MATHEMATICS OF COMPUTATION
VOLUME 42, NUMBER 166
APRIL 1984, PAGES 637–661

Hensel and Newton Methods in Valuation Rings

By Joachim von zur Gathen

Abstract. We give a computational description of Hensel's method for lifting approximate factorizations of polynomials. The general setting of valuation rings provides the framework for this and the other results of the paper. We describe a Newton method for solving algebraic and differential equations. Finally, we discuss a fast algorithm for factoring polynomials via computing short vectors in modules.

1. Introduction. Hensel and Newton methods have received quite a lot of attention in algebraic computing. We present them in their natural framework, that of valuation rings. The Hensel method deals with factorization of polynomials, the Newton method with zeros of polynomials over the given valuation ring. Both methods take an approximate solution and produce a new approximation which is better with respect to the given valuation. Apart from the pioneering paper by Zassenhaus [1969], these methods have usually only been treated in the setting of either the integers or a polynomial ring, thus requiring separate proofs for each case. The unified treatment avoids this, and incidentally obtains the Newton method as a special case of the Hensel method, also giving the aesthetical advantage of avoiding rational functions for the important application of inverting power series.

The Hensel method presented in Section 2 describes a lifting of an approximate factorization of a given polynomial over a valuation ring, where the factors are approximately relatively prime. It results in two choices of an iterative procedure, one with linear and one with quadratic convergence behavior. It allows us to describe the factorization of certain polynomials that are not squarefree over the residue class field, a case not covered by the usual formulation.

In Section 3, we present a Newton method for solving differential equations for formal power series in several variables, in the general case of systems of nonlinear partial differential equations. This includes the case of a system of algebraic equations. One obtains a simple condition which provides an iterative procedure to compute a solution.

In Section 4, we discuss an important recently discovered tool for factoring polynomials: computing short vectors in modules over (valuation) rings. This tool has been introduced by Lenstra-Lenstra-Lovász [1982] for factoring univariate integer polynomials, used in Chistov-Grigoryev [1982], Lenstra [1983] for multivariate polynomials over finite fields, and in Lenstra [1983a] for multivariate integer

Received December 22, 1981; revised April 19, 1983 and June 27, 1983.
1980 *Mathematics Subject Classification*. Primary 12J10, 12B05; Secondary 35C10, 12H20.
Key words and phrases. Valuation, factorization of polynomials, short vector algorithm, Hensel's method, Newton's method, partial differential equations.

0025-5718/84 $1.00 + $.25 per page

polynomials. Although to date the short vector algorithm provides the only worst-case polynomial-time factoring procedure for univariate integer polynomials, older algorithms, based on Berlekamp [1970] and Zassenhaus [1969], perform well in practice. For multivariate polynomials, the competition is between the short vector approach, a different method due to Kaltofen [1982] (see Kaltofen [1983], von zur Gathen-Kaltofen [1983]) which is also polynomial-time in the worst-case, and older algorithms (e.g., Musser [1975], Wang [1978], Zippel [1981]) which may require exponential time in some cases. For the case of sparse polynomials—of great practical importance—a different approach is necessary (von zur Gathen [1983]).

In Section 4, we present a short vector algorithm in the case of non-Archimedean valuations. This yields, in the final section, an algorithm for factoring univariate polynomials over a ring with sufficient valuations. Special cases of this algorithm include univariate polynomials over $\mathbf{Q}$ and bivariate polynomials over a finite field.

The benefit of this unified approach is twofold: it puts the intuitively apparent relation between the different cases into a precise framework, and it clarifies in an "axiomatic" sense which structures are needed to make the algorithm work.

2. Hensel's Lemma. By the standard definition, a valuation $v: R \to \mathbf{R}$, where R is an integral domain (commutative, with 1), satisfies for all $a, b \in R$:

(i) $v(a) \geqslant 0$,

(ii) $v(a) = 0 \Leftrightarrow a = 0$,

(iii) $v(ab) = v(a)v(b)$,

(iv) $v(a + b) \leqslant v(a) + v(b)$.

v is called non-Archimedean if

(iv)′ $v(a + b) \leqslant \max\{v(a), v(b)\}$.

For elementary properties of valuations, see, e.g., van der Waerden [1970, Chapter 18].

2.1. *Definition.* A ring R with a valuation $v: R \to \mathbf{R}_+$ is called a Hensel ring if

(i) $\forall a \in R\ v(a) \leqslant 1$,

(ii) $\forall a, b \in R\ \forall \varepsilon > 0\ \exists c \in R$ such that $(v(a) \leqslant v(b) \Rightarrow v(a - bc) \leqslant \varepsilon)$.

In other words, R is Hensel if and only if it is contained and dense in the valuation ring of its quotient field (with respect to the unique extension of v). Condition (i) implies that v is non-Archimedean. We also say that v is a Hensel valuation. We assume that c as in (ii) can be effectively computed, given a, b and ε. (This definition is not related to the "Henselian rings" of algebraic number theory.)

2.2. *Example.* $\mathbf{Z}$ with the p-adic valuation v_p ($p \in \mathbf{N}$ prime) is a Hensel ring. We have $v_p(a) = p^{-n}$ where $n = \max\{e \geqslant 0: p^e | a\}$ $(a \neq 0)$. (i) is clear, and for (ii) let $p^{-n} \leqslant \varepsilon$. We can assume $v(b) = 1$, so that b is a unit in $\mathbf{Z}/p^n\mathbf{Z}$, and any solution $c \in \mathbf{Z}$ of $bc \equiv a \bmod p^n$ will do.

2.3. *Example.* Similarly, $F[y]$ with the p-adic valuation v_p is a Hensel ring for any field F and $p \in F[y]$ irreducible. We have $v_p(f) = 2^{-n \deg p}$ where $n = \max\{e \geqslant 0: p^e | f\}$. Of special interest are the linear polynomials $p = y - a$ with $a \in F$.

For any Hensel ring R with valuation v we get a natural valuation on $R[x]$, also denoted by v, by setting

$$v\left(\sum_i f_i x^i\right) = \max_i v(f_i).$$

2.4. *Hensel's Lemma: Hypotheses.* As inputs to our algorithmic version of Hensel's lemma we have $f, f_0, \ldots, f_m, s_0, \ldots, s_m \in R[x]$, $z \in R$ and $\alpha, \delta, \varepsilon \in \mathbf{R}$, where R is a Hensel ring with valuation v. We will assume that the following conditions hold.

$$H_1: \quad v(f - f_0 \cdots f_m) \leqslant \varepsilon < 1,$$

$$H_2: \quad v\Big(\sum_{0 \leqslant i \leqslant m} s_i f_0 \cdots f_{i-1} f_{i+1} \cdots f_m - z\Big) \leqslant \delta < 1,$$

H_3: $f_1, \ldots, f_m$ are monic,
$\deg(f_0 \cdots f_m) \leqslant \deg f$,
$\deg s_i \leqslant \deg f_i$ for $1 \leqslant i \leqslant m$,
$\alpha\delta \leqslant 1$, $\alpha^2\varepsilon \leqslant 1$ and $1 \leqslant \alpha v(z)$.

Thus, $f \approx f_0 \cdots f_m$ is an approximate factorization of f, with precision ε. z plays a role similar to the gcd of $f_0, \ldots, f_m$. H_2 describes essentially a partial fraction expansion $\sum s_i/f_i$ of $z/f_0 \cdots f_m$, with precision δ. In the usual treatment of Hensel's lemma, $f_0, \ldots, f_m$ are assumed to be pairwise relatively prime (more precisely, their images in the residue class field of R modulo the maximal ideal $\{a \in R: v(a) < 1\}$ satisfy this assumption), and then one can find $s_0, \ldots, s_m, \delta$ satisfying H_2 with $z = 1$. One can then set $\alpha = 1$; in general, one will choose $\alpha = 1/v(z)$. Thus, H_2 states that "$f_0, \ldots, f_m$ are approximately pairwise relatively prime".

2.5. *Hensel's Lemma: Computation.* Steps (1) to (3) compute new values f_i^* for f_i, and steps (4) to (6) new values t_i for s_i. Steps (1), (4) deal with $1 \leqslant i \leqslant m$, and steps (2), (5) with $i = 0$, which also in H_3 plays an asymmetrical role.

(0) Set $f^* = f$, $z^* = z$, $\gamma = \max\{\delta, \alpha\varepsilon\}$, $\alpha^* = \alpha$, $\varepsilon^* = \alpha\gamma\varepsilon$ and $e = f - f_0 \cdots f_m$.

(1) For $1 \leqslant i \leqslant m$ compute $a_i, b_i, p_i \in R[x]$ such that

$$s_i e = p_i f_i + a_i,$$
$$v(zb_i - a_i) \leqslant \varepsilon\gamma,$$
$$\deg b_i \leqslant \deg a_i < \deg f_i.$$

(2) Compute $a_0, b_0 \in R[x]$ such that

$$a_0 = s_0 e + f_0 \sum_{1 \leqslant i \leqslant m} p_i,$$
$$v(zb_0 - a_0) \leqslant \varepsilon\gamma,$$
$$\deg b_0 \leqslant \deg f - \deg f_1 \cdots f_m.$$

(3) For $0 \leqslant i \leqslant m$ compute .

$$f_i^* = f_i + b_i.$$

(4) For $1 \leqslant i \leqslant m$ compute $c_i, d_i, g_i^*, q_i \in R[x]$ such that

$$g_i^* = f_0^* \cdots f_{i-1}^* f_{i+1}^* \cdots f_m^*,$$
$$s_i(s_i g_i^* - z) = q_i f_i^* + c_i,$$
$$v(zd_i - c_i) \leqslant \gamma^2,$$
$$\deg d_i \leqslant \deg c_i < \deg f_i^*.$$

(5) Compute $g_0^* = f_1^* \cdots f_m^*$, and $c_0, d_0 \in R[x]$ such that

$$c_0 = s_0\left(\sum_{0 \leqslant i \leqslant m} s_i g_i^* - z\right) + f_0^* \sum_{1 \leqslant i \leqslant m} \left(q_i + s_i\left(\sum_{\substack{0 \leqslant j \leqslant m \\ j \neq i}} s_j g_j^* / f_i^*\right)\right),$$

$$v(zd_0 - c_0) \leqslant \gamma^2,$$

$$\deg d_0 < \deg f - \deg g_0.$$

(6) For $0 \leqslant i \leqslant m$ compute $t_i = s_i - d_i$.

