf{a})\|_p$ is achieved in order to reduce ourselves to a polynomial in one variable.

There is a $j \in \{1, \ldots, d\}$ (maybe more than one) such that $\|(\nabla f)(\mathbf{a})\|_p = |(\partial f/\partial X_j)(\mathbf{a})|_p$. Pick such a j and fix all but the jth variable in $f(X_1, \ldots, X_d)$ to form

$$g(X) = f(a_1, \ldots, a_{j-1}, X, a_{j+1}, \ldots, a_d) \in \mathbf{Z}_p[X].$$

Then $g(a_j) = f(\mathbf{a})$ and $g'(a_j) = (\partial f/\partial X_j)(\mathbf{a})$, so the hypothesis of the theorem is $|g(a_j)|_p < |g'(a_j)|_p^2$. Theorem 1.1 can now be used: there is an $\alpha \in \mathbf{Z}_p$ such that $g(\alpha) = 0$ and $|\alpha - a_j|_p <$

$|g'(a_j)|_p = \|(\nabla f)(\mathbf{a})\|_p$. Letting $\boldsymbol{\alpha} = (a_1, \ldots, \alpha, \ldots, a_d)$, with α in the jth coordinate and a_i in the ith coordinate for $i \neq j$, we have $f(\boldsymbol{\alpha}) = 0$ and $\|\boldsymbol{\alpha} - \mathbf{a}\|_p = |\alpha - a_j|_p < \|(\nabla f)(\mathbf{a})\|_p$.

In the special case $|f(\mathbf{a})|_p < 1$ and $\|(\nabla f)(\mathbf{a})\|_p = 1$, the condition $\|\boldsymbol{\alpha} - \mathbf{a}\|_p < \|(\nabla f)(\mathbf{a})\|_p$ becomes $\|\boldsymbol{\alpha} - \mathbf{a}\|_p < 1$, which means $\alpha_i \equiv a_i \bmod p$ for all i. □

There is generally no uniqueness of $\boldsymbol{\alpha}$ in Theorem 2.1 (when $d > 1$) since there could be multiple coordinates at which the norm $\|(\nabla f)(\mathbf{a})\|_p$ achieves its maximal value.

Example 2.2. Let $f(X, Y) = X^2 + Y^2 + 4$ in $\mathbf{Z}_7[X]$. Then $f(1, 3) = 14 \equiv 0 \bmod 7$ while $f_X(1, 3) = 2 \not\equiv 0 \bmod 7$ and $f_Y(1, 3) = 6 \not\equiv 0 \bmod 7$, so we can solve $f(x, y) = 0$ in $\mathbf{Z}_7$ by either solving for x after fixing $y = 3$ or solving for y after fixing $x = 1$:

- $f(X, 3) = X^2 + 13$ has a root α in $\mathbf{Z}_7$ where $\alpha \equiv 1 \bmod 7$, so $f(\alpha, 3) = 0$,
- $f(1, Y) = Y^2 + 5$ has a root β in $\mathbf{Z}_7$ where $\beta \equiv 3 \bmod 7$, so $f(1, \beta) = 0$.

Example 2.3. Let $f(X, Y) = X^2 + Y^2 - 21$ in $\mathbf{Z}_2[X, Y]$. We have $f(1, 2) = -16$ and $(\nabla f)(1, 2) = (2, 4)$, so the norm $\|(\nabla f)(1, 2)\|_2 = 1/2$ is achieved by the first coordinate of the gradient and not the second. We have $|f(1, 2)|_2 < |f_X(1, 2)|_2^2$, so $f(\alpha, 2) = 0$ for some $\alpha \in \mathbf{Z}_2$ with $|\alpha - 1|_2 < 1/2$. Concretely, $\alpha^2 = 17$ and $\alpha \equiv 1 \bmod 4$.

Since $|f(1, 2)|_2 = |f_Y(1, 2)|_2^2$, Theorem 2.1 does not guarantee there is a $\beta \in \mathbf{Z}_2$ making $f(1, \beta) = 0$, and in fact there isn't: we would need $\beta^2 = 20$ and this has no solution in $\mathbf{Z}_2$.

Theorem 2.1 involves a multivariable polynomial, but the proof shows it is really about single-variable polynomials, so such a multivariable generalization of Hensel's lemma is understandably not that impressive.

3. An interesting generalization

For a version of Hensel's lemma making more substantial use of several variables, we'll consider d polynomials in d variables. Let K be a field complete with respect to an absolute value $|\cdot|$ satisfying the strong triangle inequality $|x + y| \leq \max(|x|, |y|)$, such as $K = \mathbf{Q}_p$. Let $\mathfrak{o} = \{x \in K : |x| \leq 1\}$, so $\mathfrak{o} = \mathbf{Z}_p$ when $K = \mathbf{Q}_p$.

For $d \geq 1$ set $\mathfrak{o}[\mathbf{X}] = \mathfrak{o}[X_1, \ldots, X_d]$, and for d polynomials $f_1, \ldots, f_d \in \mathfrak{o}[X_1, \ldots, X_d]$ let $\mathbf{f}(\mathbf{X}) = (f_1, \ldots, f_d) \in \mathfrak{o}[\mathbf{X}]^d$, so $\mathbf{f} \colon \mathfrak{o}^d \to \mathfrak{o}^d$.

We measure the size of a vector in K^d as we did in $\mathbf{Q}_p^d$: for $\mathbf{a} \in K^d$, its norm is

$$\|\mathbf{a}\| = \max_i |a_i|. \tag{3.1}$$

It is easy to verify that

$$\|c\mathbf{a}\| = |c|\,\|\mathbf{a}\|, \quad \|\mathbf{a} + \mathbf{a}'\| \leq \max(\|\mathbf{a}\|, \|\mathbf{a}'\|) \tag{3.2}$$

for all $c \in K$ and $\mathbf{a}$ and $\mathbf{a}'$ in K^d. On K^d we get a metric $\|\mathbf{x} - \mathbf{y}\|$, with respect to which convergence is componentwise, so K^d and $\mathfrak{o}^d$ are both complete.

By the second inequality in (3.2), $\|\mathbf{a}\| \neq \|\mathbf{a}'\| \Rightarrow \|\mathbf{a} + \mathbf{a}'\| = \max(\|\mathbf{a}\|, \|\mathbf{a}'\|)$[1] and a sequence $\{\mathbf{a}_n\}$ in K^d is Cauchy with respect to $\|\cdot\|$ if and only if $\|\mathbf{a_{n+1}} - \mathbf{a_n}\| \to 0$ as $n \to \infty$. Relative to this metric, polynomials in $K[\mathbf{X}]$ are continuous functions $K^d \to K$ and polynomials in $\mathfrak{o}[\mathbf{X}]$ are continuous functions $\mathfrak{o}^d \to \mathfrak{o}$.

An additional property of the norm concerns polynomial values on $\mathfrak{o}^d$ when coefficients are in $\mathfrak{o}$: if $F(\mathbf{X}) \in \mathfrak{o}[\mathbf{X}]$, then

$$\mathbf{x}, \mathbf{y} \in \mathfrak{o}^d \Rightarrow |F(\mathbf{x}) - F(\mathbf{y})| \leq \|\mathbf{x} - \mathbf{y}\|. \tag{3.3}$$

This is a multivariable generalization of $x^i - y^i$ being divisible by $x - y$. To check (3.3), let $\|\mathbf{x} - \mathbf{y}\| = |x_j - y_j|$ for a particular j. Then $|x_i - y_i| \leq |x_j - y_j|$ for all i, so every

[1] Assume $\|\mathbf{a}\| > \|\mathbf{a}'\|$. Then $\|\mathbf{a}\| \leq \max(\|\mathbf{a} + \mathbf{a}'\|, \|-\mathbf{a}'\|)$ and max isn't $\|-\mathbf{a}'\|$. Thus $\|\mathbf{a}\| \leq \|\mathbf{a} + \mathbf{a}'\| \leq \|\mathbf{a}\|$.

$x_i - y_i$ is in the ideal $(x_j - y_j)\mathfrak{o}$ of $\mathfrak{o}$. Therefore in the quotient ring $\mathfrak{o}/(x_j - y_j)\mathfrak{o}$ we have $x_i \equiv y_i$ for all i, so $F(\mathbf{x}) \equiv F(\mathbf{y})$ since the coefficients of the polynomial F are all in $\mathfrak{o}$. Thus $F(\mathbf{x}) - F(\mathbf{y}) \in (x_j - y_j)\mathfrak{o}$, and taking absolute values implies (3.3).

