A note on multivariate Hensel lifting

Joshua A. Grochow[*]

March 6, 2024

Hensel lifting is a technique for taking solutions to systems of equations mod p and "lifting" them to solutions mod p^2, p^4, p^8, etc., to either get at the end an integer solution or at least a p-adic solution. It is typically presented in the context of factoring polynomials over the integers (e.g., [vzGG99, §15.4]) or complete local rings (e.g., [Mur05]), where the corresponding systems have the same number of equations as variables. We are interested in this note in what happens in the general case, with no restriction on the relationship between the number n of variables and number m of equations; in particular we are interested in the "over-constrained" case, i. e., when there are more equations than variables, though our solution will be fully general. The author had difficulty finding the general situation worked out online or in the literature.[1] We claim no real novelty here, but hope these notes may be useful for someone beyond the author (for whom they were certainly useful!).

Given a system of integer polynomial equations $f_1(\vec{x}) = \cdots = f_m(\vec{x}) = 0$, and a solution $\vec{s} \in (\mathbb{Z}/p^k\mathbb{Z})^n$ (that is, $\vec{f}(\vec{s}) \equiv 0 \pmod{p^k}$), a (quadratic) *lift* of $\vec{s}$ is a vector $\vec{r} \in (\mathbb{Z}/p^{2k}\mathbb{Z})^n$ such that $\vec{r} \equiv \vec{s} \pmod{p^k}$ and $\vec{f}(\vec{r}) \equiv 0 \pmod{p^{2k}}$.

Theorem 1. *Let $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$, and suppose that $\vec{s} = (s_1, \ldots, s_n) \in \mathbb{Z}^n$ is a common root of these equations modulo p^k, that is, $\vec{f}(\vec{s}) \equiv \vec{0} \pmod{p^k}$. Let J be the $m \times n$ Jacobian matrix $J_{ij} = \frac{\partial f_i}{\partial x_j}$. The lifts of $\vec{s} \pmod{p^k}$ are in bijective correspondence with the solutions, modulo p^k, of the following integer linear equation:*

$$-\vec{f}(\vec{s})/p^k = J(\vec{s})\vec{x}$$

In particular, when $m = n$ and J is invertible modulo p^k—equivalently, is invertible modulo p—then there is always a unique lift.

Proof. Let $\vec{s} \in \mathbb{Z}^n$ be a root of $\vec{f}$ modulo p^k. Suppose $\vec{r}$ is a lift of $\vec{s}$. Since $\vec{r} \equiv \vec{s} \pmod{p^k}$, write $\vec{r}$ as $\vec{r} = \vec{s} + p^k\vec{r}'$. Since $\vec{r}$ is a root modulo p^{2k}, we have

$$\begin{array}{rcll} \vec{0} & \equiv & \vec{f}(\vec{r}) & \pmod{p^{2k}} \\ & \equiv & \vec{f}(\vec{s} + p^k\vec{r}') & \pmod{p^{2k}} \\ & \equiv & \vec{f}(\vec{s}) + p^k J(\vec{s})\vec{r}' & \pmod{p^{2k}}, \end{array}$$

where we treat $\vec{r}'$ as a $n \times 1$ column vector. The last line follows from "Taylor expansion" around $\vec{s}$, and noting that any term that involves two or more of the $\vec{r}'$ coordinates is divisible by p^{2k}.

[*] University of Colorado Boulder, Boulder, CO, USA, jgrochow@colorado.edu

[1] We had originally found [Cho58], but misunderstood the result, perhaps due to our own misunderstanding of some of the higher-level machinery used in its statement there. After initially posting this online, Juliette Bruce pointed out to us K. Conrad's lovely note [Con24]; the reader wishing for a more p-adically advanced treatment of the case where $n = m$ is advised to consult that note and references therein.

Now, since $\vec{f}(\vec{s}) \equiv \vec{0} \pmod{p^k}$, we can write the integer vector $\vec{f}(\vec{s})$ as $p^k\vec{t}$ for some $\vec{t} \in \mathbb{Z}^n$. Thus we have an integer equation of the form

$$\vec{0} = p^k\vec{t} + p^k J(\vec{s})\vec{r}' + p^{2k}\vec{m}$$

for some integer vector $\vec{m}$. Dividing through by p^k, we get

$$\begin{aligned} \vec{0} &\equiv \vec{t} + J(\vec{s})\vec{r}' && \pmod{p^{2k-k}} \\ -\vec{t} &\equiv J(\vec{s})\vec{r}' && \pmod{p^k}. \end{aligned}$$

Every lift is thus a solution to this equation modulo p^k, and the same argument read backwards gives the converse. □