2.6. *Hensel's Lemma: Conclusion.* For any $s_0^*, \ldots, s_m^* \in R[x]$ and $\delta^* \in \mathbf{R}$ we denote by H_1^*, H_2^*, H_3^* the properties H_1, H_2, H_3 for the starred elements ($f_0^*, \ldots$ as computed in 2.5), and furthermore

H_4^*: $\forall i,\ 0 \leqslant i \leqslant m,\ v(f_i^* - f_i) \leqslant \alpha\varepsilon,$
$v(s_i^* - s_i) \leqslant \alpha\gamma,$
$\forall i,\ 1 \leqslant i \leqslant m,\ \deg f_i^* = \deg f_i,$
$\deg s_i < \deg f_i \Rightarrow \deg s_i^* < \deg f_i^*.$

H_5^*: Let $I_0 \cup \cdots \cup I_p = \{0, \ldots, m\}$ be a partition with $0 \in I_0$, and $\bar{f}_1, \ldots, \bar{f}_p \in R[x]$ monic. Set

$$F_i = \prod_{j \in I_i} f_j, \quad F_i^* = \prod_{j \in I_i} f_j^*, \quad S_i^* = \sum_{j \in I_i} s_j^* \frac{F_i^*}{f_j^*}.$$

Assume that $v(\bar{f}_i - F_i) \leqslant \alpha\varepsilon$ for $1 \leqslant i \leqslant p$, $\alpha v(s_i) \leqslant 1$ for $0 \leqslant i \leqslant m$, and $\alpha\delta < 1$, $\alpha^2\delta \leqslant 1$, $\alpha^2\varepsilon < 1$, $\alpha^3\varepsilon \leqslant 1$. Replace in H_1^* to H_4^* the arguments $(m, f_i, s_i, f_i^*, s_i^*)$ by $(p, F_i, S_i^*, \bar{f}_i, \bar{s}_i)$ to get $\overline{H}_1$ to $\overline{H}_4$. Then the following are equivalent:

(a) There exist $\bar{f}_0, \bar{s}_0, \ldots, \bar{s}_p \in R[x]$ such that $\overline{H}_1$, $\overline{H}_2$, $\overline{H}_3$, $\overline{H}_4$ hold.
(b) There exists $\bar{f}_0 \in R[x]$ such that $\overline{H}_1$ holds.
(c) $\forall i,\ 1 \leqslant i \leqslant p,\ v(\bar{f}_i - F_i^*) \leqslant \varepsilon^*$.

This property H_5^* states that the f_i^* are essentially unique in the following sense. Obviously, one can group some of the f_i together to form some $F_0, \ldots, F_p$, and also change F_i to $\bar{f}_i$ within precision ε^*, and one will still have a factorization of f with precision ε^*. This is the modification allowed in (c), and "(b) $\Rightarrow$ (c)" states that it is the only way to get a factorization with precision ε^*.

H_5^* will be crucial for proving correctness of the factorization procedure in Section 5. A similar property is given by Theorem Q in Musser [1975].

We can now collect our claims about the computation 2.5 in the following theorem.

2.7. HENSEL'S LEMMA. *Assume that* $f, f_0, \ldots, f_m$, $s_0, \ldots, s_m$, $\alpha, \delta, \varepsilon$ *satisfy* H_1, H_2, H_3. *Then*

(i) *The computations in* (1) *to* (6) *can be performed in* $R[x]$.
(ii) (*Linear case*). *Let* $(s_0^*, \ldots, s_m^*, \delta^*) = (s_0, \ldots, s_m, \gamma)$. *Then* $H_1^*, \ldots, H_5^*$ *hold.*
(iii) (*Quadratic case*). *Assume that* $\deg s_i < \deg f_i$ *for* $0 \leqslant i \leqslant m$, *and let* $(s_0^*, \ldots, s_m^*, \delta^*) = (t_0, \ldots, t_m, \alpha\gamma^2)$. *Then* $H_1^*, \ldots, H_5^*$ *hold.*

For the proof, we first need

2.8. LEMMA. (i) *Let* $a, f, p, s \in R[x]$, f *monic*, $s = pf + a$ *and* $\deg a < \deg f$. *Then* $v(p) \leqslant v(s)$ *and* $v(a) \leqslant v(s)$.

(ii) *Let* $h_0, \ldots, h_m, h_0^*, \ldots, h_m^* \in R[x]$ *and* $v(h_i - h_i^*) \leqslant \varepsilon$ *for* $0 \leqslant i \leqslant m$. *Then* $v(h_0 \cdots h_m - h_0^* \cdots h_m^*) \leqslant \varepsilon$.

Proof. Assume that $l = \deg s - \deg f \geqslant 0$, and let $p = \sum_{0 \leqslant i \leqslant l} p_i x^i$. Using induction on $l - i$, one easily sees that $v(p_i) \leqslant v(s)$ for $i = l, \ldots, 0$. Hence $v(p) \leqslant v(s)$, and also $v(a) = v(s - pf) \leqslant v(s)$. This proves (i), and (ii) is obvious. □

Proof of Hensel's Lemma. Zassenhaus' [1969] original formulation amounts to choosing the new value $f_i' = f_i + es_i$ for f_i. It is a straightforward computation to check that $v(f - f_0' \cdots f_m') \leqslant \varepsilon^*$ (assuming $z = 1$), and similarly for H_2^*. In the above algorithm f_i' is replaced by f_i^* in order to make the degree conditions in H_3^* hold, and the proof involves the appropriate modification of the computation just mentioned.

Lemma 2.8(i) yields the following estimates:

$$\begin{aligned} \forall i, \quad 0 \leqslant i \leqslant m, \quad & v(e) \leqslant \varepsilon, \\ & v(a_i) \leqslant \varepsilon \leqslant \alpha^{-2} \leqslant \alpha^{-1} \leqslant v(z), \\ & v(f_i^* - f_i) = v(b_i) \leqslant \alpha\varepsilon. \end{aligned}$$

Now set $g_i = f_0 \cdots f_{i-1} f_{i+1} \cdots f_m$ for $0 \leqslant i \leqslant m$. Then

$$\begin{aligned} a_0 g_0 &= s_0 g_0 e + f_0 g_0 \sum_{1 \leqslant i \leqslant m} p_i = s_0 g_0 e + \sum_{1 \leqslant i \leqslant m} g_i (s_i e - a_i) \\ &= e\Big(\sum_{0 \leqslant i \leqslant m} s_i g_i - z \Big) + \Big(ze - \sum_{1 \leqslant i \leqslant m} a_i g_i \Big). \end{aligned}$$

Here the first summand u_1 has $v(u_1) \leqslant \varepsilon\delta$, and the second summand u_2 has $\deg u_2 \leqslant \deg f < k + \deg g_0$, where $k = \deg f - \deg g_0 + 1$. Writing $a_0 = u_3 x^k + u_4$ with $\deg u_4 < k$, we have

$$u_1 = a_0 g_0 - u_2 = u_3 \big(g_0 x^k \big) + u_4 g_0 - u_2,$$

and $\deg(u_4 g_0 - u_2) < \deg(g_0 x^k)$. Lemma 2.8(i) implies that $v(u_3) \leqslant v(u_1) \leqslant \varepsilon\delta \leqslant \varepsilon\gamma$, and thus b_0 as in (2) can be computed by truncating $a_0 \pmod{x^k}$ and dividing the coefficients by z (with precision $\varepsilon\gamma$).

Since f_i is monic for $1 \leqslant i \leqslant m$, the division in (1) can be performed in $R[x]$, and we have proved (i) for the steps (1), (2), (3).

$$\begin{aligned} f - \big(f_0 + a_0 z^{-1}\big) \cdots \big(f_m + a_m z^{-1}\big) &= f - f_0 \cdots f_m - z^{-1} \sum_{0 \leqslant i \leqslant m} a_i g_i - h \\ &= e z^{-1} \Big(z - \sum_{0 \leqslant i \leqslant m} s_i g_i \Big) - h, \end{aligned}$$

where h is defined by the first equation. In particular, $v(h) \leqslant (\alpha\varepsilon)^2$. Since

$$v\big(f_i^* - \big(f_i + a_i z^{-1}\big)\big) = v(z)^{-1} v(z b_i - a_i) \leqslant \alpha\gamma\varepsilon,$$

Lemma 2.8(ii) implies that

$$v(f - f_0^* \cdots f_m^*) \leqslant \max\left\{ v\left(ez^{-1}\left(z - \sum_{0 \leqslant i \leqslant m} s_i g_i \right) \right), v(h), \alpha\gamma\varepsilon \right\} = \alpha\gamma\varepsilon.$$

This proves H_1^* to H_4^* in the linear case (ii).

Now assume the hypotheses of (iii), and let $r = \sum_{0 \leqslant i \leqslant m} s_i g_i^* - z$. We have shown that $v(r) \leqslant \gamma$. Writing

$$s_i r = \left(q_i + s_i \sum_{\substack{0 \leqslant j \leqslant m \\ j \neq i}} s_j g_j^* / f_i^* \right) f_i^* + c_i,$$

we get from Lemma 2.8(i)

$$\begin{aligned} \forall i, \quad 0 \leqslant i \leqslant m, \quad & v(c_i) \leqslant \gamma, \\ & v(s_i^* - s_i) = v(d_i) \\ & \leqslant v(z)^{-1} \max\{v(zd_i - c_i), v(c_i)\} \leqslant \alpha\gamma. \end{aligned}$$

Also

$$\begin{aligned} c_0 g_0^* &= s_0 g_0^* r + \sum_{1 \leqslant i \leqslant m} g_i^* (s_i r - c_i) \\ &= r\left(\sum_{0 \leqslant i \leqslant m} s_i g_i^* - z \right) + \left(zr - \sum_{1 \leqslant i \leqslant m} c_i g_i^* \right). \end{aligned}$$

Here, the first summand w_1 has $v(w_1) \leqslant \gamma^2$, and the second summand w_2 has $\deg w_2 < \deg f$. As above for b_0, it follows now that d_0 in (5) can be computed by truncating $c_0 \pmod{x^{k-1}}$ and dividing the coefficients by z (with precision γ^2).

$$\begin{aligned} & \sum_{0 \leqslant i \leqslant m} (s_i - c_i z^{-1}) g_i^* - z \\ &= s_0 g_0^* - z^{-1}\left(s_0 g_0^* r + f_0^* g_0^* \sum_{1 \leqslant i \leqslant m} (s_i r - c_i)/f_i^* \right) + \sum_{1 \leqslant i \leqslant m} (s_i - c_i z^{-1}) g_i^* - z \\ &= r - rz^{-1} \sum_{0 \leqslant i \leqslant m} s_i g_i^* = -r^2 z^{-1}. \end{aligned}$$

It follows that

$$\begin{aligned} & v\left(\sum_{0 \leqslant i \leqslant m} s_i^* g_i^* - z \right) \\ & \quad = v\left(\sum_{0 \leqslant i \leqslant m} (s_i - c_i z^{-1}) g_i^* - z - z^{-1} \sum_{0 \leqslant i \leqslant m} (zd_i - c_i) g_i^* \right) \\ & \quad \leqslant \alpha\gamma^2. \end{aligned}$$

This shows that H_1^* to H_4^* hold in the quadratic case (iii), and the only work left to do is to prove the uniqueness statement H_5^* in both the linear and quadratic case.