The *derivative matrix* and *Jacobian* of $\mathbf{f}(\mathbf{X}) \in \mathfrak{o}[\mathbf{X}]^d$ are

$$(D\mathbf{f})(\mathbf{X}) = \left(\frac{\partial f_i}{\partial X_j}\right)_{1 \le i,j \le d}, \quad J_{\mathbf{f}}(\mathbf{X}) = \det((D\mathbf{f})(\mathbf{X})) \in \mathfrak{o}[\mathbf{X}].$$

Example 3.1. If $d = 1$ then $\mathbf{f}(\mathbf{X}) = f(X)$ is a polynomial in one variable. We have $(D\mathbf{f})(\mathbf{X}) = f'(X)$ and $J_{\mathbf{f}}(\mathbf{X}) = f'(X)$.

Example 3.2. If $d = 2$ then $\mathbf{f}(\mathbf{X}) = (f_1(X,Y), f_2(X,Y))$ is a vector of two 2-variable polynomials. We have

$$(D\mathbf{f})(\mathbf{X}) = \begin{pmatrix} \partial f_1/\partial X & \partial f_1/\partial Y \\ \partial f_2/\partial X & \partial f_2/\partial Y \end{pmatrix}$$

and

$$J_{\mathbf{f}}(\mathbf{X}) = \frac{\partial f_1}{\partial X}\frac{\partial f_2}{\partial Y} - \frac{\partial f_1}{\partial Y}\frac{\partial f_2}{\partial X}.$$

For each $\mathbf{a} \in \mathfrak{o}^d$ and each $\mathbf{f} = (f_1, \ldots, f_d) \in \mathfrak{o}[X_1, \ldots, X_d]^d$ we have

- the vector $\mathbf{f}(\mathbf{a}) = (f_1(\mathbf{a}), \ldots, f_d(\mathbf{a}))$ in $\mathfrak{o}^d$,
- the $d \times d$ matrix $(D\mathbf{f})(\mathbf{a})$ with entries in $\mathfrak{o}$,
- the scalar $J_{\mathbf{f}}(\mathbf{a}) = \det((D\mathbf{f})(\mathbf{a}))$ in $\mathfrak{o}$.

The number $f'(a)$ when $d = 1$ generalizes in two ways when $d > 1$: to the $d \times d$ matrix $(D\mathbf{f})(\mathbf{a})$ and to the number $J_{\mathbf{f}}(\mathbf{a})$.

Here is a multivariable version of Hensel's lemma where all coordinates play an important role, not just one of them as in Theorem 2.1.

Theorem 3.3. *Let $\mathbf{f} = (f_1, \ldots, f_d) \in \mathfrak{o}[X_1, \ldots, X_d]^d$ and $\mathbf{a} = (a_1, \ldots, a_d) \in \mathfrak{o}^d$ satisfy*

$$0 \neq \|\mathbf{f}(\mathbf{a})\| < |J_{\mathbf{f}}(\mathbf{a})|^2.$$

There is a unique $\boldsymbol{\alpha} \in \mathfrak{o}^d$ such that $\mathbf{f}(\boldsymbol{\alpha}) = \mathbf{0}$ and $\|\boldsymbol{\alpha} - \mathbf{a}\| < |J_{\mathbf{f}}(\mathbf{a})|$. More precisely,

- (1) $\|\boldsymbol{\alpha} - \mathbf{a}\| = \|((D\mathbf{f})(\mathbf{a}))^{-1}\mathbf{f}(\mathbf{a})\| \le \|\mathbf{f}(\mathbf{a})\| / |J_{\mathbf{f}}(\mathbf{a})| < |J_{\mathbf{f}}(\mathbf{a})|$,
- (2) $|J_{\mathbf{f}}(\boldsymbol{\alpha})| = |J_{\mathbf{f}}(\mathbf{a})|$.

In particular, if $\|\mathbf{f}(\mathbf{a})\| < 1$ and $|J_{\mathbf{f}}(\mathbf{a})| = 1$ then there is a unique $\boldsymbol{\alpha} \in \mathfrak{o}^d$ such that $\mathbf{f}(\boldsymbol{\alpha}) = \mathbf{0}$ and $\|\boldsymbol{\alpha} - \mathbf{a}\| < 1$.

For $d = 1$ and $K = \mathbf{Q}_p$, this is Theorem 1.1. A proof of Theorem 1.1 can be based on Newton's method $\alpha_{n+1} = \alpha_n - f(\alpha_n)/f'(\alpha_n)$ for $f(X) \in \mathfrak{o}[X]$ and the proof of Theorem 3.3 below will be based on the multivariable version of Newton's method:

$$\boldsymbol{\alpha}_{n+1} = \boldsymbol{\alpha}_n - ((D\mathbf{f})(\boldsymbol{\alpha}_n))^{-1}\mathbf{f}(\boldsymbol{\alpha}_n)$$

for $\mathbf{f}(\mathbf{X}) \in \mathfrak{o}[\mathbf{X}]^d$ and $\boldsymbol{\alpha}_n \in \mathfrak{o}^d$, starting at $\boldsymbol{\alpha}_1 = \mathbf{a}$.

Example 3.4. Working on $\mathbf{Z}_5^2$, set $\mathbf{f}(x,y) = (x^3+xy+6y^3-1, x^2y+xy^2+5y)$ and $\mathbf{a} = (0,1)$. Then $\mathbf{f}(\mathbf{a}) = (5,5) \equiv (0,0) \bmod 5$ and $(D\mathbf{f})(\mathbf{a}) = \left(\begin{smallmatrix} 1 & 18 \\ 1 & 5 \end{smallmatrix}\right)$, so $J_{\mathbf{f}}(\mathbf{a}) = -13 \not\equiv 0 \bmod 5$. We have $\|\mathbf{f}(\mathbf{a})\|_5 = 1/5$ and $|J_{\mathbf{f}}(\mathbf{a})|_5 = 1$, so Theorem 3.3 tells us there is a unique solution to $\mathbf{f}(x,y) = (0,0)$ in $\mathbf{Z}_5^2$ with $\|(x,y) - (0,1)\|_5 < 1$, which means $x \equiv 0 \bmod 5$ and $y \equiv 1 \bmod 5$. The vector $\binom{x}{y}$ is the limit of the sequence $\boldsymbol{\alpha}_n = \binom{x_n}{y_n}$, where $\boldsymbol{\alpha}_1 = \mathbf{a} = \binom{0}{1}$ and for $n \ge 1$,

$$\begin{aligned} \boldsymbol{\alpha}_{n+1} &= \boldsymbol{\alpha}_n - ((D\mathbf{f})(\boldsymbol{\alpha}_n))^{-1}\mathbf{f}(\boldsymbol{\alpha}_n) \\ &= \begin{pmatrix} x_n \\ y_n \end{pmatrix} - \begin{pmatrix} 3x_n^2 + y_n & x_n + 18y_n^2 \\ 2x_ny_n + y_n^2 & x_n^2 + 2x_ny_n + 5 \end{pmatrix}^{-1} \begin{pmatrix} x_n^3 + x_ny_n + 6y_n^3 - 1 \\ x_n^2y_n + x_ny_n^2 + 5y_n \end{pmatrix}. \end{aligned}$$

Initial values of $\boldsymbol{\alpha}_n$ are $\boldsymbol{\alpha}_1 = (0,1)$, $\boldsymbol{\alpha}_2 = (-5,1)$, and $\boldsymbol{\alpha}_3 = (-5360/1637, 862/1637)$. Using PARI-GP, here are the 5-adic expansions of the first five $\boldsymbol{\alpha}_n$:

$$\begin{aligned}
\boldsymbol{\alpha}_1 &= \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \\
\boldsymbol{\alpha}_2 &= \begin{pmatrix} 0+4\cdot 5+4\cdot 5^2+4\cdot 5^3+4\cdot 5^4+4\cdot 5^5+4\cdot 5^6+4\cdot 5^7+4\cdot 5^8+\cdots \\ 1+0\cdot 5+0\cdot 5^2+0\cdot 5^3+0\cdot 5^4+0\cdot 5^5+0\cdot 5^6+0\cdot 5^7+0\cdot 5^8+\cdots \end{pmatrix}, \\
\boldsymbol{\alpha}_3 &= \begin{pmatrix} 0+4\cdot 5+3\cdot 5^2+4\cdot 5^3+4\cdot 5^4+1\cdot 5^5+4\cdot 5^6+0\cdot 5^7+1\cdot 5^8+\cdots \\ 1+0\cdot 5+2\cdot 5^2+2\cdot 5^3+4\cdot 5^4+4\cdot 5^5+1\cdot 5^6+1\cdot 5^7+4\cdot 5^8+\cdots \end{pmatrix}, \\
\boldsymbol{\alpha}_4 &= \begin{pmatrix} 0+4\cdot 5+3\cdot 5^2+4\cdot 5^3+2\cdot 5^4+1\cdot 5^5+1\cdot 5^6+0\cdot 5^7+4\cdot 5^8+\cdots \\ 1+0\cdot 5+2\cdot 5^2+2\cdot 5^3+3\cdot 5^4+4\cdot 5^5+3\cdot 5^6+2\cdot 5^7+0\cdot 5^8+\cdots \end{pmatrix}, \\
\boldsymbol{\alpha}_5 &= \begin{pmatrix} 0+4\cdot 5+3\cdot 5^2+4\cdot 5^3+2\cdot 5^4+1\cdot 5^5+1\cdot 5^6+0\cdot 5^7+1\cdot 5^8+\cdots \\ 1+0\cdot 5+2\cdot 5^2+2\cdot 5^3+3\cdot 5^4+4\cdot 5^5+3\cdot 5^6+2\cdot 5^7+1\cdot 5^8+\cdots \end{pmatrix}.
\end{aligned}$$