Let's briefly recall what can happen for solving not-necessarily-square linear equations modulo p^k. We are solving an equation of the form $\vec{t} = J\vec{x} \pmod{p^k}$, where J is $m \times n$, $\vec{x}$ is $n \times 1$, and $\vec{t}$ is $m \times 1$. By Smith Normal Form, there are invertible matrices A of size $m \times m$ and B of size $n \times n$ (invertible modulo p^k, which is equivalent to invertible modulo p) such that AJB^{-1} is diagonal, where the diagonal entries are powers of p in nondecreasing order. We thus reduce to solving

$$A\vec{t} = (AJB^{-1})(B\vec{x}) \pmod{p^k}$$

for $B\vec{x}$ modulo p^k, where AJB^{-1} is diagonal. For simplicity of notation, let us write

$$\vec{t}' := A\vec{t} \qquad J' := AJB^{-1} \qquad \vec{x}' := B\vec{x}$$

so our equation becomes

$$\vec{t}' = J'\vec{x}' \pmod{p^k}.$$

- When $m = n$ and, for each i, the i-th diagonal entry of J' is p^{k_i}, this equation has a solution if and only if the i-th entry of $\vec{t}'$ is divisible by p^{k_i} for all i. In this case, the set of solutions consists of any one solution, plus any solution to the homogeneous equation $0 = J'\vec{z}' \pmod{p^k}$. The solutions to the latter are precisely $\vec{z}' = (z_1 p^{k-k_1}, z_2 p^{k-k_2}, \cdots, z_n p^{k-k_n})^T$ modulo p^k.

  In particular, if $m = n$ and $k_i = 0$ for all i, then there is always a unique solution modulo p^k (hence, a unique lift).

- When $m > n$, the criterion is essentially the same, where we consider $k_i = k$ for all $i > n$. That is, there exists a solution if and only if $p^{k_i} | t_i'$ for all i; for $i > n$, by our convention, this means that $t_i' = 0$ modulo p^k. The solutions to the homogeneous equation have the same description as before.

In characteristic zero, the solvability of linear equations has a nice characterization in terms of determinants (minors). For $\mathbb{Z}$-linear equations modulo p^k, the best analogue I could find was [HS-G86]; I would be grateful for a reference to a more complete determinantal characterization.

The following example shows that in the non-square case, the Jacobian being full rank is not sufficient for existence of a lift (a mistake I made originally, which led me to work out this note).

Example 1. Consider the following integer equations:

$$\begin{aligned} 0 &= f_1(x) := x^2 + 1 \\ 0 &= f_2(x) := x^2 - 4x + 3. \end{aligned}$$

The Jacobian matrix here is just the single column vector $\begin{pmatrix} 2x \\ 2x-4 \end{pmatrix}$. Consider $p = 5$; the solutions to the first equation mod 5 are ± 2, and the only one of these that is also a root of f_2 is $-2 \pmod 5$. The Jacobian evaluated at -2 is $\begin{pmatrix} 1 \\ 2 \end{pmatrix} \pmod 5$, which is full rank. Despite J itself being full rank, the unique solution modulo 5 does not lift to any solution modulo 25: Modulo $5^2 = 25$, the only roots of f_1 are $\pm 7 \pmod{25}$, and only $-7 \pmod{25}$ is a lift of $-2 \pmod 5$. But $f_2(-7) = 49 + 28 + 3 = 49 + 31 = 80 \not\equiv 0 \pmod{25}$.

Following the theorem, we can see what the issue is. Namely, at $-2 \pmod 5$, we have $f_1(-2) = 5$ and $f_2(-2) = 15$, so $\vec{f}(\vec{s})/5 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$, and our lifting equation is

$$\begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} x \pmod 5$$

That is, we have the two equations $x = 1 \pmod 5$ and $3 = 2x \pmod 5$, which clearly have no solution (plug $x = 1$ into the second equation to get a contradiction).

This example can be analyzed more completely as follows. A little Gröbner basis computation yields that $\langle 10, 2x + 4, x^2 + 1 \rangle$ is a Gröbner basis over $\mathbb{Z}$ for the ideal $\langle f_1, f_2 \rangle$. In other words, any solution x to this equation in a ring R must come from a (unital) ring homomorphism $\varphi\colon \mathbb{Z}[x]/\langle 10, 2x + 4, x^2 + 1 \rangle \to R$ as $\varphi(x)$. As the former ring is $(\mathbb{Z}/10\mathbb{Z})[x]/\langle 2x + 4, x^2 + 1 \rangle$, we see that the *only* solutions to this pair of equations are those that exist in rings admitting a homomorphism from $\mathbb{Z}/10\mathbb{Z}$, which is to say, rings of characteristic dividing 10.

The following example even admits some solutions over $\mathbb{Z}$, while having others mod p that don't lift to solutions mod p^2.

Example 2. Consider

$$\begin{aligned} 0 &= g_1(x) := x^4 - 1 \\ 0 &= g_2(x) := (x - 1)(x - 2) \end{aligned}$$

Over $\mathbb{Z}$, the unique solution is $x = 1$, which works over every ring. However, modulo 5, we also have that $2 \pmod 5$ is a solution to both equations. Our lifting equation at $x = 2 \pmod 5$ is

$$\begin{pmatrix} 3 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} x \pmod 5,$$

which we again see has no solution.