"(a) $\Rightarrow$ (b)" is trivial. For "(b) $\Rightarrow$ (c)", choose some $\bar{f}_0$ as in (b) and let $\bar{e} = f - \bar{f}_0 \cdots \bar{f}_p$, $\bar{g}_i = \bar{f}_0 \cdots \bar{f}_{i-1} \bar{f}_{i+1} \cdots \bar{f}_p$, $G_i^* = F_0^* \cdots F_{i-1}^* F_{i+1}^* \cdots F_p^*$. It follows that $v(\bar{f}_i - F_i^*) \leqslant \alpha\varepsilon$ for $1 \leqslant i \leqslant p$, and also

$$\begin{aligned} v(\bar{f}_0 - F_0^*) &= v((\bar{f}_0 - F_0^*)\bar{g}_0) \\ &= v((\bar{f}_0 \bar{g}_0 - f) + F_0^*(G_0^* - \bar{g}_0) + (f - F_0^* G_0^*)) \leqslant \alpha\varepsilon. \end{aligned}$$

Now choose $u \in R$ such that

$$v(u) = \max_{0 \leqslant i \leqslant p} \{v(\bar{f}_i - F_i^*)\},$$

and set

$$h_i = \frac{1}{u}(\bar{f}_1 - F_i^*) \in K[x],$$

where K is the quotient field of R. Then $v(u) \leqslant \alpha\varepsilon$, and $v(h_i) \leqslant 1$ for $0 \leqslant i \leqslant p$. Also

$$\begin{aligned}\varepsilon^* &\geqslant v(f - \bar{f}_0 \cdots \bar{f}_p) = v(f - (F_0^* + uh_0) \cdots (F_p^* + uh_p)) \\ &= v\Big(f - F_0^* \cdots F_p^* - u \sum_{0 \leqslant i \leqslant p} G_i^* h_i + u^2 w\Big)\end{aligned}$$

for some $w \in K[x]$ with $v(w) \leqslant 1$. Since $v(F^*)$, $v(h_i) \leqslant 1$ for all i and $(\alpha\varepsilon)^2 \leqslant \varepsilon^*$, this implies that

$$v(u)v\Big(\sum_{0 \leqslant i \leqslant p} G_i^* h_i\Big) \leqslant \varepsilon^*.$$

It is sufficient to show $v(u) \leqslant \varepsilon^*$. $D = \{d \in K\colon v(d) \leqslant 1\}$ is a valuation ring with maximal ideal $m = \{d \in D\colon v(d) < 1\}$, and residue class homomorphism $\rho\colon D \to D/m$. We also denote the homomorphism $D[x] \to (D/m)[x]$ by ρ. We have S_i/z, $h_i \in D[x]$ for all i.

$$v\Big(\sum_{0 \leqslant i \leqslant p} S_i^* G_i^*/z - 1\Big) = v\Big(\sum_{0 \leqslant i \leqslant m} s_i^* g_i^*/z - 1\Big) \leqslant \alpha\delta^* \leqslant \alpha\gamma < 1.$$

It follows that

$$\begin{aligned}&\sum_{0 \leqslant i \leqslant m} \rho(S_i^*/z)\rho(G_i^*) - 1 = 0, \\ &\gcd\big(\rho(G_0^*), \ldots, \rho(G_p^*)\big) = 1, \\ &\forall i, \quad 0 \leqslant i \leqslant p, \quad \gcd\big(\rho(F_i^*), \rho(G_i^*)\big) = 1.\end{aligned}$$

Now if $v(\Sigma_{0 \leqslant i \leqslant p} G_i^* h_i) \geqslant 1$, then $v(u) \leqslant \varepsilon^*$ and we are done. On the other hand, if $v(\Sigma_{0 \leqslant i \leqslant p} G_i^* h_i) < 1$, then

$$\begin{aligned}&\sum_{0 \leqslant i \leqslant p} \rho(G_i^*)\rho(h_i) = 0, \\ &\forall i, \quad 0 \leqslant i \leqslant p, \quad \rho(F_i^*) \text{ divides } \rho(G_i^*)\rho(h_i), \\ &\forall i, \quad 0 \leqslant i \leqslant p, \quad \rho(F_i^*) \text{ divides } \rho(h_i).\end{aligned}$$

For $1 \leqslant i \leqslant p$, F_i^* is monic and $\deg h_i < \deg F_i^*$, hence $\rho(h_i) = 0$ and $v(h_i) < 1$. It follows that

$$\begin{aligned}\beta &= \max_{1 \leqslant i \leqslant p} v(\bar{f}_i - F_i^*) < v(u) = v(\bar{f}_0 - F_0^*), \\ v(u) &= v((\bar{f}_0 - F_0^*)\bar{g}_0) \\ &= v(f - \bar{e} + F_0^*(G_0^* - \bar{g}_0) - f + e^*) \leqslant \max\{\varepsilon^*, \beta, \varepsilon^*\},\end{aligned}$$

and hence $v(u) \leqslant \varepsilon^*$.

For "(c) $\Rightarrow$ (a)", write $f = \bar{f}_0(\bar{f}_1 \cdots \bar{f}_p) + \bar{e}$ with $\bar{f}_0, \bar{e} \in R[x]$ and $\deg \bar{e} < \deg(\bar{f}_1 \cdots \bar{f}_p)$, let $\bar{g}_i$, G_i^* be as above, and $e^* = f - F_0^* G_0^*$. The equation $F_0^*(G_0^* - \bar{g}_0) + e^* = (\bar{f}_0 - F_0^*)\bar{g}_0 + \bar{e}$ and Lemma 2.8 yield the following estimates:

$$
\begin{aligned}
&v(\bar{g}_0 - G_0^*) \leqslant \varepsilon^*,\\
&v(e^* + f_0^*(\bar{g}_0 - G_0^*)) \leqslant \varepsilon^*,\\
&v(\bar{f}_0 - F_0^*) \leqslant \varepsilon^*,\\
&\forall i, \quad 0 \leqslant i \leqslant p, \quad v(\bar{g}_i - G_i^*) \leqslant \varepsilon^*.
\end{aligned}
$$

Now it is easy to check that with $\bar{s}_i = S_i^*$ for $0 \leqslant i \leqslant p$ properties $\overline{H}_1, \ldots, \overline{H}_4$ hold. □

Of course we want to iterate the computation in 2.5. We shall write

$$(f_0, \ldots, f_m, s_0, \ldots, s_m, \varepsilon)_l^* = (f_0^*, \ldots, f_m^*, \varepsilon^*)$$

for the linear case, and

$$(f_0, \ldots, f_m, s_0, \ldots, s_m, \delta, \varepsilon)_q^* = (f_0^*, \ldots, f_m^*, s_0^*, \ldots, s_m^*, \delta^*, \varepsilon^*)$$

for the quadratic case (omitting the other input-output-data). Assume $f, f_0, \ldots, f_m, s_0, \ldots, s_m, z, \alpha, \delta, \varepsilon$ given such that H_1, H_2, H_3 hold. Let $\gamma = \max\{\delta, \alpha\varepsilon\}$, and assume $\alpha\gamma < 1$. For the linear iteration, we define $(f_{0k}, \ldots, f_{mk}, \varepsilon_k)$ for $k \geqslant 0$ by

$$
\begin{aligned}
(f_{00}, \ldots, f_{m0}, \varepsilon_0) &= (f_0, \ldots, f_m, \varepsilon),\\
(f_{0k}, \ldots, f_{mk}, \varepsilon_k) &= (f_{0,k-1}, \ldots, f_{m,k-1}, s_0, \ldots, s_m, \varepsilon_{k-1})_l^*.
\end{aligned}
$$

By induction on k one sees that this is well-defined, and $\varepsilon_k = \varepsilon(\alpha\gamma)^k$. Thus we obtain a Cauchy sequence of polynomials of bounded degree. In the completion of R this sequence converges coefficientwise with a linear rate of convergence, and the limit polynomials form a factorization of f. Note that we never have to perform steps (4), (5), (6), and we can also skip step (2), since by H_5^* we can recover f_0 to the required precision at any stage of the iteration.

For the quadratic iteration, we define $(f_{0k}, \ldots, f_{mk}, s_{0k}, \ldots, s_{mk}, \delta_k, \varepsilon_k)$ for $k \geqslant 0$ by

$$
\begin{aligned}
(f_{00}, \ldots, \varepsilon_0) &= (f_0, \ldots, \gamma, \varepsilon),\\
(f_{0k}, \ldots, \varepsilon_k) &= (f_{0,k-1}, \ldots, f_{m,k-1}, s_{0,k-1}, \ldots, s_{m,k-1}, \delta_{k-1}, \varepsilon_{k-1})_q^*.
\end{aligned}
$$

Again this is well-defined, and

$$\varepsilon_k = \varepsilon(\alpha\gamma)^{2^k - 1}, \qquad \delta_k = \frac{\gamma}{\varepsilon}\varepsilon_k.$$

If R is complete, this sequence converges quadratically to a factorization of f.

We can rephrase the uniqueness property as follows: If we start with an approximate factorization close to a true factorization of f, then the results of the iteration will get closer and closer to that true factorization:

2.9. COROLLARY. *Assume that $f, f_0, \ldots, f_m, s_0, \ldots, s_m, \alpha, \delta, \varepsilon$ satisfy H_1, H_2, H_3, that $\alpha, \delta, \varepsilon$ satisfy the numerical conditions in H_5^*, and that $f_0^\#, \ldots, f_m^\#, \varepsilon^\#$ have been computed by a Hensel iteration (linear or quadratic). Furthermore, assume that $a \in R$ with $v(a) = 1$, $g_0 \in R[x]$ and $g_1, \ldots, g_p \in K[x]$ are monic with $ag_i \in R[x]$ and*

$$f = g_0 \cdots g_p \quad (\text{in } K[x]),$$

that $I_0, \dots, I_p, F_0, \dots, F_p$ *are as in* H_5^*, *and*

$$v(aF_i - ag_i) \leqslant \alpha\varepsilon$$

for $1 \leqslant i \leqslant p$. *Then, writing* $F_i^{\#} = \prod_{j \in I_i} f_j^{\#}$, *we have for* $1 \leqslant i \leqslant p$

$$v(aF_i^{\#} - ag_i) \leqslant \varepsilon^{\#}.$$

Proof. It is sufficient to prove the claim for one step of the Hensel iteration, since the conditions H_1, H_2, H_3 are inherited from step to step. But then the claim is a direct consequence of H_5^* (using g_i for $\bar{f}_i$). □

We want to discuss an estimate of the number of "basic operations" that a Hensel iteration uses. We make the following (reasonable) assumptions.

For any $a, b \in R$, addition and multiplication with precison ε (i.e., the computation of some $c \in R$ such that $v(a + b - c) \leqslant \varepsilon$, resp. $v(ab - c) \leqslant \varepsilon$) and division with precision ε (as in Definition 2.1(ii)) can be performed in $T(\varepsilon)$ basic operations. T is nonincreasing (i.e., $\varepsilon < \delta \Rightarrow T(\delta) \leqslant T(\varepsilon)$), and then for $\beta \leqslant 1$

$$\sum_{1 \leqslant i \leqslant N} T(\varepsilon\beta^i) \leqslant NT(\varepsilon\beta^N).$$

If we use straightforward polynomial arithmetic, then addition, multiplication and division with remainder of polynomials in $R[x]$ of degrees at most n with precision ε can be performed in $O(n^2T(\varepsilon))$ operations. In our two prominent examples—$R = \mathbf{Z}$ with a p-adic valuation, and $R = F[y]$ with the y-adic valuation—these assumptions are satisfied using straightforward arithmetic, with $T(\varepsilon) = O(\log^2 \varepsilon)$. A basic operation is a bit operation for $R = \mathbf{Z}$, and an arithmetic operation in F for $R = F[y]$.

For simplicity, we give the following estimate only for the linear iteration.

2.10. PROPOSITION. *Suppose an input is given as for a linear Hensel iteration. Then the Nth result* $(f_{0N}, \dots, f_{mN}, \varepsilon_N)$ *can be computed in* $O(n^3NT(\varepsilon_N))$ *basic operations, where* $n = \deg f$.