From these calculations, the agreement between $\boldsymbol{\alpha}_n$ and $\boldsymbol{\alpha}_{n+1}$ is doubling at each step:

$$\|\boldsymbol{\alpha}_2 - \boldsymbol{\alpha}_1\|_5 = 1/5, \quad \|\boldsymbol{\alpha}_3 - \boldsymbol{\alpha}_2\|_5 = 1/5^2, \quad \|\boldsymbol{\alpha}_4 - \boldsymbol{\alpha}_3\|_5 = 1/5^4, \quad \|\boldsymbol{\alpha}_5 - \boldsymbol{\alpha}_4\|_5 = 1/5^8.$$

We have $\boldsymbol{\alpha}_n \to \binom{x}{y}$ where

$$\begin{aligned}
x &= 0+4\cdot 5+3\cdot 5^2+4\cdot 5^3+2\cdot 5^4+1\cdot 5^5+1\cdot 5^6+0\cdot 5^7+1\cdot 5^8+4\cdot 5^9+\cdots, \\
y &= 1+0\cdot 5+2\cdot 5^2+2\cdot 5^3+3\cdot 5^4+4\cdot 5^5+3\cdot 5^6+2\cdot 5^7+1\cdot 5^8+3\cdot 5^9+\cdots
\end{aligned}$$

and the following 5-adic expansions illustrate the convergence of $\mathbf{f}(\boldsymbol{\alpha}_n)$ to $\binom{0}{0}$:

$$\mathbf{f}(\boldsymbol{\alpha}_1) = \begin{pmatrix} 5 \\ 5 \end{pmatrix}, \ \mathbf{f}(\boldsymbol{\alpha}_2) = \begin{pmatrix} -5^3 \\ 5^2 \end{pmatrix}, \ \mathbf{f}(\boldsymbol{\alpha}_3) = \begin{pmatrix} 3\cdot 5^5+\cdots \\ 2\cdot 5^4+\cdots \end{pmatrix}, \ \mathbf{f}(\boldsymbol{\alpha}_4) = \begin{pmatrix} 2\cdot 5^9+\cdots \\ 3\cdot 5^8+\cdots \end{pmatrix}.$$

Now we turn to a proof of Theorem 3.3.

Proof. Existence of $\boldsymbol{\alpha}$: Define $\boldsymbol{\alpha}_n$ in K^d for $n \geq 1$ by $\boldsymbol{\alpha}_1 = \mathbf{a}$, and for $n \geq 1$

$$\boldsymbol{\alpha}_{n+1} = \boldsymbol{\alpha}_n - ((D\mathbf{f})(\boldsymbol{\alpha}_n))^{-1}\mathbf{f}(\boldsymbol{\alpha}_n).$$

From the hypothesis that $\|\mathbf{f}(\mathbf{a})\| < |J_{\mathbf{f}}(\mathbf{a})|^2$ we have $J_{\mathbf{f}}(\mathbf{a}) \neq 0$, so $t := \|\mathbf{f}(\mathbf{a})\|/|J_{\mathbf{f}}(\mathbf{a})|^2$ satisfies $0 \leq t < 1$.

We will show by induction on n that

(i) $\|\boldsymbol{\alpha}_n\| \leq 1$, *i.e.*, $\boldsymbol{\alpha}_n \in \mathfrak{o}^d$,
(ii) $|J_{\mathbf{f}}(\boldsymbol{\alpha}_n)| = |J_{\mathbf{f}}(\mathbf{a})|$ (so $(D\mathbf{f})(\boldsymbol{\alpha}_n)$ is invertible, since it has determinant $J_{\mathbf{f}}(\boldsymbol{\alpha}_n) \neq 0$),
(iii) $\|\mathbf{f}(\boldsymbol{\alpha}_n)\| \leq |J_{\mathbf{f}}(\mathbf{a})|^2 t^{2^{n-1}}$.

When $n = 1$, part (i) is a hypothesis of the theorem, part (ii) follows from the definition of $\boldsymbol{\alpha}_1$, and part (iii) follows from the definition of t (as an equality, not just an inequality).

To prove the inductive step for (i), (ii), and (iii), we will use a polynomial identity: for $f \in \mathfrak{o}[X_1, \ldots, X_d]$, $\mathbf{X} = (X_1, \ldots, X_d)$, and $\mathbf{Y} = (Y_1, \ldots, Y_d)$,

$$f(\mathbf{X}+\mathbf{Y}) = f(\mathbf{X}) + \sum_{1\leq i\leq d} \frac{\partial f}{\partial X_i} Y_i + \sum_{1\leq i,j\leq d} C_{ij}(\mathbf{X},\mathbf{Y}) Y_i Y_j, \tag{3.4}$$

where $C_{ij}(\mathbf{X},\mathbf{Y}) \in \mathfrak{o}[\mathbf{X},\mathbf{Y}]$. This is essentially a formal Taylor expansion in d variables. We'll prove (3.4) by induction on d. For $d = 1$, (3.4) is the standard single-variable expansion

$$f(X+Y) = f(X) + f'(X)Y + C(X,Y)Y^2$$

with $C(X,Y) \in \mathfrak{o}[X,Y]$ when $f(X) \in \mathfrak{o}[X]$, which is used to prove the single-variable Hensel's lemma and we treat this as already known (anybody reading a proof of the multivariable Hensel's lemma should already have read a proof of the single-variable case). For $d \geq 2$, write f as a polynomial in X_d:

$$f(X_1, \ldots, X_d) = \sum_{r \geq 0} g_r(X_1, \ldots, X_{d-1}) X_d^r \tag{3.5}$$

where $g_r \in \mathfrak{o}[X_1, \ldots, X_{d-1}]$ and $g_r = 0$ for large r (f is a polynomial). We can apply (3.4) to each g_r by induction (with $d-1$ in place of d), so working in $\mathfrak{o}[\mathbf{X}, \mathbf{Y}]$ modulo the ideal generated by all $Y_i Y_j$,

$$\begin{aligned} f(X_1 + Y_1, \ldots, X_d + Y_d) &= \sum_{r \geq 0} g_r(X_1 + Y_1, \ldots, X_{d-1} + Y_{d-1})(X_d + Y_d)^r \\ &\equiv \sum_{r \geq 0} \left(g_r(X_1, \ldots, X_{d-1}) + \sum_{1 \leq i \leq d-1} \frac{\partial g_r}{\partial X_i} Y_i \right) (X_d^r + r X_d^{r-1} Y_d) \\ &\equiv \sum_{r \geq 0} g_r(X_1, \ldots, X_{d-1}) X_d^r + \sum_{r \geq 0} g_r(X_1, \ldots, X_{d-1}) r X_d^{r-1} Y_d \\ &\quad + \sum_{1 \leq i \leq d-1} \left(\sum_{r \geq 0} \frac{\partial g_r}{\partial X_i} X_d^r \right) Y_i \\ &\equiv f(X_1, \ldots, X_d) + \sum_{1 \leq i \leq d} \frac{\partial f}{\partial X_i} Y_i. \end{aligned}$$

does this use any special property of $\mathfrak{o}[\,]$?

This congruence in $\mathfrak{o}[\mathbf{X}, \mathbf{Y}]$ modulo the ideal generated by all $Y_i Y_j$ is exactly (3.4) for polynomials in d variables, so we are done proving (3.4) for all d.