As before we can analyze this a bit more fully. By factoring $x-1$ out of both equations, we see that the ideal $\langle g_1, g_2 \rangle$ is equal to the product of ideals $\langle x-1 \rangle \cdot \langle (x+1)(x^2+1), (x-2) \rangle$. The integer solution corresponds to the ideal $\langle x-1 \rangle$. While we could use a Gröbner basis to analyze the solutions to the other ideal, we can analyze it more directly because it contains the monic linear polynomial $x-2$. Thus, we find that roots of the ideal $\langle (x+1)(x^2+1), x-2 \rangle$ are only possible when $x = 2$ is a solution to $(x + 1)(x^2 + 1)$, that is, in rings where $15 = 0$, or equivalently, in rings admitting a homomorphism from $\mathbb{Z}/15\mathbb{Z}$.

One might hope for an example where the integer (or complex) solution was not "so independent" from the unliftable solution mod p, for example, both living on the same irreducible component. However, building and verifying such an example is beyond the scope of this note.

Note that the phenomenon of Example 2—having solutions over $\mathbb{C}$ but also having solutions modulo p that don't lift to p^2—cannot happen with linear equations $A\vec{x} = \vec{b}$: by Smith Normal Form we may assume that A is diagonal with $a_{11}|a_{22}|\cdots|a_{nn}$. Since we are assuming the Jacobian is full rank modulo p, we must have all a_{ii} are units modulo p. To have a solution modulo p but not modulo p^2, it is necessary and sufficient for some entry of $\vec{b}$ beyond the first n to be a multiple of p but not of p^2. But since the rows of A after the n-th are all zero, such a system does not have a solution over $\mathbb{Q}$. As $\mathbb{Z}$-linear equations have solutions over $\mathbb{Q}$ iff they have solutions over $\mathbb{C}$, it also cannot have solutions over $\mathbb{C}$.

Remark 1 (Generalization to commutative rings)**.** Since the case of lifting factorizations of polynomials can also be generalized to an arbitrary (local) commutative ring, it is natural to wonder whether the same could be true for generalizing Theorem 1. And indeed, the proof goes through *mutatis mutandis* when we replace $\mathbb{Z}$ with a commutative ring R, and we replace the prime p with an element $\pi \in R$ that is a non-zerodivisor.

This generalization to commutative rings seems especially useful when the principal ideal $\langle \pi \rangle$ is also maximal, for then $R/\langle \pi \rangle$ is a field and finding a solution mod π can be done using standard techniques over fields before attempting to lift.

Remark 2 (For the experts, from an expert)**.** Daniel Litt (personal communication, 2024) pointed out to us that Theorem 1 is a special case of the following more general fact. Suppose R is any commutative ring and $I \subseteq R$ is an ideal that squares to zero, and V is a variety with a point x defined over R/I. Then, if there are any lifts of x to R-points of V, the set of all such lifts is a torsor for $\mathrm{Hom}(\Omega_V|_x, I)$, where $\Omega_V|_x$ is the module of (Kähler) differentials of V at x. He claims that the proof of this follows from [Stacks, Tag 08S3, Lemma 91.2.1(2)], with a proof that is, and I quote, "the same as [what we wrote above], but perhaps not obviously the same." Furthermore, there is an element of $\mathrm{Ext}^1_{R[V]}(NL_{R[V]/R}, I)$ whose vanishing is a necessary and sufficient condition for the existence of a lift, where NL denotes the naive cotangent complex. I hope to someday understand this remark. As a starting point, we can see that in our case we will have $R = \mathbb{Z}/p^{2k}\mathbb{Z}$, $I = \langle p^k \rangle$, $\Omega_V|_x$ should correspond to our use of the Jacobian, and the element of Ext should generalize our comments above about the existence of solutions to linear equations modulo p^k.

Acknowledgments

We thank Clément Cannone, Daniel Litt, and Juliette Bruce for encouragement to post this note. We than D. Litt for Remark 2, J. Bruce for the pointer to [Con24], and A. Natarajan for the pointer to [Mur05].

References

[Cho58] Chow, Wei Liang. The criterion for unit multiplicity and a generalization of Hensel's lemma. *Amer. J. Math.* 80:539–552, 1958. MR0103193.

[Con24] Conrad, Keith. A multivariable Hensel's lemma. Accessed 2024. https://kconrad.math.uconn.edu/blurbs/gradnumthy/multivarhensel.pdf

[Mur05] Murfet, Daniel. Hensel's Lemma. Notes, accessed 2024. http://therisingsea.org/notes/HenselsLemma.pdf

[HS-G86] Hermida, J. A. and Sánchez-Giralda, T. Linear equations over commutative rings and determinantal ideals. *J. Algebra* 99:72–79, 1986. DOI:10.1016/0021-8693(86)90054-2

[Stacks] The Stacks Project Authors. *The Stacks Project*, accessed 2024. https://stacks.math.columbia.edu

[vzGG99] von zur Gathen, Joachim and Gerhard, Jürgen. *Modern Computer Algebra.* Cambridge University Press, 1999.