Proof. Note that it is sufficient to perform all computations for the kth result with precision ε_k. The total number of basic operations in steps (0), (1), (2), (3) then is, up to a constant,

$$\sum_{1 \leqslant k \leqslant N} n^3 T(\varepsilon_k) \leqslant n^3 \sum_{1 \leqslant k \leqslant N} T\big(\varepsilon(\alpha\gamma)^k\big) \leqslant n^3 NT(\varepsilon_N). \quad \square$$

3. Newton's Method.

3.1. THEOREM. *Let* R *be a Hensel ring,* $f \in R[x]$, $a, b \in R$ *and* $\alpha, \delta, \varepsilon \in \mathbf{R}$ *such that*

$$N_1: \quad v(f(a)) \leqslant \varepsilon,$$
$$N_2: \quad v(a - b) \leqslant \delta,$$
$$N_3: \quad \alpha\delta \leqslant 1 \leqslant \alpha v(f'(b)) \quad \text{and} \quad \alpha^2\varepsilon \leqslant 1.$$

Let $a^* = a - f(a)/f'(b)$, $\gamma = \max\{\delta, \alpha\varepsilon\}$, $\delta^* = \gamma$, *and* $\varepsilon^* = \alpha\gamma\varepsilon$. *Let* N_i^* *denote condition* N_i *with* (a, δ, ε) *replaced by* $(a^*, \delta^*, \varepsilon^*)$, *for* $i = 1, 2, 3$. *Then* N_1^*, N_2^*, N_3^* *hold, and furthermore*

$$N_4^*: \quad v(a^* - a) \leqslant \alpha\varepsilon.$$

N_5^*: *Let* $\bar{a} \in R$ *such that* $v(\bar{a} - a) \geqslant \varepsilon < 1$, *and assume* $\alpha = 1$, $\delta < 1$. *Replace* a^* *by* $\bar{a}$ *in* N_i^* *to get* $\bar{N}_i$, *for* $i = 1, 2, 3, 4$. *Then the following are equivalent*:

(a) $\bar{N}_1, \bar{N}_2, \bar{N}_3, \bar{N}_4$ *hold*.

(b) $\bar{N}_1$ *holds*.

(c) $v(\bar{a} - a^*) \geqslant \varepsilon^*$.

Proof. We first observe that for $h \in R[x]$, $c \in R$, $\varepsilon \in \mathbf{R}$ we have

$$v(h(c)) \geqslant \varepsilon \Leftrightarrow \exists r \in R[x] \quad v\big(h - (x - c)h'(c) - (x - c)^2 r\big) \geqslant \varepsilon.$$

A first-degree Taylor expansion of h around c proves " $\Rightarrow$ ", and " $\Leftarrow$ " follows by dividing h by $x - c$ with remainder and using Lemma 1.8(i).

Now use " $\Rightarrow$ " with $h = f$, $c = a$ to get $r \in R[x]$, and set $m = 1$, $f_0 = f'(a) + (x - a)r$, $f_1 = x - a$, $s_0 = -r$, $s_1 = 1$, $z = f'(b)$. Then H_1, H_2, H_3 hold, and we can apply Hensel's lemma. We find $a_1 = f(a)$, $v(f'(b)b_1 - f(a)) \geqslant \gamma\varepsilon$, $v(f_1^* - (x - a^*)) \geqslant \varepsilon^*$, and $v(f - f_0^*(x - a^*)) \geqslant \varepsilon^*$. All the claims now follow from $H_1^*, \ldots, H_5^*$. □

Note that while Yun [1976] motivates the Hensel method as a special form of the Newton method ("Hensel meets Newton"), here the Newton method is a corollary of the Hensel method ("Hensel beats Newton").

If $\alpha\gamma < 1$, then again we get iterations which converge linearly (using a fixed b) resp. quadratically (adapting b at each step) if R is complete. (Fellmann [1977] contains a Newton iteration akin to the one presented here.)

Thus for the linear iteration, we are given $f \in R[x]$, $a_1 \in R$ and $\varepsilon < 1$ such that N_1, N_2, N_3 are satisfied with $b = a = a_1$, $\delta = \varepsilon$ and $\alpha = 1$. If we then assume that

$$v(a_{k+1} - (a_k - f(a_k)/f'(b))) \geqslant \varepsilon^{k+1},$$

Theorem 3.1 implies that

$$v(f(a_k)) \geqslant \varepsilon^k$$

for $k \geqslant 1$, and that a_k is uniquely determined with precision ε^k by

$$v(f(a_k)) \geqslant \varepsilon^k \quad \text{and} \quad v(a_1 - a_k) \geqslant \varepsilon.$$

An important application in algebraic computing of Newton iteration is the inversion of power series (Sieveking [1972], Kung [1974]), using the y-adic valuation v on $R = F[[y]]$. Unfortunately, applying Newton's method to the natural candidate $f = bx - 1$ ($b \in R$ a unit) fails to yield a fast computation, and one has to use the rational function $x^{-1} - b$. However, the above Hensel lemma with $f_0 = b, f_1 = x - a$, $s_0 = -b$, $s_1 = x$, $z = 1$ proves that if $v(ba - 1) \geqslant \varepsilon$, then $v(ba^* - 1) \geqslant \varepsilon^2$ where $a^* = a + a(1 - ab)$, and thus yields the desired fast computation.

For a valuation satisfying 2.1(i), but not necessarily 2.1(ii), this argument will also show that b^{-1} can be approximated with arbitrary precision for $b \in R$ with $v(b) = 1$. However, this does not mean that 2.1(ii) follows from 2.1(i). An example (besides trivial valuations) is $R = F[y^2, y^3] \subseteq F[y]$, where F is a field and v induced by the y-adic valuation on $F[y]$. Here y^3/y^2 cannot be approximated with precision $\varepsilon = \frac{1}{4}$.

We now want to apply Newton's method to differential equations, taking the general case of systems of nonlinear partial differential equations. This includes the

case of systems of algebraic equations. The solutions that we consider are formal power series in several variables and can be approximated to arbitrary precision by polynomials. Thus we only work with the latter. We first present a framework for describing these equations, then a Newton lemma, and finally a simple condition on the equation which ensures that the Newton lemma can be applied iteratively to improve approximate solutions. This iteration also requires an initial approximation; the lack of further boundary conditions makes the solution nonunique, and we compute a particular solution. But on the one hand, the algorithm (Theorem 3.4) can be modified to accommodate such boundary conditions, and on the other hand, the construction indicates what kind of boundary conditions might guarantee existence and uniqueness of solutions. We will not deal with this question in the sequel. (Precious little is known about this problem relative to solutions that are real functions, say; one general result is in Friedrichs [1958].) The intention of the development presented below is not to provide practical algorithms, but to show how these rather general equations fit into the setting of this paper.

Now let F be a field, $R = F[y_1, \ldots, y_p]$ with the $(y_1, \ldots, y_p)$-adic valuation v, so that $v(a) = 2^{-j}$ if the lowest nonzero terms of $a \in R \setminus \{0\}$ have total degree j. We write D_i for $\partial/\partial y_i$, so that $D_i\colon R \to R$ is an additive mapping and $v(D_i(a)) \leqslant \mu v(a)$ for all $a \in R$ with $\mu = 2$.

3.2. *Definition.* For any $m \geqslant 1$ and q, $1 \leqslant q < \infty$, v induces the L_q-norm

$$v_q\colon \quad R^m \to \mathbf{R}$$
$$a \mapsto \Big(\sum_{1 \leqslant i \leqslant m} v(a_i)^q \Big)^{1/q}$$

and also the L_∞-norm

$$v_\infty\colon \quad R^m \to \mathbf{R}$$
$$a \mapsto \max_{1 \leqslant i \leqslant m} v(a_i).$$

Note that for any $q \leqslant \infty$ and $a \in R$ we have $v_\infty(a) \leqslant v_q(a)$.

In order to encode differential equations, let $W = \{1, \ldots, m\} \times \mathbf{N}^p$ and $S = R[\{x_w\colon w \in W\}]$. For $a \in R^m$ we have the evaluation homomorphism $S \to R$ sending x_w to $x_w(a) = D_1^{w_1} \cdots D_p^{w_p}(a_{w_0})$. This is a ring homomorphism, and fixing w, we get an additive mapping $R^m \to R$ with $a \to x_w(a)$. Thus x_w stands for the differential operator that takes the w_0th component of $a \in R^m$ and applies $D_i^{w_i}$ to it, $1 \leqslant i \leqslant p$. S consists of all polynomial expressions in such operators.

Now let $n \geqslant 1$ and $f = (f_1, \ldots, f_n) \in S^n$, where

$$f_j = \cdot \sum_{\substack{l \geqslant 0 \\ w_1, \ldots, w_l \in W}} f_{j w_1 \cdots w_l} x_{w_1} \cdots x_{w_l}.$$

Then $f = 0$ represents the system of nonlinear partial differential equations

$$0 = \sum f_{j w_1 \cdots w_l} \frac{\partial^{w_{11} + \cdots + w_{1p}}}{(\partial y_1)^{w_{11}} \cdots (\partial y_p)^{w_{1p}}} \big(a_{w_{10}}(y_1, \ldots, y_p)\big)$$
$$\cdots \frac{\partial^{w_{l1} + \cdots + w_{lp}}}{(\partial y_1)^{w_{l1}} \cdots (\partial y_p)^{w_{lp}}} \big(a_{w_{l0}}(y_1, \ldots, y_p)\big) \qquad (1 \leqslant j \leqslant n),$$

where $a \in R^m$. Note that this includes the case of algebraic equations (when $w = (w_0, 0, \ldots, 0)$) and also differential equations on affine algebraic varieties.

We say that $u \in \mathbf{N}^p$ occurs in f if there exist $l \geqslant 0$, $j \leqslant n$, $1 \leqslant i \leqslant l$ and $w_1, \ldots, w_l \in W$ such that $f_{jw_1 \cdots w_l} \neq 0$ and $w_i = (w_{i0}, u_1, \ldots, u_p)$. The order of f is

$$k = \max\{u_1 + \cdots + u_p : u \in \mathbf{N}^p \text{ occurs in } f\},$$

and the highest-order operators of f form

$$K = \{u \in \mathbf{N}^p : u \text{ occurs in } f \text{ and } u_1 + \cdots + u_p = k\}.$$

Thus, f is an algebraic equation if and only if $k = 0$. We have the following Newton lemma for differential equations.

3.3. LEMMA. *Let $f \in S^n$ have order k, $1 \leqslant q \leqslant \infty$, $a, b, c \in R^m$, $\gamma, \delta, \varepsilon \in \mathbf{R}$ satisfy*

$$D_1: \quad v_q(f(a)) \leqslant \varepsilon,$$
$$D_2: \quad v_q(b - a) \leqslant \delta,$$

set $\gamma = \max\{\mu^k \delta, \varepsilon\}$, and assume that $v_q(c) \leqslant \mu^{-k}\varepsilon$ and

$$v_q\left(f(a) + \sum_{w \in W} \frac{\partial f}{\partial x_w}(b) \cdot x_w(c)\right) \leqslant \varepsilon\gamma.$$

Furthermore, let $a^* = a + c$, $\varepsilon^* = n^{1/q}\gamma\varepsilon$ and replace (a, ε) by (a^*, ε^*) in D_1, D_2 to get D_1^*, D_2^*. Then D_1^*, D_2^* hold.

Proof. Denote by m_a the maximal ideal in S generated by $\{x_w - x_w(a) : w \in W\}$. Using the Taylor expansion

$$f_j = f_j(a) + \sum_{w \in W} \frac{\partial f_j}{\partial x_w}(a)(x_w - x_w(a)) + r_j$$

for $1 \leqslant j \leqslant n$ and some $r_j \in m_a^2$, the proof is straightforward. □

Note that the arguments of v_q in D_1, D_2 might have different lengths, and that we only need the hypotheses for $q = \infty$ in order to prove the conclusions for general q.

From the above lemma we want to get an iterative procedure again for the computation of approximate solutions of $f = 0$. This is achieved by the following sufficient criterion on f, which insures that a c as in Lemma 3.3 can be efficiently computed at all stages of an iteration. Then we can approximate a solution to arbitrary precision, provided the convergence factor $n^{1/q}\gamma$ is less than 1 and an initial solution $a \in R^m$ is known with $v_q(f(a)) < 1$.