If $\mathbf{f} = (f_1, \ldots, f_d)$ is a d-tuple of polynomials in $\mathfrak{o}[\mathbf{X}] = \mathfrak{o}[X_1, \ldots, X_d]$ then using (3.4) in each coordinate of $\mathbf{f}$ with f running through $f_1, \ldots, f_d$ gives us

$$\begin{aligned} \mathbf{f}(\mathbf{X} + \mathbf{Y}) &= \begin{pmatrix} \vdots \\ f_k(\mathbf{X} + \mathbf{Y}) \\ \vdots \end{pmatrix}_{1 \leq k \leq d} \\ &= \begin{pmatrix} \vdots \\ f_k(\mathbf{X}) + \sum_{1 \leq i \leq d} \frac{\partial f_k}{\partial X_i} Y_i + \sum_{1 \leq i,j \leq d} C_{ijk}(\mathbf{X}, \mathbf{Y}) Y_i Y_j \\ \vdots \end{pmatrix}_{1 \leq k \leq d} \\ &= \mathbf{f}(\mathbf{X}) + ((D\mathbf{f})(\mathbf{X})) \begin{pmatrix} Y_1 \\ \vdots \\ Y_d \end{pmatrix} + \begin{pmatrix} R_1(\mathbf{X}, \mathbf{Y}) \\ \vdots \\ R_d(\mathbf{X}, \mathbf{Y}) \end{pmatrix}, \end{aligned} \tag{3.6}$$

where $R_k(\mathbf{X}, \mathbf{Y}) = \sum_{1 \leq i,j \leq d} C_{ijk}(\mathbf{X}, \mathbf{Y}) Y_i Y_j$ is a sum of terms that are an $\mathfrak{o}[\mathbf{X}, \mathbf{Y}]$-multiple of some $Y_i Y_j$. The formal identity (3.6) implies by substitution that

$$\mathbf{f} \in \mathfrak{o}[\mathbf{X}]^d, \quad \mathbf{x}, \mathbf{y} \in \mathfrak{o}^d \Longrightarrow \boxed{\mathbf{f}(\mathbf{x} + \mathbf{y}) = \mathbf{f}(\mathbf{x}) + ((D\mathbf{f})(\mathbf{x}))\mathbf{y} + \mathbf{z}, \text{ where } \|\mathbf{z}\| \leq \|\mathbf{y}\|^2} \tag{3.7}$$

since each component of $\mathbf{z}$ is a sum of terms that are an $\mathfrak{o}$-multiple of some $y_i y_j$.

Now assume (i), (ii), and (iii) hold for some $n \geq 1$. Part (ii) implies $(D\mathbf{f})(\boldsymbol{\alpha}_n)$ has nonzero determinant. Since $(D\mathbf{f})(\boldsymbol{\alpha}_n)$ has all entries in $\mathfrak{o}$, Cramer's formula tells us the inverse of

the $d \times d$ matrix $(D\mathbf{f})(\boldsymbol{\alpha}_n)$ has entries in $\mathfrak{o}$ divided by $J_{\mathbf{f}}(\boldsymbol{\alpha}_n)$. Therefore for all $\mathbf{x} \in \mathfrak{o}^d$,

$$\|((D\mathbf{f})(\boldsymbol{\alpha}_n))^{-1}\mathbf{x}\| \leq \frac{1}{|J_{\mathbf{f}}(\boldsymbol{\alpha}_n)|}\|\mathbf{x}\| = \frac{1}{|J_{\mathbf{f}}(\mathbf{a})|}\|\mathbf{x}\| \tag{3.8}$$

by (ii), so by the definition of $\boldsymbol{\alpha}_{n+1}$,

$$\|\boldsymbol{\alpha}_{n+1} - \boldsymbol{\alpha}_n\| = \|((D\mathbf{f})(\boldsymbol{\alpha}_n))^{-1}\mathbf{f}(\boldsymbol{\alpha}_n)\| \leq \frac{1}{|J_{\mathbf{f}}(\mathbf{a})|}\|\mathbf{f}(\boldsymbol{\alpha}_n)\| \leq |J_{\mathbf{f}}(\mathbf{a})|t^{2^{n-1}}, \tag{3.9}$$

where the second inequality is from (iii). Since $0 \leq |J_{\mathbf{f}}(\mathbf{a})| \leq 1$ and $0 \leq t < 1$, we have $\|\boldsymbol{\alpha}_{n+1} - \boldsymbol{\alpha}_n\| < 1$, so $\|\boldsymbol{\alpha}_n\| \leq 1 \Rightarrow \|\boldsymbol{\alpha}_{n+1}\| \leq 1$, which is (i) for $n+1$.

To prove (ii) for $n+1$, we use (3.3) for the polynomial $F(\mathbf{X}) = J_{\mathbf{f}}(\mathbf{X}) \in \mathfrak{o}[\mathbf{X}]$ evaluated at $\boldsymbol{\alpha}_{n+1}$ and $\boldsymbol{\alpha}_n$ in $\mathfrak{o}$:

$$|J_{\mathbf{f}}(\boldsymbol{\alpha}_{n+1}) - J_{\mathbf{f}}(\boldsymbol{\alpha}_n)| \leq \|\boldsymbol{\alpha}_{n+1} - \boldsymbol{\alpha}_n\|. \tag{3.10}$$

By (3.9), $\|\boldsymbol{\alpha}_{n+1} - \boldsymbol{\alpha}_n\| \leq |J_{\mathbf{f}}(\mathbf{a})|t^{2^{n-1}} < |J_{\mathbf{f}}(\mathbf{a})|$. Thus $|J_{\mathbf{f}}(\boldsymbol{\alpha}_{n+1}) - J_{\mathbf{f}}(\boldsymbol{\alpha}_n)| < |J_{\mathbf{f}}(\mathbf{a})|$. By (ii) for n we have $|J_{\mathbf{f}}(\boldsymbol{\alpha}_n)| = |J_{\mathbf{f}}(\mathbf{a})|$, so $|J_{\mathbf{f}}(\boldsymbol{\alpha}_{n+1})| = |J_{\mathbf{f}}(\mathbf{a})|$, which is (ii) for $n+1$.

To prove (iii) for $n+1$, we will use (3.7) with $\mathbf{x} = \boldsymbol{\alpha}_n$ and $\mathbf{y} = -((D\mathbf{f})(\boldsymbol{\alpha}_n))^{-1}\mathbf{f}(\boldsymbol{\alpha}_n)$. Obviously $\mathbf{x} \in \mathfrak{o}^d$, and by (3.8) and (iii) for n, $\|\mathbf{y}\| \leq \|\mathbf{f}(\boldsymbol{\alpha}_n)\|/|J_{\mathbf{f}}(\boldsymbol{\alpha}_n)| \leq |J_{\mathbf{f}}(\mathbf{a})|t^{2^{n-1}} < 1$, so $\mathbf{y} \in \mathfrak{o}^d$. Thus by (3.7),

$$\begin{aligned} \mathbf{f}(\boldsymbol{\alpha}_{n+1}) &= \mathbf{f}(\boldsymbol{\alpha}_n - ((D\mathbf{f})(\boldsymbol{\alpha}_n))^{-1}\mathbf{f}(\boldsymbol{\alpha}_n)) \\ &= \mathbf{f}(\boldsymbol{\alpha}_n) + ((D\mathbf{f})(\boldsymbol{\alpha}_n))\left(-((D\mathbf{f})(\boldsymbol{\alpha}_n))^{-1}\mathbf{f}(\boldsymbol{\alpha}_n)\right) + \mathbf{z}, \end{aligned} \tag{3.11}$$

where $\|\mathbf{z}\| \leq \|\mathbf{y}\|^2 \leq |J_{\mathbf{f}}(\mathbf{a})|^2 t^{2^n}$ by the upper bound on $\|\mathbf{y}\|$. Simplifying (3.11),

$$\mathbf{f}(\boldsymbol{\alpha}_{n+1}) = \mathbf{f}(\boldsymbol{\alpha}_n) - \mathbf{f}(\boldsymbol{\alpha}_n) + \mathbf{z} = \mathbf{z},$$

so

$$\|\mathbf{f}(\boldsymbol{\alpha}_{n+1})\| = \|\mathbf{z}\| \leq |J_{\mathbf{f}}(\mathbf{a})|^2 t^{2^n}.$$

This proves (iii) for $n+1$, so we have finished proving (i), (ii), and (iii) for all $n \geq 1$.

The sequence $\{\boldsymbol{\alpha}_n\}$ in $\mathfrak{o}^d$ is Cauchy with respect to $\|\cdot\|$ since $\|\boldsymbol{\alpha}_{n+1} - \boldsymbol{\alpha}_n\| \leq |J_{\mathbf{f}}(\mathbf{a})|t^{2^{n-1}} \leq t^{2^{n-1}}$ by (3.9) and the upper bound tends to 0 as $n \to \infty$. Since $\mathfrak{o}^d$ is complete,

$$\boldsymbol{\alpha} := \lim_{n\to\infty} \boldsymbol{\alpha}_n$$

exists and (iii) tells us that as $n \to \infty$ we have $\|\mathbf{f}(\boldsymbol{\alpha}_n)\| \to 0$. The continuity of polynomials in $\mathfrak{o}[\mathbf{X}]$ as functions $\mathfrak{o}^d \to \mathfrak{o}$ implies $\mathbf{f}(\boldsymbol{\alpha}_n) \to \mathbf{f}(\boldsymbol{\alpha})$, so $\|\mathbf{f}(\boldsymbol{\alpha})\| = 0$ and thus $\mathbf{f}(\boldsymbol{\alpha}) = \mathbf{0}$.

Bounds on $\|\boldsymbol{\alpha} - \mathbf{a}\|$: We want to show

$$\|\boldsymbol{\alpha} - \mathbf{a}\| = \|((D\mathbf{f})(\mathbf{a}))^{-1}\mathbf{f}(\mathbf{a})\| \leq \|\mathbf{f}(\mathbf{a})\|/|J_{\mathbf{f}}(\mathbf{a})| < |J_{\mathbf{f}}(\mathbf{a})|. \tag{3.12}$$

The exact formula for $\|\boldsymbol{\alpha} - \mathbf{a}\|$, which in several variables is at first surprising (we learned it from [3, Theorem 23]), will be proved from the weaker bound $\|\boldsymbol{\alpha} - \mathbf{a}\| < |J_{\mathbf{f}}(\mathbf{a})|$, so first we'll prove the inequalities in (3.12) and then come back to get the exact formula for $\|\boldsymbol{\alpha} - \mathbf{a}\|$.

From (3.9) we have $\|\boldsymbol{\alpha}_{n+1} - \boldsymbol{\alpha}_n\| \leq |J_{\mathbf{f}}(\mathbf{a})|t^{2^{n-1}}$, and $t^{2^{n-1}} \leq t$, so $\|\boldsymbol{\alpha}_{n+1} - \boldsymbol{\alpha}_n\| \leq |J_{\mathbf{f}}(\mathbf{a})|t$ for all n. Therefore $\|\boldsymbol{\alpha}_n - \boldsymbol{\alpha}_1\| \leq |J_{\mathbf{f}}(\mathbf{a})|t$ for all n by the strong triangle inequality for $\|\cdot\|$, so letting $n \to \infty$ gives us

$$\|\boldsymbol{\alpha} - \mathbf{a}\| \leq |J_{\mathbf{f}}(\mathbf{a})|t = |J_{\mathbf{f}}(\mathbf{a})|\frac{\|\mathbf{f}(\mathbf{a})\|}{|J_{\mathbf{f}}(\mathbf{a})|^2} = \frac{\|\mathbf{f}(\mathbf{a})\|}{|J_{\mathbf{f}}(\mathbf{a})|}, \tag{3.13}$$

which is the first inequality in (3.12). The second follows from $\|\mathbf{f}(\mathbf{a})\| < |J_{\mathbf{f}}(\mathbf{a})|^2$.

To explain why $\|\boldsymbol{\alpha}-\mathbf{a}\| = \|((D\mathbf{f})(\mathbf{a}))^{-1}\mathbf{f}(\mathbf{a})\|$, consider separately the cases $\mathbf{f}(\mathbf{a}) = \mathbf{0}$ and $\mathbf{f}(\mathbf{a}) \neq \mathbf{0}$. If $\mathbf{f}(\mathbf{a}) = \mathbf{0}$ then (3.13) implies $\|\boldsymbol{\alpha}-\mathbf{a}\| = \mathbf{0}$, so $\|\boldsymbol{\alpha}-\mathbf{a}\| = \|((D\mathbf{f})(\mathbf{a}))^{-1}\mathbf{f}(\mathbf{a})\|$ since both sides are 0. If $\mathbf{f}(\mathbf{a}) \neq \mathbf{0}$ then $\boldsymbol{\alpha} \neq \mathbf{a}$. Use (3.7) with $\mathbf{x} = \mathbf{a}$ and $\mathbf{y} = \boldsymbol{\alpha}-\mathbf{a}$:

$$\mathbf{0} = \mathbf{f}(\boldsymbol{\alpha}) = \mathbf{f}(\mathbf{a}+(\boldsymbol{\alpha}-\mathbf{a})) = \mathbf{f}(\mathbf{a}) + ((D\mathbf{f})(\mathbf{a}))(\boldsymbol{\alpha}-\mathbf{a}) + \mathbf{z} \tag{3.14}$$

where $\|\mathbf{z}\| \leq \|\boldsymbol{\alpha}-\mathbf{a}\|^2$. We already showed $\|\boldsymbol{\alpha}-\mathbf{a}\| < |J_{\mathbf{f}}(\mathbf{a})|$, so $\|\mathbf{z}\| < |J_{\mathbf{f}}(\mathbf{a})|\,\|\boldsymbol{\alpha}-\mathbf{a}\|$ since $\|\boldsymbol{\alpha}-\mathbf{a}\| > 0$. In (3.14), solve for $\mathbf{f}(\mathbf{a})$ and apply the inverse of $(D\mathbf{f})(\mathbf{a})$ to both sides:

$$\mathbf{f}(\mathbf{a}) = -((D\mathbf{f})(\mathbf{a}))(\boldsymbol{\alpha}-\mathbf{a}) - \mathbf{z} \Longrightarrow ((D\mathbf{f})(\mathbf{a}))^{-1}\mathbf{f}(\mathbf{a}) = -(\boldsymbol{\alpha}-\mathbf{a}) - ((D\mathbf{f})(\mathbf{a}))^{-1}\mathbf{z} \tag{3.15}$$

and reasoning as in (3.8) tells us (using the bound $\|\mathbf{z}\| < |J_{\mathbf{f}}(\mathbf{a})|\,\|\boldsymbol{\alpha}-\mathbf{a}\|$ above)

$$\|((D\mathbf{f})(\mathbf{a}))^{-1}\mathbf{z}\| \leq \frac{1}{|J_{\mathbf{f}}(\mathbf{a})|}\|\mathbf{z}\| < \|\boldsymbol{\alpha}-\mathbf{a}\|.$$

Therefore (3.15) and the strong triangle inequality imply $\|((D\mathbf{f})(\mathbf{a}))^{-1}\mathbf{f}(\mathbf{a})\| = \|\boldsymbol{\alpha}-\mathbf{a}\|$.

Calculation of $\|J_{\mathbf{f}}(\boldsymbol{\alpha})\|$: Part (ii) tells us that $|J_{\mathbf{f}}(\boldsymbol{\alpha}_n)| = |J_{\mathbf{f}}(\mathbf{a})|$ for all n, so continuity of $J_{\mathbf{f}}(\mathbf{x})$ as a function of $\mathbf{x} \in \mathfrak{o}^d$ implies by passage to the limit that $|J_{\mathbf{f}}(\boldsymbol{\alpha})| = |J_{\mathbf{f}}(\mathbf{a})|$.

Uniqueness of $\boldsymbol{\alpha}$: If $\boldsymbol{\beta} \in \mathfrak{o}^d$ satisfies $\mathbf{f}(\boldsymbol{\beta}) = \mathbf{0}$ and $\|\boldsymbol{\beta}-\mathbf{a}\| < |J_{\mathbf{f}}(\mathbf{a})|$ we will show $\boldsymbol{\beta} = \boldsymbol{\alpha}$. (Since $\mathbf{a} \in \mathfrak{o}^d$ and $|J_{\mathbf{f}}(\mathbf{a})| \leq 1$, if $\boldsymbol{\beta}$ were in K^d then it would have to be in $\mathfrak{o}^d$.) Set $\mathbf{h} = \boldsymbol{\beta}-\boldsymbol{\alpha}$, so $\mathbf{h} \in \mathfrak{o}^d$ and $\boldsymbol{\beta} = \boldsymbol{\alpha}+\mathbf{h}$. We want to show $\mathbf{h} = \mathbf{0}$.

In (3.6) set $\mathbf{X} = \boldsymbol{\alpha}$ and $\mathbf{Y} = \mathbf{h}$:

$$\mathbf{0} = \mathbf{f}(\boldsymbol{\beta}) = \mathbf{f}(\boldsymbol{\alpha}+\mathbf{h}) = \mathbf{f}(\boldsymbol{\alpha}) + ((D\mathbf{f})(\boldsymbol{\alpha}))\mathbf{h} + \begin{pmatrix} R_1(\boldsymbol{\alpha},\mathbf{h}) \\ \vdots \\ R_d(\boldsymbol{\alpha},\mathbf{h}) \end{pmatrix} = ((D\mathbf{f})(\boldsymbol{\alpha}))\mathbf{h} + \begin{pmatrix} R_1(\boldsymbol{\alpha},\mathbf{h}) \\ \vdots \\ R_d(\boldsymbol{\alpha},\mathbf{h}) \end{pmatrix},$$

where $R_k(\mathbf{X},\mathbf{Y}) = \sum_{i,j} C_{ijk}(\mathbf{X},\mathbf{Y})Y_iY_j$ for polynomials $C_{ijk}(\mathbf{X},\mathbf{Y}) \in \mathfrak{o}[\mathbf{X},\mathbf{Y}]$. Thus

$$((D\mathbf{f})(\boldsymbol{\alpha}))\mathbf{h} = \begin{pmatrix} -R_1(\boldsymbol{\alpha},\mathbf{h}) \\ \vdots \\ -R_d(\boldsymbol{\alpha},\mathbf{h}) \end{pmatrix} = \begin{pmatrix} -\sum_{i,j} C_{ij1}(\boldsymbol{\alpha},\mathbf{h})h_ih_j \\ \vdots \\ -\sum_{i,j} C_{ijd}(\boldsymbol{\alpha},\mathbf{h})h_ih_j \end{pmatrix}. \tag{3.16}$$