Define r, s by $2^{-r} \leqslant \varepsilon < 2^{-r+1}, 2^{-s-1} \leqslant \varepsilon\gamma < 2^{-s}$, and let

$$l = \binom{p + k + s}{p} - \binom{p + k + r - 1}{p}.$$

Then l is the dimension of the vector space over F

$$\{d \in R : v(d) \leqslant 2^{-(k+r)} \text{ and } \deg d \leqslant k + s\},$$

and thus the number of coefficients of c that are relevant for the hypothesis of Lemma 3.3.

3.4. THEOREM. (i) *Assume* $k \geqslant 1$, $\operatorname{char} F = 0$ *and that there exists an injection* $\phi: \{1, \ldots, n\} \to \{1, \ldots, m\}$ *such that*

$$\forall i \leqslant n \quad \exists u \in K \quad v\left(\frac{\partial f_i}{\partial x_{(\phi(i),u)}}(b)\right) = 1.$$

Then some c *as in Lemma* 3.3 *can be computed by solving a nonsingular triangular system of size* l *of linear equations over* F.

(ii) *Assume* $k = 0$, *and that the* $m \times n$*-matrix* M *over* F *with*

$$M_{ij} = \frac{\partial f_i}{\partial x_{(j,0,\ldots,0)}}(b)\bigg|_{y_1 = \cdots = y_p = 0}$$

has rank n. *Let* M' *be any nonsingular* $n \times n$*-submatrix of* M. *Then* c *as in Lemma* 3.3 *can be computed by solving for each* d, $r \leqslant d \leqslant s$, $\binom{p+d}{p}$ *systems of linear equations with coefficient matrix* M'.

Proof. (i) We can assume that $\phi(i) = i$ for $1 \leqslant i \leqslant n$. For $1 \leqslant i \leqslant m$ and $u \in K$ we set

$$e_{iu} = \frac{\partial f_i}{\partial x_{iu}}(b)\bigg|_{y_1 = \cdots = y_p = 0},$$

and for any $u \in \mathbf{Z}^p$ we define

$$y^u = \begin{cases} y_1^{u_1} \cdots y_p^{u_p} & \text{if } u \in \mathbf{N}^p, \\ 0 & \text{otherwise.} \end{cases}$$

For $d \geqslant 0$, let $U_d = \{u \in \mathbf{N}^p : u_1 + \cdots + u_p = d\}$, so that

$$H_d = \bigoplus_{u \in U_d} y^u F \subset R$$

is the $\binom{p+d}{p}$-dimensional F-vector space of homogeneous polynomials of degree d. We want to compute some $c = (c_1, \ldots, c_m) \in R^m$ satisfying the condition of Lemma 3.3. Write $c_i = \sum_{r \leqslant l \leqslant s} c_{i,k+l}$ with $c_{ij} \in H_j$, and set $c_i = 0$ for $n < i \leqslant m$. We can compute $(c_{ij})_{1 \leqslant i \leqslant n}$ consecutively for $j = k + r, \ldots, k + s$ by requiring that

$$\forall i \leqslant n \quad f_i(a) + \sum_{w \in W} \frac{\partial f_i}{\partial x_w}(b) x_w \left(\sum_{r \leqslant l \leqslant j} (c_{1,k+l}, \ldots, c_{n,k+l}) \right)$$
$$\in \left(m_0^{j-k}\right)^m \subseteq R^m,$$

where $m_0^{j-k} = \{a \in R : v(a) \geqslant 2^{-(j-k)}\}$. In order to perform this computation it suffices that the linear mapping

$$\psi_d : H_{k+d}^m \to H_d^n$$
$$z \mapsto \left(\sum_{u \in K} e_{iu} x_{(i,u)}(z) \right)_{1 \leqslant i \leqslant n}$$

be surjective for $d \geqslant 0$, and for this in turn it is sufficient that the linear mapping

$$\psi_{id} : H_{k+d} \to H_d$$
$$z \mapsto \sum_{u \in K} e_{iu} D_1^{u_1} \cdots D_p^{u_p}(z)$$

be surjective for all $i \leqslant n$. Fix some i, $1 \leqslant i \leqslant n$, and let $t \in \mathbf{N}^p$ be minimal with respect to the lexicographical order $\prec$ on $\mathbf{N}^p$ such that $t \in K$ and $e_{it} \neq 0$. For $v \in U_d$, $u \in U_k$ the trivial fact ($u \prec t$ or $u = t$ or $t \prec u$) implies that $e_{iu} = 0$ or $u = t$ or $D_1^{u_1} \cdots D_p^{u_p}(y^{v+t})$ is a multiple of y^{v+t-u}. Thus

$$\psi_{id}(y^{v+t}) = e_{it}(v_1 + t_1)_{t_1} \cdots (v_p + t_p)_{t_p} y^v + \sum_{\substack{u \in K \\ v+t-u \prec v}} e_{iu}(v_1 + t_1)_{u_1} \cdots (v_p + t_p)_{u_p} y^{v+t-u}.$$

Using $v = (0, \ldots, 0, d)$, this shows that $y_p^d \in \mathrm{Im}(\psi_{id})$, and by induction on the lexicographical order that

$$\forall v \in U_d \quad y^v \in \mathrm{Im}(\psi_{id}),$$

hence $H_d = \mathrm{Im}(\psi_{id})$.

Thus the computation of the coefficients of $c_{ij} \in H_j$ proceeds according to the lexicographical order on U_{j-d}, solving a triangular system of linear equations whose diagonal entries are all nonzero integer multiples of e_{it}.

(ii) We can assume $n = m$ and write

$$c = (c_1, \ldots, c_n), \qquad c_i = \sum_{\substack{r \leqslant d \leqslant s \\ u \in U_d}} c_{iu} y^u.$$

Computing for consecutive $d = r, r+1, \ldots$ the c_{iu} (for all $u \in U_d$), we find the system of equations

$$\forall i \leqslant n \quad 0 = \sum_{1 \leqslant j \leqslant n} M_{ij} c_{ju} + \text{coefficient at } y^u \text{ of } \left(f_i(a) + \sum \frac{\partial f_i}{\partial x_{(j,0,\ldots,0)}}(b) \sum_{\substack{l \prec d \\ v \in U_l}} c_{jv} y^v \right). \quad \square$$

4. Short Vectors in Modules. In Section 5, we will consider the problem of factoring polynomials over a valuation ring. Lenstra-Lenstra-Lovász [1982] introduced the technique of computing short vectors in $\mathbf{Z}$-modules ("lattices") to obtain a polynomial-time factorization algorithm for univariate integer polynomials. In this section, we consider this technique in the context of valuation rings. We present an algorithm that computes a shortest vector in a non-Archimedean valuation module.

4.1. *Definition.* A nontrivial valuation $w\colon R \to \mathbf{R}$ is called a Euclidean valuation if there exists β, $0 < \beta < 1$, such that

$$E_1\colon \quad \forall a \in R \quad (a \neq 0 \Rightarrow w(a) \geqslant 1),$$
$$E_2\colon \quad \forall a, b \in R \quad \exists q \in R \quad (b \neq 0 \Rightarrow w(a - qb) \leqslant \beta w(b)).$$

R is then called a Euclidean valuation ring. (The reason for calling the valuation w rather than v will become clear in the next section.)

Condition E_2 says that division with remainder is possible, with the remainder having value at most β times the value of the divisor. Such a ring is then Euclidean (in the usual sense), and the Euclidean algorithm to compute a greatest common

divisor of $a, b \in R$ takes at most

$$1 + \frac{\log(w(b))}{\log(1/\beta)} = O(\log w(b))$$

division steps. We have two standard examples of Euclidean valuation rings: $\mathbf{Z}$ with the absolute value, and $F[y]$ with $w(f) = 2^{\deg f}$, where F is a field. In both cases we can choose $\beta = 1/2$.

4.2. *Remark.* We could also define a "pseudo-Euclidean valuation ring" in which only pseudo-division is required. That is, E_2 is replaced by

$$\forall a, b \in R \quad \exists c, q \in R \quad b \neq 0 \Rightarrow w(c) = 1 \quad \text{and} \quad w(ca - qb) \leqslant \beta w(b).$$

If F is an integral domain, then $F[y]$ with $w(f) = 2^{\deg f}$ would satisfy this requirement.

4.3. *Definition.* Let $f_1, \ldots, f_n \in R^n$, $M = \sum_{1 \leqslant i \leqslant n} f_i R \subseteq R^n$ the R-module generated by $f_1, \ldots, f_n$, and write $f_i = (f_{i1}, \ldots, f_{in})$ with $f_{ij} \in R$. We call

$$w(M) = w\Big(\det\big((f_{ij})_{i,j}\big)\Big) \in \mathbf{R}$$

the value of M.

One easily verifies that $w(M)$ is well-defined: $f_1, \ldots, f_n$ are linearly independent over the quotient field of R iff $w(M) \neq 0$. If $w(M) \neq 0$, then any other sequence of n vectors generating M differs from $(f_1, \ldots, f_n)$ by a linear transformation which is invertible over R. The determinant d of this transformation has $w(d) = 1$, using E_1.

Definition 4.3 is really a special case of a more general notion. For any R-module M and $n \geqslant 0$ one can consider the exterior power $\Lambda^n M$. This is again an R-module (see, e.g., Bourbaki [1958, Chapter 3, 5.5]). If $M \subseteq R^n$, then $\Lambda^n M \subseteq \Lambda^n R^n \cong R$ is an ideal, and in the case of Definition 4.3 we have

$$w(M) = \min\{w(a) : a \in \Lambda^n M \setminus \{0\}\},$$

if $\Lambda^n M \neq 0$. We note the following

4.4. LEMMA. *Let $N \subseteq M \subseteq R^n$ be R-modules. Then either $w(N) = 0$ or $w(M) \leqslant w(N)$.*

1. *Proof.* Let $f_1, \ldots, f_n$ and $g_1, \ldots, g_n$ generate M and N, respectively. Then there exist $a_{ij} \in R$ $(1 \leqslant i, j \leqslant n)$ such that $g_i = \sum_{1 \leqslant j \leqslant n} a_{ij} f_j$. Thus

$$w(N) = w\big(\det(g_{ik})\big) = w\big(\det(a_{ij})\det(f_{jk})\big) = w\big(\det(a_{ij})\big) w(M).$$

By condition E_1, either $w(\det(a_{ij})) = 0$ or $w(\det(a_{ij})) \geqslant 1$.

2. *Proof.* The functoriality of Λ^n implies $\Lambda^n N \subseteq \Lambda^n M$. Thus either $\Lambda^n N = 0$ or $w(M) \leqslant w(N)$. □

Recall the norms w_q on R^n for $1 \leqslant q \leqslant \infty$ from Definition 3.2.

4.5. LEMMA (HADAMARD'S INEQUALITY). *Let M be the module generated by $f_1, \ldots, f_n \in R^n$. Then*

(i) $w(M) \leqslant \prod_{1 \leqslant i \leqslant n} w_2(f_i)$,

(ii) *If w is non-Archimedean, then $w(M) \leqslant \prod_{1 \leqslant i \leqslant n} w_\infty(f_i)$.*

Proof. If w is Archimedean, then $R \subseteq \mathbf{C}$ and w is the absolute value (Ostrowski [1918]). (i) is the usual Hadamard inequality (see, e.g., Knuth [1981, 4.6.1]). If w is non-Archimedean, then

$$w(M) = w\Big(\sum_{\pi \in S_n} f_{1,\pi 1} \cdots f_{n,\pi n}\Big)$$
$$\leqslant \max_{\pi \in S_n} w(f_{1,\pi 1}) \cdots w(f_{n,\pi n}) \leqslant w_\infty(f_1) \cdots w_\infty(f_n). \quad \square$$

We now consider the computational problem of finding a short vector in an R-module. Lenstra-Lenstra-Lovász [1982] presented an algorithm for $R = \mathbf{Z}$ with the absolute value. In the remainder of this section, we restrict attention to non-Archimedean valuations. In this setting, a more powerful result is possible than in the Archimedean case: one can efficiently compute a shortest vector. This has been used in Chistov-Grigoryev [1982] and Lenstra [1983] for factoring multivariate polynomials over finite fields. The method presented here generalizes Lenstra's approach.

For the rest of this section, let R be a ring with a non-Archimedean Euclidean valuation w. For $n \geqslant 1$, we write $w = w_\infty : R^n \to \mathbf{R}$.

4.6. *Definition.* We call a sequence $(f_1, \ldots, f_n)$ with $f_i = (f_{i1}, \ldots, f_{in}) \in R^n$ *reduced* if $f_1, \ldots, f_n$ are linearly independent over the quotient field of R, and the following hold for all i, j, $1 \leqslant i \leqslant j \leqslant n$:

$$R_1: \quad w(f_i) = w(f_{ii}),$$
$$R_2: \quad w(f_i) \leqslant w(f_j),$$
$$R_3: \quad w(f_{ji}) < w(f_{jj}) \quad \text{if } i \neq j.$$

The assumption of linear independence is not essential; the development of this section goes through with minor modifications in the general case.

4.7. THEOREM. *Let $(f_1, \ldots, f_n)$ be reduced, and $M \subseteq R^n$ the module generated. Then*

$$w(f_1) = \min\{w(m) : m \in M \setminus \{0\}\}.$$

Proof. Let

$$x = (x_1, \ldots, x_n) = \sum_{1 \leqslant i \leqslant n} r_i f_i \in M \setminus \{0\}$$

with $r_1, \ldots, r_n \in R$. Let $u = \max\{w(r_i f_i) : 1 \leqslant i \leqslant n\}$ and $k = \min\{i : w(r_i f_i) = u\}$. We consider

$$x_k = r_k f_{kk} + \sum_{1 \leqslant j < k} r_j f_{jk} + \sum_{k < j \leqslant n} r_j f_{jk}.$$

If $j < k$, then

$$w(r_j f_{jk}) \leqslant w(r_j) w(f_j) < u = w(r_k f_{kk}),$$

using condition (R_1). If $k < j$, then

$$w(r_j f_{jk}) < w(r_j) w(f_{jj}) = w(r_j f_j) \leqslant u.$$

Thus in both cases, $w(r_j f_{jk}) < u = w(r_k f_{kk})$, and hence

$$w(f_1) \leqslant w(f_k) = w(f_{kk}) \leqslant w(r_k f_{kk}) = w(x_k) \leqslant w(x),$$

where the last equality uses the fact that w is non-Archimedean. $\square$

We now present an algorithm that transforms $f_1,\dots,f_n \in R^n$ into a reduced sequence generating the same module.

Algorithm REDUCED BASIS.

Input: $f_1,\dots,f_n \in R^n$ linearly independent, where R is a Euclidean valuation ring.

Output: A reduced sequence $(g_1,\dots,g_n)$ and an $n \times n$-permutation matrix A such that $Ag_1,\dots,Ag_n$ generate the R-module $M = \sum f_i R$.

1. Set $k = 1$, $A = \mathrm{Id}$, and $g_i = f_i$ for $1 \leqslant i \leqslant n$.
2. Do steps 3 to 7 while $k \leqslant n$.
3. Choose m, $k \leqslant m \leqslant n$, with
$$w(g_m) = \min\{w(g_i): k \leqslant i \leqslant n\} = u,$$
and interchange g_k and g_m.
4. Do step 5 for $i = k-1,\dots,1$.
5. Find $q \in R$ such that
$$w(g_{ki} - qg_{ii}) \leqslant \beta w(g_{ii}),$$
and replace g_k by $g_k - qg_i$. (We will see that $g_{ii} \neq 0$.)
6. If $w(g_k) = u$, then interchange two columns from $k,\dots,n$ such that $w(g_k) = w(g_{kk})$ after the interchange. (We will see that $w(g_{ki}) < u$ for $1 \leqslant i < k$, so that the interchange is possible.) If B is the matrix of this column permutation, replace A by AB. Replace k by $k+1$.
7. If $w(g_k) < u$, then replace k by
$$\max\{i: i = 1 \text{ or } (1 \leqslant i < k \text{ and } w(g_i) \leqslant w(g_k))\}.$$
8. Return $(g_1,\dots,g_n)$ and A.

4.8. THEOREM. *Let $f_1,\dots,f_n \in R^n$ be linearly independent over the quotient field of the Euclidean valuation ring R. With this input,* REDUCED BASIS *has the following properties:*

(i) *It correctly computes a reduced sequence $(g_1,\dots,g_n)$ with $g_i \in R^n$, and an $n \times n$-permutation matrix A such that*
$$\sum_{1 \leqslant i \leqslant n} (Ag_i)R = \sum_{1 \leqslant i \leqslant n} f_i R.$$

(ii) *If $w(f_i) \leqslant W$ for all i, $1 \leqslant i \leqslant n$, then it uses $O(n^4 \log W)$ operations in R.*

Proof. Throughout the algorithm, the R-module generated by $g_1,\dots,g_n$ remains unchanged except in step 6. But if $\sum_{1 \leqslant i \leqslant n} Ag_i R = \sum_{1 \leqslant i \leqslant n} f_i R$ and $B(\bar{g}_1,\dots,\bar{g}_n) = (g_1,\dots,g_n)$, then
$$\sum_{1 \leqslant i \leqslant n} (AB\bar{g}_i)R = \sum_{1 \leqslant i \leqslant n} f_i R.$$
(Read the transpose of a vector whenever necessary.) In particular, the last claim in (i) follows, and each g_i computed in the algorithm is nonzero.

For $1 \leqslant k \leqslant n+1$, call a sequence $(g_1,\dots,g_n)$ k-reduced if conditions R_1, R_2, R_3 hold for all i, j with $1 \leqslant i \leqslant j < k$, and $w(g_i) \leqslant w(g_j)$ for $1 \leqslant i < k \leqslant j \leqslant n$. Thus "$(n+1)$-reduced" is the same as "reduced". We now show the following claim: Each time the algorithm passes through step 2, $(g_1,\dots,g_n)$ is k-reduced (with the current value of k).

Correctness then follows (using (ii)), since the algorithm terminates in step 2 with $k = n + 1$.

At the first pass through step 2, $k = 1$ and the claim is trivial.

After passing through step 2, steps 3, 4, 5 do not affect the first $k - 1$ rows or columns. The claim and $g_i \neq 0$ imply $g_{ii} \neq 0$ for $i < k$, so that step 5 can be executed. Either the condition in step 6 or the condition in step 7 is satisfied, but not both. If step 7 is applicable, then clearly the claim is satisfied at the next pass through step 2. It is now sufficient to show that $w(g_{ik}) < u$ for $1 \leqslant i < k$ in step 6, since then the claim is true in the next pass through step 2.

So fix some i, $1 \leqslant i < k$, and consider $q \in R$ as computed in step 5. It is sufficient to show that

$$w((g_k - qg_i)_j) \leqslant w(g_k) \quad \text{for } 1 \leqslant j < k,$$
$$w((g_k - qg_i)_i) < w(g_k).$$

The choice of q implies that

$$\begin{aligned} w(g_{ki}) &= w(qg_{ii}) = w(q)w(g_i), \\ w(g_{ki} - qg_{ii}) &\leqslant \beta w(g_{ii}) < w(g_{ii}) = w(g_i) \leqslant w(g_k), \\ w(g_{kj} - qg_{ij}) &\leqslant \max\{w(g_{kj}), w(q)w(g_{ij})\} \\ &\leqslant \max\{w(g_k), w(q)w(g_i)\} = w(g_k) \end{aligned}$$

for $1 \leqslant j \leqslant n$.

For (ii), consider the function $s = \prod_{1 \leqslant i \leqslant n} w(g_i)$. Initially, $s \leqslant W^n$. By what we just proved, s does not increase in step 5. But then s does not ever increase in the algorithm. It strictly decreases by a factor $\leqslant \beta$ if the condition in step 7 is satisfied. Otherwise step 6 is applicable, where k increases by 1. Since $k \leqslant n + 1$, the total number of passes through steps 6 and 7 is $O(n \log_{1/\beta}(W^n))$ or $O(n^2 \log W)$.

The only computations in R of the algorithm are in step 5, which has one division with remainder and n multiplications and subtractions. Thus each pass through step 6 or 7 requires $O(n^2)$ operations, taking the loop of step 4 into account. □

5. Factorization of Polynomials. In this section we describe an algorithm for factoring polynomials over a ring with valuations. We view as the goal of a factorization procedure for polynomials from $R[x]$ (where R is an integral domain with quotient field K) to find, given $f \in R[x]$, polynomials $f_1, \ldots, f_r \in R[x]$ which are irreducible in $K[x]$ and such that $f = af_1 \cdots f_r$ for some $a \in K$. For a somewhat "axiomatic" description of the factoring algorithm we shall want to use the following ingredients.

Suppose we have a ring R with a set V of valuations, and a further valuation w, and also $B_u \in \mathbf{R}$ for $u \in V$ and $B \in \mathbf{R}$. Then $((B_u), B)$ is called an *inverse bound* (for V and w) if

$$\forall a \in R \quad (w(a) < B \text{ and } \forall u \in V \; u(a) \leqslant B_u) \Rightarrow a = 0.$$

5.1. *Definition.* A ring R with a set V of nontrivial Hensel valuations and a Euclidean valuation w is called a ring with sufficient valuations if the following conditions are satisfied.

S_1 (*Modular factorization*): For $v \in V$, consider the maximal ideal $m_v = \{a \in R: v(a) < 1\}$ in R. We assume an effective factorization procedure in $(R/m_v)[x]$, and $p_v \in R$ such that $m_v = p_v R$. (Note that R/m_v is a field.)

S_2 (*Inverse bounds*): For any $b \in R$ one can effectively find $v \in V$ such that $v(b) = 1$. Set $\varepsilon = v(p_v)$. For any $B \in \mathbf{R}$ one can effectively compute an $N \in \mathbf{N}$ such that with

$$B_u = \begin{cases} \varepsilon^N & \text{if } u = v, \\ 1 & \text{if } u \in V \setminus \{v\}, \end{cases}$$

$((B_u), B)$ is an inverse bound for V and w.

S_3 (*Gauss lemma*): Let K be the quotient field of R. For any $f \in K[x]$ one can effectively compute $a \in R \setminus \{0\}$ such that for any monic $g \in K[x]$ dividing f (in $K[x]$) we have $ag \in R[x]$.

We shall show that for a ring R with sufficient valuations one can efficiently compute the factorization of any polynomial from $R[x]$.

We did not want to assume that R is a unique factorization domain, so that our methods also apply, e.g., to rings of integers in number fields. However, for a ring R with sufficient valuations, $R[x]$ has a property almost as strong as unique factorization (and which might be called unique "pseudo-factorization"). For every $f \in R[x]$, there exist $f_1, \ldots, f_r \in K[x]$ irreducible monic and $a \in R$ such that $af_i \in R[x]$ and $a^r f = \operatorname{lc}(f)(af_1) \cdots (af_r)$ in $R[x]$. Here a comes from the Gauss lemma S_3, $\operatorname{lc}(f)$ is the leading coefficient of f, K is the quotient field of R, and $f_1, \ldots, f_r$ are unique (up to permutations).