From $\|\boldsymbol{\beta}-\mathbf{a}\| < |J_{\mathbf{f}}(\mathbf{a})|$ and $\|\boldsymbol{\alpha}-\mathbf{a}\| < |J_{\mathbf{f}}(\mathbf{a})|$ we get $\|\mathbf{h}\| = \|\boldsymbol{\beta}-\boldsymbol{\alpha}\| < |J_{\mathbf{f}}(\mathbf{a})|$, so $\mathbf{h} = J_{\mathbf{f}}(\mathbf{a})\mathbf{v}$ where $\|\mathbf{v}\| < 1$. In terms of components, for $i = 1,\ldots,d$ we have $h_i = J_{\mathbf{f}}(\mathbf{a})v_i$ where $|v_i| < 1$. We will show $\mathbf{v} = \mathbf{0}$, so $\mathbf{h} = \mathbf{0}$.

Setting h_i and h_j in (3.16) to be $J_{\mathbf{f}}(\mathbf{a})v_i$ and $J_{\mathbf{f}}(\mathbf{a})v_j$ and then dividing both sides of (3.16) by the nonzero number $J_{\mathbf{f}}(\mathbf{a})$,

$$((D\mathbf{f})(\boldsymbol{\alpha}))\mathbf{v} = J_{\mathbf{f}}(\mathbf{a})\begin{pmatrix} -\sum_{i,j} C_{ij1}(\boldsymbol{\alpha},\mathbf{h})v_iv_j \\ \vdots \\ -\sum_{i,j} C_{ijd}(\boldsymbol{\alpha},\mathbf{h})v_iv_j \end{pmatrix}.$$

For a $d \times d$ matrix A, let $\mathrm{adj}(A)$ be its "classical adjoint" of A: this is the matrix whose entries are, up to sign, the $(d-1)\times(d-1)$ minors in A so $A\,\mathrm{adj}(A) = \mathrm{adj}(A)A = (\det A)I_d$. Then $J_{\mathbf{f}}(\mathbf{a})I_d = \det((D\mathbf{f})(\mathbf{a}))I_d = ((D\mathbf{f})(\boldsymbol{\alpha}))\,\mathrm{adj}((D\mathbf{f})(\boldsymbol{\alpha}))$, so

$$((D\mathbf{f})(\boldsymbol{\alpha}))\mathbf{v} = ((D\mathbf{f})(\boldsymbol{\alpha}))\,\mathrm{adj}((D\mathbf{f})(\boldsymbol{\alpha}))\begin{pmatrix} -\sum_{i,j} C_{ij1}(\boldsymbol{\alpha},\mathbf{h})v_iv_j \\ \vdots \\ -\sum_{i,j} C_{ijd}(\boldsymbol{\alpha},\mathbf{h})v_iv_j \end{pmatrix}.$$

The matrix $((D\mathbf{f})(\boldsymbol{\alpha}))$ is in $\mathrm{GL}_n(K)$, so we can multiply by its inverse on the left on both sides above:

$$\mathbf{v} = \mathrm{adj}((D\mathbf{f})(\boldsymbol{\alpha})) \begin{pmatrix} -\sum_{i,j} C_{ij1}(\boldsymbol{\alpha}, \mathbf{h}) v_i v_j \\ \vdots \\ -\sum_{i,j} C_{ijd}(\boldsymbol{\alpha}, \mathbf{h}) v_i v_j \end{pmatrix}. \tag{3.17}$$

Every entry of the matrix $\mathrm{adj}((D\mathbf{f})(\boldsymbol{\alpha}))$ is in $\mathfrak{o}$, each $C_{ijk}(\boldsymbol{\alpha}, \mathbf{h})$ for $1 \leq k \leq d$ is in $\mathfrak{o}$, and $|v_i v_j| \leq \|\mathbf{v}\|^2$ for all i and j, so taking norms of both sides of (3.17) implies

$$\|\mathbf{v}\| \leq \|\mathbf{v}\|^2. \tag{3.18}$$

Since $\|\mathbf{v}\| < 1$, the inequality (3.18) forces $\|\mathbf{v}\|$ to be 0, so $\mathbf{v} = \mathbf{0}$. □

Remark 3.5. There is a multivariable Hensel's lemma that has a weaker condition than $\|\mathbf{f}(\mathbf{a})\| < |J_{\mathbf{f}}(\mathbf{a})|^2$ when $|J_{\mathbf{f}}(\mathbf{a})| < 1$. See [2].

The condition $|f(a)|_p < |f'(a)|_p^2$ in Theorem 1.1 is reasonable, since if $f(X)$ has a simple root $\alpha \in \mathbf{Z}_p$, then all $a \in \mathbf{Z}_p$ that are close enough to α (the bound $|a-\alpha|_p < |f'(\alpha)|_p$ suffices) satisfy $|f(a)|_p < |f'(a)|_p^2$. The following theorem shows the hypothesis $\|\mathbf{f}(\mathbf{a})\| < |J_{\mathbf{f}}(\mathbf{a})|^2$ in Theorem 3.3 is reasonable too.

Theorem 3.6. *If $\mathbf{f}(\mathbf{X}) \in \mathfrak{o}[\mathbf{X}]^d$ and $\mathbf{f}(\boldsymbol{\alpha}) = \mathbf{0}$ with $J_{\mathbf{f}}(\boldsymbol{\alpha}) \neq 0$, then $\|\mathbf{f}(\mathbf{a})\| < |J_{\mathbf{f}}(\mathbf{a})|^2$ for all $\mathbf{a} \in \mathfrak{o}^d$ close enough to $\boldsymbol{\alpha}$: it is sufficient that $\|\mathbf{a} - \boldsymbol{\alpha}\| < |J_{\mathbf{f}}(\boldsymbol{\alpha})|^2 / \|(D\mathbf{f})(\boldsymbol{\alpha})\|$.*

Division by $\|(D\mathbf{f})(\boldsymbol{\alpha})\|$ is allowed since the matrix $(D\mathbf{f})(\boldsymbol{\alpha})$ is not O, as its determinant $J_{\mathbf{f}}(\boldsymbol{\alpha})$ is assumed to be nonzero.

Proof. Let $\boldsymbol{\gamma} = \mathbf{a} - \boldsymbol{\alpha}$, so $\mathbf{a} = \boldsymbol{\alpha} + \boldsymbol{\gamma}$. By (3.7),

$$\mathbf{f}(\mathbf{a}) = \mathbf{f}(\boldsymbol{\alpha} + \boldsymbol{\gamma}) = \mathbf{f}(\boldsymbol{\alpha}) + ((D\mathbf{f})(\boldsymbol{\alpha}))\boldsymbol{\gamma} + \mathbf{z} = ((D\mathbf{f})(\boldsymbol{\alpha}))\boldsymbol{\gamma} + \mathbf{z}$$

where $\|\mathbf{z}\| \leq \|\boldsymbol{\gamma}\|^2$. We will show both vectors $((D\mathbf{f})(\boldsymbol{\alpha}))\boldsymbol{\gamma}$ and $\mathbf{z}$ have norm less than $|J_{\mathbf{f}}(\boldsymbol{\alpha})|^2$, so $\|\mathbf{f}(\mathbf{a})\| < |J_{\mathbf{f}}(\boldsymbol{\alpha})|^2$, and then we'll show $|J_{\mathbf{f}}(\boldsymbol{\alpha})| = |J_{\mathbf{f}}(\mathbf{a})|$.

Our argument will use a matrix norm. For a $d \times d$ matrix $A = (a_{ij})$ with entries in $\mathfrak{o}$, set the *norm* of A to be $\|A\| = \max_{i,j} |a_{ij}|$. Two properties of this matrix norm are

- $\|A\mathbf{x}\| \leq \|A\| \, \|\mathbf{x}\|$ for $\mathbf{x} \in \mathfrak{o}^d$,
- $\|AB\| \leq \|A\| \, \|B\|$ for $d \times d$ matrices A and B with entries in $\mathfrak{o}$. (We do *not* always have equality here. For example, working over $\mathbf{Z}_p$, if $A = \left(\begin{smallmatrix} p+1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & -1 \\ -1 & p+1 \end{smallmatrix}\right)$ then $AB = \left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right)$, so $\|A\| = \|B\| = 1$ while $\|AB\| = 1/p < \|A\| \, \|B\|$.)