5.2. *Example*. Let us first examine what the above ingredients are in the paradigm $R = \mathbf{Z}$. We take the absolute value for w and the set of p-adic valuations v_p for V ($p \in \mathbf{N}$ prime). Then the product formula holds

$$\forall a \in \mathbf{Z} \setminus \{0\} \quad w(a) \prod_{v \in V} v(a) = 1,$$

and for any prime number p and $k \in \mathbf{N}$ the following is an inverse bound for V and w

$$B_u = \begin{cases} p^{-k} & u = v_p, \\ 1 & \text{otherwise}, \end{cases} \qquad B = p^k.$$

The term "inverse bound" is motivated by this situation where either $\prod_{v \in V} v(a) = w(a)^{-1}$ or $a = 0$. The relevance of the product formula for factorization is pointed out in Trotter [1980]. Modular factorization is given by Berlekamp's algorithm, and $m_{v_p} = p\mathbf{Z}$. In S_2, with $v = v_p$, any N such that $B \leqslant p^N$ is sufficient. If $f \in \mathbf{Q}[x]$, $b \in \mathbf{Z}$ and $bf \in \mathbf{Z}[x]$, then $a = b \operatorname{lc}(f)$ satisfies the Gauss lemma S_3.

5.3. *Example*. The polynomial ring $R = F[y]$ over a field F fits into the picture as follows: We take the set

$$V = \{v_p : p \in F[y] \text{ monic irreducible}\}$$

of p-adic valuations on R as in Example 2.3, and for w the degree valuation with $w(f) = 2^{\deg f}$ (and $w(0) = 0$). Then again a product formula holds:

$$\forall a \in R \setminus \{0\} \quad w(a) \prod_{v \in V} v(a) = 1.$$

Thus for any $v_p \in V$ and $k \in \mathbf{N}$ the following is an inverse bound:

$$B_u = \begin{cases} 2^{-k \deg p} & \text{if } u = v_p, \\ 1 & \text{otherwise,} \end{cases} \qquad B = 2^{k \deg p}.$$

If F is infinite, then it is sufficient to take the subset

$$V' = \{v_p : \exists a \in F \text{ such that } p = y - a\}$$

of V. If F is finite, then with this V' the halting condition will not be satisfied; this fact manifests itself in the necessity for field extensions—given by R/m_v with $v \in V \setminus V'$—when factoring bivariate polynomials over finite fields (Chistov-Grigoryev [1982], Lenstra [1983], von zur Gathen-Kaltofen [1983]).

We first remark that one of the assumptions follows from the others.

5.4. LEMMA. *Condition E_1 for w is a consequence of the other assumptions.*

Proof. We have to show that $w(a) \geqslant 1$ for all $a \in R \setminus \{0\}$. So assume that $w(a) < 1$ for some $a \in R \setminus \{0\}$. Set $B = 1$, and use the halting condition to find $v \in V$, $\varepsilon > 0$, $N \in \mathbf{N}$ and the corresponding $B_u \in \mathbf{R}$ (for $u \in V$) such that $((B_u), B)$ is an inverse bound. Since v is nontrivial and $v(b) \leqslant 1$ for all $b \in R$, we can choose a $b \in R$ such that $0 < v(b) < 1$. Also choose $k \geqslant 1$ such that $w(a)^k w(b) < 1$, and set $c = a^k b$. Then

$$v(c^N) = v(a^{kN}) v(b^N) \leqslant v(b)^N \leqslant \varepsilon^N = B_v,$$

$$w(c^N) = \left(w(a)^k w(b)\right)^N < 1 = B.$$

It follows that $a^{kN} b^N = c^N = 0$, contradicting the fact that $a, b \neq 0$ and R is an integral domain. □

The following lemma will provide the connection between short vectors in modules and polynomial factorization. For $f, h \in R[x]$, $v \in V$ and $\varepsilon \geqslant 0$, we say that h divides f with precision ε (with respect to v) if $v(f - sh) \leqslant \varepsilon$ for some $s \in R[x]$ with $\deg s \leqslant \deg f - \deg h$. Throughout this section we consider the norm $w_q : R^n \to \mathbf{R}$ with $q = 2$ if w is Archimedean, and $q = \infty$ otherwise. For any n, we identify a polynomial in $R[x]$ of degree less than n with its coefficient vector in R^n.

5.5. LEMMA. *Let $f, g, h \in R[x]$ have positive degrees n, m, k, respectively, $v \in V$, and suppose that h is monic and divides both f and g with precision ε (with respect to v). Let $((B_u), B)$ be an inverse bound, and assume that $B_u = 1$ for $u \neq v$, $\varepsilon \leqslant B_v < 1$ and $w_q(f)^m w_q(g)^n < B$. Then f and g have a nontrivial common factor in $K[x]$, where K is the quotient field of R.*

Proof. The lemma is trivial if $\varepsilon = 0$. We also have $\varepsilon < 1$. So assume $\varepsilon > 0$, and let $p \in R$, $l \in \mathbf{N}$ with $m_v = pR$ and

$$v(p^l) \leqslant \varepsilon < v(p^{l-1}).$$

Consider the R-module $M \subseteq R^{m+n}$ generated by

$$\{p^l x^i : 0 \leqslant i < k\} \cup \{h x^i : 0 \leqslant i < m + n - k\}.$$

For any $r \in R[x]$ of degree $< m + n$ we have

$$\begin{aligned} &h \text{ divides } r \text{ with precision } \varepsilon \\ &\Leftrightarrow \exists s \in R[x] \text{ such that } \deg s < m + n - k \quad \text{and} \quad v(hs - r) \leqslant \varepsilon \\ &\Leftrightarrow r \in M. \end{aligned}$$

The generators for M form an upper triangular matrix, with p^l and 1 on the diagonal. Let d be the determinant of that matrix. Then $d = p^{lk}$, $w(M) = w(d)$, and

$$v(d) = v(p)^{lk} \leqslant \varepsilon^k \leqslant B_v.$$

Now consider the module $N \subseteq R^{m+n}$ generated by

$$\{fx^i : 0 \leqslant i < m\} \cup \{gx^i : 0 \leqslant i < n\}.$$

By assumption, each fx^i and gx^i is in M, hence $N \subseteq M$. If $w(N) \neq 0$, then

$$w(d) = w(M) \leqslant w(N) \leqslant w_q(f)^m w_q(g)^n < B$$

(using Lemmas 4.4 and 4.5), and hence $d = 0$ by S_2, contradicting the linear independence of the generators of M. Thus $w(N) = 0$ and hence N has rank $< n + m$. There exist $s_0, \ldots, s_{m-1}, t_0, \ldots, t_{n-1} \in R$, not all zero, such that

$$\sum_{0 \leqslant i < m} s_i f x^i + \sum_{0 \leqslant i < n} t_i g x^i = 0.$$

Then for $s = \sum_{0 \leqslant i < m} s_i x^i$, $t = \sum_{0 \leqslant i < n} t_i x^i \in R[x]$ we have $sf + tg = 0$. This implies that $\gcd(f, g)$ is nontrivial in $K[x]$. □

We now present an algorithm for factoring polynomials in $R[x]$. We assume a nondecreasing function τ: $\mathbf{N} \to \mathbf{R}$ and a short vector algorithm which, given $f_1, \ldots, f_n \in R^n$ linearly independent, computes $x \in \sum f_i R = M$ such that

$$\forall y \in M \setminus \{0\} \quad w_q(x) \leqslant \tau(n) w_q(y).$$

If w is non-Archimedean, then we can take our algorithm REDUCED BASIS and $\tau(n) = 1$. If w is the absolute value on $R = \mathbf{Z}$, then we can take the short vector algorithm from Lenstra-Lenstra-Lovász [1982] and $\tau(n) = 2^{(n-1)/2}$.

Algorithm FACTOR.

Input: A polynomial $f \in R[x]$, where R is a ring with sufficient valuations (V, w).

Output: If f is reducible, then (e, a), where $a \in R$, and $e \in R[x]$ is a proper factor of $a^2 f$.

1. Compute $a \in R$ as in S_3, set $n = \deg f$,

$$C = \begin{cases} w(2^n) w_2(f) & \text{if } w \text{ is Archimedean,} \\ w_\infty(f) & \text{otherwise,} \end{cases}$$

and $B = (C^2 w(a) \tau(2n))^n + 1$.

2. Take $b = a \cdot \operatorname{discr}(f)$, find v, ε, N, and B_u for $u \in V$ as in S_2, and $p \in R$ such that $m_v = pR$ (using S_1). (Then $v(b) = 1$, $\varepsilon = v(p)$ and $B_v = \varepsilon^N$.)
3. Compute a factorization $f \equiv f_0 f_1 \bmod m_v$ in $(R/m_v)[x]$, with $f_0, f_1 \in R[x]$, and f_1 monic and irreducible in $(R/m_v)[x]$.
4. Use Hensel's lemma to get a factorization $f \equiv F_0 F_1 \bmod m_v^N$ in $(R/m_v^N)[x]$, with $F_0, F_1 \in R[x]$, F_1 monic, and $F_i \equiv f_i \bmod m_v$.

5. Set $k = \deg F_1$. For $m = k, \ldots, n-1$ do steps 6 and 7.
6. Consider the R-module $M \subseteq R^{m+n}$ generated by
$$\{p^N x^i : 0 \leqslant i < k\} \cup \{F_1 x^i : 0 \leqslant i < m+n-k\}.$$
Apply the short vector algorithm to find a short vector $g \in M$.
7. Compute the monic polynomial $e_1 = \gcd(f, g) \in K[x]$. If $e_1 \neq 1$ and $\deg e_1 < n$, then return (e, a) with $e = ae_1$, and stop.
8. Return "f is irreducible".

5.6. THEOREM. *Assume that R is a ring with sufficient valuations, and $f \in R[x]$ of degree n is reducible. Then algorithm* FACTOR *returns a proper factor $e \in R[x]$ of $a^2 f$ (with $a \in R$ as in S_3).*

Proof. If e is returned from step 7, then there exists some monic $u \in K[x]$ such that $f = \mathrm{lc}(f) e_1 u$. Then $a^2 f = \mathrm{lc}(f) \cdot e \cdot au$ is a factorization in $R[x]$. All we have to show is that if f is reducible (in $K[x]$), then e is indeed returned from step 7. So we can assume that $g_0 \in K[x]$ is a monic irreducible factor of f, $g_1 = ag_0 \in R[x]$ and f_1 divides g_1 with precision ε, i.e. $f_1 \bmod p$ divides $g_1 \bmod p$ in $R/m_v[x]$. The fact that $v(b) = 1$ implies that $f \bmod p$ is squarefree and $\gcd(f_0, f_1) \equiv 1 \bmod m_v$, and we can find $s_0, s_1 \in R[x]$ such that the conditions H_1, H_2, H_3 of the Hensel lemma hold with $z = 1$, $\alpha = 1$, $\delta = \varepsilon$. Thus we can execute step 4, and the uniqueness property of Hensel's lemma (Corollary 2.9) implies that F_1 divides g_1 with precision ε^N.

As usual, we set $q = 2$ if w is Archimedean, and $q = \infty$ otherwise. By Lemma 5.7 below, we have
$$w_q(g_1) = w(a) w_q(g_0) \leqslant w(a) C.$$
Consider now the module M in step 6 with $m = \deg g_1$, and the short vector $g \in M$. Thus M consists of those polynomials in $R[x]$ of degree $< m+n$ which F_1 divides with precision ε^N. In particular, $g_1 \in M$ and
$$w_q(g) \leqslant \tau(n+m) w_q(g_1) \leqslant w(a) \tau(2n) C.$$
It follows that
$$w_q(f)^m w_q(g)^n \leqslant w_q(f)^n (w(a)\tau(2n)C)^n < B,$$
and Lemma 5.5 (with F_1 for h) implies that $\gcd(f, g) \neq 1$ in $K[x]$. □

In the above proof, we used the following bound on factors of polynomials due to Mignotte [1974].