For a $d \times d$ matrix A with entries in $\mathfrak{o}$, its classical adjoint $\mathrm{adj}(A)$ also has entries in $\mathfrak{o}$. Taking the matrix norm on both sides of the equation $A \, \mathrm{adj}(A) = (\det A) I_d$ gives us

$$|\det A| = \|(\det A) I_d\| = \|A \, \mathrm{adj}(A)\| \leq \|A\| \, \|\mathrm{adj}(A)\| \leq \|A\|. \tag{3.19}$$

To show $\|((D\mathbf{f})(\boldsymbol{\alpha}))\boldsymbol{\gamma}\| < |J_{\mathbf{f}}(\boldsymbol{\alpha})|^2$, start from

$$\|((D\mathbf{f})(\boldsymbol{\alpha}))\boldsymbol{\gamma}\| \leq \|(D\mathbf{f})(\boldsymbol{\alpha})\| \, \|\boldsymbol{\gamma}\| = \|(D\mathbf{f})(\boldsymbol{\alpha})\| \, \|\mathbf{a} - \boldsymbol{\alpha}\|.$$

On the right, $\|(D\mathbf{f})(\boldsymbol{\alpha})\| > 0$ since $\det((D\mathbf{f})(\boldsymbol{\alpha})) = J_{\mathbf{f}}(\boldsymbol{\alpha}) \neq 0$. By hypothesis $\|\mathbf{a} - \boldsymbol{\alpha}\| < |J_{\mathbf{f}}(\boldsymbol{\alpha})|^2 / \|(D\mathbf{f})(\boldsymbol{\alpha})\|$, so

$$\|((D\mathbf{f})(\boldsymbol{\alpha}))\boldsymbol{\gamma}\| \leq \|(D\mathbf{f})(\boldsymbol{\alpha})\| \, \|\mathbf{a} - \boldsymbol{\alpha}\| < \|(D\mathbf{f})(\boldsymbol{\alpha})\| \, \frac{|J_{\mathbf{f}}(\boldsymbol{\alpha})|^2}{\|(D\mathbf{f})(\boldsymbol{\alpha})\|} = |J_{\mathbf{f}}(\boldsymbol{\alpha})|^2.$$

This calculation explains the bound $\|\mathbf{a} - \boldsymbol{\alpha}\| < |J_{\mathbf{f}}(\boldsymbol{\alpha})|^2 / \|(D\mathbf{f})(\boldsymbol{\alpha})\|$ as a hypothesis in the theorem.

To show $\|\mathbf{z}\| < |J_{\mathbf{f}}(\boldsymbol{\alpha})|^2$,

$$\|\mathbf{z}\| \le \|\boldsymbol{\gamma}\|^2 = \|\mathbf{a}-\boldsymbol{\alpha}\|^2 < \frac{|J_{\mathbf{f}}(\boldsymbol{\alpha})|^4}{\|(D\mathbf{f})(\boldsymbol{\alpha})\|^2}.$$

We want $|J_{\mathbf{f}}(\boldsymbol{\alpha})|^4/\|(D\mathbf{f})(\boldsymbol{\alpha})\|^2 \le |J_{\mathbf{f}}(\boldsymbol{\alpha})|^2$, or equivalently $|J_{\mathbf{f}}(\boldsymbol{\alpha})| \le \|(D\mathbf{f})(\boldsymbol{\alpha})\|$. Applying (3.19) to the matrix $A = (D\mathbf{f})(\boldsymbol{\alpha})$ gives us

$$|J_{\mathbf{f}}(\boldsymbol{\alpha})| \le \|(D\mathbf{f})(\boldsymbol{\alpha})\|, \tag{3.20}$$

so we are done with the proof that $|\mathbf{f}(\mathbf{a})| < |J_{\mathbf{f}}(\boldsymbol{\alpha})|^2$. It remains to prove $|J_{\mathbf{f}}(\boldsymbol{\alpha})| = |J_{\mathbf{f}}(\mathbf{a})|$.

(The bound (3.20) shows $|J_{\mathbf{f}}(\boldsymbol{\alpha})|^2/\|(D\mathbf{f})(\boldsymbol{\alpha})\| \le |J_{\mathbf{f}}(\boldsymbol{\alpha})| \le 1$ since $\mathbf{f} \in \mathfrak{o}[\mathbf{X}]^d$ and $\boldsymbol{\alpha} \in \mathfrak{o}^d$, so any $\mathbf{a}$ in K^d satisfying $\|\mathbf{a}-\boldsymbol{\alpha}\| < |J_{\mathbf{f}}(\boldsymbol{\alpha})|^2/\|(D\mathbf{f})(\boldsymbol{\alpha})\|$ must be in $\mathfrak{o}^d$.)

Since $\mathbf{a}$ and $\boldsymbol{\alpha}$ are in $\mathfrak{o}^d$, as with (3.10) we have

$$|J_{\mathbf{f}}(\mathbf{a}) - J_{\mathbf{f}}(\boldsymbol{\alpha})| \le \|\mathbf{a}-\boldsymbol{\alpha}\| < \frac{|J_{\mathbf{f}}(\boldsymbol{\alpha})|^2}{\|(D\mathbf{f})(\boldsymbol{\alpha})\|} \le |J_{\mathbf{f}}(\boldsymbol{\alpha})|, \tag{3.21}$$

where the last inequality follows from (3.20). Thus $|J_{\mathbf{f}}(\mathbf{a}) - J_{\mathbf{f}}(\boldsymbol{\alpha})| < |J_{\mathbf{f}}(\boldsymbol{\alpha})|$, so $|J_{\mathbf{f}}(\mathbf{a})| = |J_{\mathbf{f}}(\boldsymbol{\alpha})|$. □

Remark 3.7. The bound $\|\mathbf{a}-\boldsymbol{\alpha}\| < |J_{\mathbf{f}}(\boldsymbol{\alpha})|^2/\|(D\mathbf{f})(\boldsymbol{\alpha})\|$ in Theorem 3.6 is not the nicest multivariable generalization of $|a-\alpha| < |f'(\alpha)|$ that could be imagined. A nicer one would be $\|\mathbf{a}-\boldsymbol{\alpha}\| < |J_{\mathbf{f}}(\boldsymbol{\alpha})|$ (note $|J_{\mathbf{f}}(\boldsymbol{\alpha})|^2/\|(D\mathbf{f})(\boldsymbol{\alpha})\| \le |J_{\mathbf{f}}(\boldsymbol{\alpha})|$ by (3.20)). Is Theorem 3.6 valid using $\|\mathbf{a}-\boldsymbol{\alpha}\| < |J_{\mathbf{f}}(\boldsymbol{\alpha})|$?

Just as Theorem 2.1 is an easy generalization of the single-variable Hensel's lemma in Theorem 1.1, there is an easy generalization of Theorem 3.3 that allows more variables than the number of polynomials.

Theorem 3.8. *For $m \ge d$, let $\mathbf{f} = (f_1, \ldots, f_d) \in \mathfrak{o}[X_1, \ldots, X_m]^d$ and $\mathbf{a} = (a_1, \ldots, a_m) \in \mathfrak{o}^m$ satisfy*

$$\|\mathbf{f}(\mathbf{a})\| < |J_{\mathbf{f},d}(\mathbf{a})|^2 \tag{3.22}$$

where

$$J_{\mathbf{f},d}(\mathbf{a}) = \det\left(\frac{\partial f_i}{\partial X_j}(\mathbf{a})\right)_{1\le i,j\le d}. \tag{3.23}$$

There is an $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in \mathfrak{o}^d$ such that $\mathbf{f}(\alpha_1, \ldots, \alpha_d, a_{d+1}, \ldots, a_m) = \mathbf{0}$ and $|\alpha_i - a_i| < |J_{\mathbf{f},d}(\mathbf{a})|$ for $i = 1, \ldots, d$.

In particular, if $\|\mathbf{f}(\mathbf{a})\| < 1$ and $|J_{\mathbf{f},d}(\mathbf{a})| = 1$ then there is an $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in \mathfrak{o}^d$ such that $\mathbf{f}(\alpha_1, \ldots, \alpha_d, a_{d+1}, \ldots, a_m) = \mathbf{0}$ and $|\alpha_i - a_i| < 1$ for $i = 1, \ldots, d$.

Proof. Reduce to the setting of d polynomials in d variables by replacing $f_i(X_1, \ldots, X_m)$ with $f_i(X_1, \ldots, X_d, a_{d+1}, \ldots, a_m) \in \mathfrak{o}[X_1, \ldots, X_d]$ for $1 \le i \le d$ and apply Theorem 3.3 to these. □

We avoided overloading the notation in Theorem 3.8 by fixing all but the first d variables to define $|J_{\mathbf{f},d}(\mathbf{a})|$, but we could have fixed all but any subset of d variables or replaced (3.22) with $\|\mathbf{f}(\mathbf{a})\| < \max_S |J_{\mathbf{f},S}(\mathbf{a})|^2$ where the maximum runs over all d-element subsets S of $\{1, \ldots, m\}$ and $J_{\mathbf{f},S}(\mathbf{a})$ is defined as in (3.23) with the indices from 1 to d replaced by the numbers in S.