5.7. LEMMA. *Let $f, g \in K[x]$ be monic, $m = \deg g$, and $2 \leqslant q \leqslant \infty$, and suppose that g divides f. Then*
$$w_q(g) \leqslant w(2^m) w_2(f).$$
If w is non-Archimedean, then
$$w_\infty(g) \leqslant w_\infty(f).$$

Proof. We can assume $f = (x - c_1) \cdots (x - c_n)$ with $c_1, \ldots, c_n \in F$, since w extends (nonuniquely) to a valuation on some splitting field of f over F.

If w is Archimedean, then F is a subfield of $\mathbf{C}$ and w the restriction of the absolute value (Ostrowski [1918]), and Mignotte [1974] proves that with $g = \sum_{0 \leqslant i \leqslant m} g_i x^i$ we have

$$w(g_i) \leqslant \binom{m}{i} w_2(f)$$

for all i. Then

$$w_2(g) \leqslant w_2(f)\left(\sum_{0 \leqslant i \leqslant m} \binom{m}{i}^2\right)^{1/2} \leqslant w_2(f) \sum_{0 \leqslant i \leqslant m} \binom{m}{i} = 2^m w_2(f).$$

If w is non-Archimedean, then w_∞ is a valuation on $F[x]$, and

$$w_\infty(f) = w_\infty(x - c_1) \cdots w_\infty(x - c_n) = w(c_1 \cdots c_k)$$

if $w(c_1), \ldots, w(c_k) > 1$ and $w(c_{k+1}), \ldots, w(c_n) \leqslant 1$. Vieta's expression of g_i in terms of some of the c_j proves the claim. □

5.8. *Remark*. Let us estimate the running time of FACTOR. We will want to use the estimates in Proposition 2.10 and Theorem 4.8(ii). For those two estimates, however, different models were appropriate. In Proposition 2.10 we counted "basic operations"—essentially corresponding to bit operations if $R = \mathbf{Z}$ and to arithmetic operations in F if $R = F[y]$—and in Theorem 4.8 we counted arithmetic operations in R. Below, we outline an estimate for FACTOR in terms of both these counts. In order to establish an estimate in terms of "basic operations" only, one would first have to introduce bounds for the computations implicit in Definitions 4.1 and 5.1, and then bound the size of intermediate results. In specific examples ($\mathbf{Z}$ or $F[y]$) both steps are not too hard, but it is not clear which approach would make sense in the general setting. Thus we consider the procedures implied in Definition 5.1 as executed for free, and only count the arithmetic operations. They occur in steps 4, 6 and 7. By Proposition 2.10, step 4 takes $O(n^3 NT(\varepsilon^N))$ basic operations. For step 6, let us assume that there exist "small representatives" for R/m_v^N: for $v \in V$, $N \in \mathbf{N}$, and $a \in R$ there exists $b \in R$ such that $a \equiv b \bmod m_v^N$ and $w(b) \leqslant w(p_v)^N$. Such representatives clearly exist in our two paradigms $\mathbf{Z}$ and $F[y]$. We can give a time estimate for step 6 only for non-Archimedean w, since we only presented a short vector algorithm for this case. Then for the generators of the module M in step 6, we have $w(p^N x^i) = w(p)^N$ and, using representatives as above, also $w(F_1 x^i) = w(F_1) \leqslant w(p)^N$. It follows from Theorem 4.8 that step 6 can be performed in $O(n^4 N \log w(p))$ operations in R.

For the gcd in step 7, we can use a subresultant algorithm (Collins [1967], Brown [1971]) taking $O(n^4)$ operations in R.

5.9. *Remark*. It is easy to adapt the method to include the case of an algebraic number field K. Let R be its ring of integers, V the set of q-adic valuations, where $q \subseteq R$ is a prime ideal, and let the finite set W consist of the Archimedean valuations on R which are obtained from the absolute value on $\mathbf{C}$ via the different complex and real embeddings of K. Again, a Gauss lemma holds (but is not trivial as in $\mathbf{Z}$ or $F[y]$), and also a product formula (see e.g. Trotter [1980]). Chistov-Grigoryev [1982], Landau [1982], and Lenstra [1982] have factoring algorithms over algebraic number fields.

5.10. *Remark.* In order to apply the algorithm, we assumed that the input polynomial f is squarefree. If we can compute the "squarefree factorization" of an arbitrary polynomial, then we can apply our factorization algorithm, and the answer furnished will easily yield the factorization of the original polynomial. Computing this squarefree factorization is easy in characteristic zero and over finite fields. (See Knuth [1981, 4.6.2].)

In particular, one can effectively decide squarefreeness in characteristic zero provided that the arithmetic operations can be effectively executed. Things are different in positive characteristic. In the general case, computing the squarefree part of a polynomial boils down to computing pth roots in fields of characteristic $p > 0$. An adaptation of an argument by Fröhlich and Sheperdson [1956] shows that any general answer will have to take the representation of the field into account: let $S \subseteq \mathbf{N}$ be recursively enumerable, but not recursive, and $x, y_0, y_1, \ldots$ indeterminates over $\mathbf{Z}/2\mathbf{Z}$. Let $R = (\mathbf{Z}/2\mathbf{Z})[y_0, y_1, \ldots]$, and consider in the quotient field K of R the subfield F generated by $\{y_i\colon i \in \mathbf{N} \setminus S\} \cup \{y_i^2\colon i \in S\}$. Any algorithm that decides for any i whether $x^2 - y_i^2 \in F[x]$ is squarefree or not would yield an algorithm for deciding membership in S; hence no such algorithm exists. Note also that F is isomorphic to K, and it is easy to decide whether an $f \in K[x]$ is squarefree: we can assume that $f \in R[x]$ is primitive over R, and then f is squarefree if and only if $\gcd(f, \partial f/\partial x) = 1$ or there exists an $i \in \mathbf{N}$ such that $\gcd(f, \partial f/\partial y_i) = 1$.

5.11. *Remark.* The factorization algorithm makes essential use of the interplay between two valuations v and w on a ring R. A natural problem in this context is approximation: given some a in the completion of R with respect to v, and $\delta_1, \delta_2, \varepsilon \in \mathbf{R}$, find $b, c \in R$ such that $v(ac - b) \leqslant \varepsilon$ and $w(b) \leqslant \delta_1$, $w(c) \leqslant \delta_2$. This question includes rational approximation of real numbers, conversion of Hensel codes (see,e.g.,Miola [1982]), and Padé approximation of formal power series. Does there exist a general approximation algorithm that solves both these cases?

Department of Computer Science
University of Toronto
Toronto, Ontario, Canada M5S 1A4

E. R. BERLEKAMP, "Factoring polynomials over finite fields," *Bell System Tech. J.*, v. 46, 1967, pp. 1853–1859.

N. BOURBAKI, *Eléments de Mathématiques, Livre* II: *Algèbre*, Hermann, Paris, 1958.

W. S. BROWN, "On Euclid's algorithm and the computation of polynomial greatest common divisors," *J. Assoc. Comput. Math.*, v. 18, 1971, pp. 478–504.

A. L. CHISTOV & D. YU. GRIGORYEV, *Polynomial-Time Factoring of the Multivariable Polynomials Over a Global Field*, LOMI preprint E-5-82, Leningrad, 1982.

G. E. COLLINS, "Subresultants and reduced polynomial remainder sequences," *J. Assoc. Comput. Mach.*, v. 14, 1967, pp. 128–142.

A. FELLMANN, *Newton-Iteration über nicht-archimedisch bewerteten vollständigen Ringen*, Diplomarbeit, Zürich, 1977.

K. O. FRIEDRICHS, "Symmetric positive linear differential equations," *Comm. Pure Appl. Math.*, v. 9, 1958, pp. 333–418.

A. FRÖHLICH & J. C. SHEPHERDSON, "Effective procedures in field theory," *Philos. Trans. Roy. Soc. London Ser. A*, v. 248, 1955–56, pp. 407–432.

J. VON ZUR GATHEN, *Factoring Sparse Multivariate Polynomials*, Proc. 24th Annual IEEE Sympos. Foundations of Computer Science, Tucson, 1983, pp. 172–179.

J. VON ZUR GATHEN & E. KALTOFEN, *Polynomial-Time Factorization of Multivariate Polynomials Over Finite Fields*, Proc. 10th ICALP, Barcelona, 1983, pp. 250–263.

E. KALTOFEN, *A Polynomial-Time Reduction from Bivariate to Univariate Integral Polynomial Factorization*, Proc. 23rd Annual IEEE Sympos. Foundations of Computer Science, Chicago, 1982, pp. 57–64.

E. KALTOFEN, "Polynomial-time reduction from multivariate to bivariate and univariate integer polynomial factorization," *SIAM J. Comput.* (To appear.)

D. E. KNUTH, *The Art of Computer Programming*, Vol. 2, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

H. T. KUNG, "On computing reciprocals of power series," *Numer. Math.*, v. 22, 1974, pp. 341–348.

S. LANDAU, *Factoring Polynomials Over Algebraic Number Fields*, Manuscript, 1982.

A. K. LENSTRA, *Factoring Polynomials Over Algebraic Number Fields*, Preprint, Mathematisch Centrum, Amsterdam, 1982.

A. K. LENSTRA, *Factoring Multivariate Polynomials Over Finite Fields*, Proc. 15th ACM Sympos. Theory of Computing, Boston, 1983, pp. 189–192.

A. K. LENSTRA [83a], *Factoring Multivariate Integral Polynomials*, Proc. 10th ICALP, Barcelona, 1983, pp. 458–465.

A. K. LENSTRA, H. W. LENSTRA & L. LOVÁSZ, "Factoring polynomials with rational coefficients," *Math. Ann.*, v. 261, 1982, pp. 515–534.

M. MIGNOTTE, "An inequality about factors of polynomials," *Math. Comp.*, v. 28, 1974, pp. 1153–1157.

A. M. MIOLA, "The conversion of Hensel codes to their rational equivalents," *SIGSAM Bull.*, v. 16, 1982, pp. 24–26.

D. R. MUSSER, "Multivariate polynomial factorization," *J. Assoc. Comput. Mach.*, v. 22, 1975, pp. 291–308.

A. OSTROWSKI, "Ueber einige Lösungen der Funktionalgleichung $\varphi(x) \cdot \varphi(y) = \varphi(xy)$," *Acta Math.*, v. 41, 1918, pp. 271–284.

M. SIEVEKING, "An algorithm for division of powerseries," *Computing*, v. 10, 1972, pp. 153–156.

H. F. TROTTER, *Algebraic Numbers and Polynomial Factorization*, Lecture Notes for AMS short course, Ann Arbor, August 1980.

B. L. VAN DER WAERDEN, *Modern Algebra*, Vol. 1, Ungar, New York, 1970.

P. S. WANG, "An improved multivariate polynomial factoring algorithm," *Math. Comp.*, v. 32, 1978, pp. 1215–1231.

D. Y. Y. YUN, "Hensel meets Newton—Algebraic constructions in an analytic setting," In *Analytic Computational Complexity* (J. F. Traub, ed.), Academic Press, New York, 1976.

H. ZASSENHAUS, "On Hensel factorization. I," *J. Number Theory*, v. 1, 1969, pp. 291–311.

R. ZIPPEL, *Newton's Iteration and the Sparse Hensel Algorithm*, Proc. 1981 ACM Sympos. Symbolic and Algebraic Computation, Utah, 1981, pp. 68–72.