4. The multivariable Hensel's lemma for power series

Hensel's lemma works not just for systems of polynomial equations, but also for systems of power series equations. There are two standard types of power series: the series in the d-variable Tate ring $\mathfrak{o}\{\mathbf{X}\}$ (coefficients tending to 0 with the degree of the monomial) and the d-variable formal power series in $\mathfrak{o}[\![\mathbf{X}]\!]$. A series in $\mathfrak{o}\{\mathbf{X}\}$ is convergent on $\mathfrak{o}^d$ (remember that in complete non-archimedean rings, the order of addition for a numerical series can be rearranged without affecting the value) and defines a continuous function $\mathfrak{o}^d \to \mathfrak{o}$, while a series in $\mathfrak{o}[\![\mathbf{X}]\!]$ is convergent on $\mathfrak{m}^d$, where $\mathfrak{m}$ is the maximal ideal of $\mathfrak{o}$, and defines a continuous function $\mathfrak{m}^d \to \mathfrak{o}$. Therefore we seek a version of Hensel's lemma for $\mathbf{f}(\mathbf{x}) = \mathbf{0}$ where $\mathbf{f} \in \mathfrak{o}\{\mathbf{X}\}^d$ and for $\mathbf{f}(\mathbf{x}) = \mathbf{0}$ where $\mathbf{f} \in \mathfrak{o}[\![\mathbf{X}]\!]^d$.

Theorem 4.1. *Let $\mathbf{f} = (f_1, \ldots, f_d) \in \mathfrak{o}\{X_1, \ldots, X_d\}^d$ and $\mathbf{a} = (a_1, \ldots, a_d) \in \mathfrak{o}^d$ satisfy*

$$\|\mathbf{f}(\mathbf{a})\| < |J_{\mathbf{f}}(\mathbf{a})|^2.$$

There is a unique $\boldsymbol{\alpha} \in \mathfrak{o}^d$ such that $\mathbf{f}(\boldsymbol{\alpha}) = \mathbf{0}$ and $\|\boldsymbol{\alpha} - \mathbf{a}\| < |J_{\mathbf{f}}(\mathbf{a})|$. More precisely,

(1) $\|\boldsymbol{\alpha} - \mathbf{a}\| = \left\|((D\mathbf{f})(\mathbf{a}))^{-1}\mathbf{f}(\mathbf{a})\right\| \leq \|\mathbf{f}(\mathbf{a})\| / |J_{\mathbf{f}}(\mathbf{a})| < |J_{\mathbf{f}}(\mathbf{a})|$,
(2) $|J_{\mathbf{f}}(\boldsymbol{\alpha})| = |J_{\mathbf{f}}(\mathbf{a})|$.

In particular, if $\|\mathbf{f}(\mathbf{a})\| < 1$ and $|J_{\mathbf{f}}(\mathbf{a})| = 1$ then there is a unique $\boldsymbol{\alpha} \in \mathfrak{o}^d$ such that $\mathbf{f}(\boldsymbol{\alpha}) = \mathbf{0}$ and $\|\boldsymbol{\alpha} - \mathbf{a}\| < 1$.

Proof. The proof of Theorem 3.3 can be adapted to the setting of power series in $\mathfrak{o}\{\mathbf{X}\}$, defining $\boldsymbol{\alpha}$ as a limit for a multivariable Newton's method. The key point is that the polynomial identity (3.4) when $f \in \mathfrak{o}[\mathbf{X}]$ extends to the case $f \in \mathfrak{o}\{\mathbf{X}\}$, by the same proof. The only difference in the proof is that the coefficients $g_r \in \mathfrak{o}\{X_1, \ldots, X_{d-1}\}$ need not be 0 for large r. Equations (3.6) and (3.7) also generalize to $\mathbf{f} \in \mathfrak{o}\{\mathbf{X}\}^d$, with $C_{ijk}(\mathbf{X}, \mathbf{Y}) \in \mathfrak{o}\{\mathbf{X}, \mathbf{Y}\}$, and once we have those two equations the rest of the proof of Theorem 3.3 carries over. Remember that each element of $\mathfrak{o}\{\mathbf{X}\}$ is a continuous mapping $\mathfrak{o}^d \to \mathfrak{o}$. □

An application of Theorem 4.1 to Diophantine equations is described by Cassels [1, pp. 228–231] using Hensel's lemma for two power series over $\mathbf{Z}_p$ in two variables. The method as well as the version of Hensel's lemma used are attributed there to work of Skolem in the 1930s, so Skolem may have been the first to formulate Hensel's lemma for more than one equation. A similar application is given by Smart [4, pp. 36–39].

Theorem 4.2. *Let $\mathbf{f} = (f_1, \ldots, f_d) \in \mathfrak{o}[\![X_1, \ldots, X_d]\!]^d$ and $\mathbf{a} = (a_1, \ldots, a_d) \in \mathfrak{m}^d$ satisfy*

$$\|\mathbf{f}(\mathbf{a})\| < |J_{\mathbf{f}}(\mathbf{a})|^2.$$

There is a unique $\boldsymbol{\alpha} \in \mathfrak{m}^d$ such that $\mathbf{f}(\boldsymbol{\alpha}) = \mathbf{0}$ and $\|\boldsymbol{\alpha} - \mathbf{a}\| < |J_{\mathbf{f}}(\mathbf{a})|$. More precisely,

(1) $\|\boldsymbol{\alpha} - \mathbf{a}\| = \left\|((D\mathbf{f})(\mathbf{a}))^{-1}\mathbf{f}(\mathbf{a})\right\| \leq \|\mathbf{f}(\mathbf{a})\| / |J_{\mathbf{f}}(\mathbf{a})| < |J_{\mathbf{f}}(\mathbf{a})|$,
(2) $|J_{\mathbf{f}}(\boldsymbol{\alpha})| = |J_{\mathbf{f}}(\mathbf{a})|$.

In particular, if $\|\mathbf{f}(\mathbf{a})\| < 1$ and $|J_{\mathbf{f}}(\mathbf{a})| = 1$ then there is a unique $\boldsymbol{\alpha} \in \mathfrak{m}^d$ such that $\mathbf{f}(\boldsymbol{\alpha}) = \mathbf{0}$ and $\|\boldsymbol{\alpha} - \mathbf{a}\| < 1$.

Proof. As with the proof of Theorem 4.1, equations (3.4), (3.6), and (3.7) can be established for formal power series over $\mathfrak{o}$, where the analogue of (3.7) is

$$\mathbf{f} \in \mathfrak{o}[\![\mathbf{X}]\!]^d, \quad \mathbf{x}, \mathbf{y} \in \mathfrak{m}^d \Longrightarrow \mathbf{f}(\mathbf{x} + \mathbf{y}) = \mathbf{f}(\mathbf{x}) + ((D\mathbf{f})(\mathbf{x}))\mathbf{y} + \mathbf{z}, \text{ where } \|\mathbf{z}\| \leq \|\mathbf{y}\|^2.$$

With this in place, the rest of the proof of Theorem 3.3 carries over. Some attention needs to be paid to a few places where $\mathfrak{m}^d$ replaces $\mathfrak{o}^d$ (both are complete since both are closed in K^d). For example, $\boldsymbol{\alpha}_1 = \mathbf{a} \in \mathfrak{m}^d$ by hypothesis and for $n \geq 1$, $\|\boldsymbol{\alpha}_{n+1} - \boldsymbol{\alpha}_n\| \leq |J_{\mathbf{f}}(\mathbf{a})| t^{2^{n-1}} \leq t < 1$, so $\boldsymbol{\alpha}_n \in \mathfrak{m}^d$ for all n by induction and thus $\boldsymbol{\alpha} = \lim \boldsymbol{\alpha}_n \in \mathfrak{m}^d$. □

Theorems 3.6 and 3.8 and their proofs carry over to power series of both types. Details are left to the reader.

References

[1] J. W. S. Cassels, *Local Fields*, Cambridge Univ. Press, Cambridge, 1986.

[2] B. Fisher, "A Note on Hensel's Lemma in Several Variables," *Proc. Amer. Math. Soc.* **125** (1997), 3185–3189.

[3] F.-V. Kuhlmann, "Maps on ultrametric spaces, Hensel's Lemma, and differential equations over valued fields," *Comm. Algebra* **39** (2011), 1730–1776. Online at https://arxiv.org/abs/1003.5677.

[4] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, Cambridge Univ. Press, Cambridge, 1998.