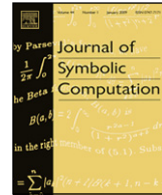




Contents lists available at SciVerse ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Detecting lacunary perfect powers and computing their roots

Mark Giesbrecht^{a,1}, Daniel S. Roche^b

^a Cheriton School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada

^b Department of Computer Science, United States Naval Academy, Annapolis, MD, USA

ARTICLE INFO

Article history:

Received 4 January 2009

Accepted 18 January 2010

Available online 5 September 2011

Keywords:

Sparse/lacunary polynomial

Perfect power

Black-box computation

ABSTRACT

We consider solutions to the equation $f = h^r$ for polynomials f and h and integer $r \geq 2$. Given a polynomial f in the lacunary (also called *sparse* or *super-sparse*) representation, we first show how to determine if f can be written as h^r and, if so, to find such an h . This is a Monte Carlo randomized algorithm whose cost is polynomial in the number of non-zero terms of f and in $\log \deg f$, i.e., polynomial in the size of the lacunary representation, and it works over $\mathbb{F}_q[x]$ (for large characteristic) as well as $\mathbb{Q}[x]$. We also give two deterministic algorithms to compute the perfect root h given f and r . The first is output-sensitive (based on the sparsity of h) and works only over $\mathbb{Q}[x]$. A sparsity-sensitive Newton iteration forms the basis for the second approach to computing h , which is extremely efficient and works over both $\mathbb{F}_q[x]$ (for large characteristic) and $\mathbb{Q}[x]$, but depends on a number-theoretic conjecture. Work of Erdős, Schinzel, Zannier, and others suggests that both of these algorithms are unconditionally polynomial-time in the lacunary size of the input polynomial f . Finally, we demonstrate the efficiency of the randomized detection algorithm and the latter perfect root computation algorithm with an implementation in the C++ library NTL.

© 2011 Elsevier Ltd. All rights reserved.

1. Introduction

In this paper we consider the problem of determining whether a polynomial f equals h^r for some other polynomial h and integer $r \geq 2$, and if so, finding h and r . The novel aspect of this current work

E-mail addresses: mwg@cs.uwaterloo.ca (M. Giesbrecht), roche@usna.edu (D.S. Roche).

¹ Tel.: +1 519 888 4567 36582; fax: +1 519 885 1208.

is that our algorithms are efficient for the *lacunary* (also called *sparse* or *supersparse*) representation of polynomials. Specifically, we write

$$f = \sum_{1 \leq i \leq t} c_i \bar{x}^{\bar{e}_i} \in F[x_1, \dots, x_\ell], \tag{1.1}$$

where F is a field, $c_0, \dots, c_t \in F \setminus \{0\}$, $\bar{e}_1, \dots, \bar{e}_t \in \mathbb{N}^\ell$ are distinct exponent tuples with $0 \leq \|\bar{e}_1\|_1 \leq \dots \leq \|\bar{e}_t\|_1 = \deg f$, and $\bar{x}^{\bar{e}_i}$ is the monomial $x_1^{e_{i1}} x_2^{e_{i2}} \dots x_\ell^{e_{i\ell}}$ of degree $\|\bar{e}_i\|_1 = \sum_{1 \leq j \leq \ell} e_{ij}$. We say f is t -sparse and write $\tau(f) = t$. We present algorithms which require time polynomial in $\tau(f)$ and $\log \deg f$.

Computational work on *lacunary* polynomials has proceeded steadily for the past three decades. From the dramatic initial intractability results of Plaisted (1977, 1984), through progress in algorithms (e.g., Ben-Or and Tiwari (1988), Shparlinski (2000) and Kaltofen and Lee (2003)) and complexity (e.g., Karpinski and Shparlinski (1999), Quick (1986) and von zur Gathen et al. (1993)), to recent breakthroughs in root finding and factorization (Cucker et al., 1999; Kaltofen and Koiran, 2006; Lenstra, 1999), these works have important theoretical and practical consequences. The lacunary representation is arguably more intuitive than the standard dense representation, and in fact corresponds to the default linked-list representation of polynomials in modern computer algebra systems such as Maple and Mathematica.

We will always assume that $\tau(f) \geq 2$; otherwise $f = x^n$, and determining whether f is a perfect power is equivalent to determining whether $n \in \mathbb{N}$ is composite, and to factoring n if we wish to produce r dividing n such that $f = (x^{n/r})^r$. Surprisingly, the intractability of the latter problem is avoided when $\tau(f) \geq 2$.

We first consider detecting perfect powers and computing the power r for the univariate case

$$f = \sum_{1 \leq i \leq t} c_i x^{e_i} \in F[x], \tag{1.2}$$

where $0 \leq e_1 < e_2 < \dots < e_t = \deg f$.

Two cases for the field F are handled: the integers and finite fields of characteristic p greater than the degree of f . When $f \in \mathbb{Z}[x]$, our algorithms also require time polynomial in $\log \|f\|_\infty$, where $\|f\|_\infty = \max_{1 \leq i \leq t} |c_i|$ (for $f \in \mathbb{Q}[x]$, we simply work with $\bar{f} = cf \in \mathbb{Z}[x]$, for the smallest $c \in \mathbb{Z} \setminus \{0\}$). This reflects the bit-length of coefficients encountered in the computations. Efficient techniques will also be presented for reducing the multivariate case to the univariate one, and for computing a root h such that $f = h^r$.

1.1. Related work and methods

Two well-known techniques can be applied to the problem of testing for perfect powers, and both are very efficient when $f = h^r$ is dense. We can compute the squarefree decomposition of f as in Yun (1976), and determine whether f is a perfect power by checking whether the greatest (integer) common divisor of the exponents of all nontrivial factors in the squarefree decomposition is at least 2. An even faster method (in theory and practice) to find h given $f = h^r$ is by a Newton iteration. This technique has also proven to be efficient in computing perfect roots of (dense) multi-precision integers (Bach and Sorenson, 1993; Bernstein, 1998). In summary however, we note that both these methods require approximately linear time in the *degree* of f , which may be exponential in the lacunary size.

Newton iteration has also been applied to finding perfect polynomial roots of lacunary (or other) polynomials given by straight-line programs. Kaltofen (1987) shows how to compute a straight-line program for h , given a straight-line program for $f = h^r$ and the value of r . This method has complexity polynomial in the size of the straight-line program for f , and in the degree of h , and in particular is effective for large r . We do not address the powerful generality of straight-line programs, but do avoid the dependence on the degree of h .

Closest to this current work, Shparlinski (2000) shows how to recognize whether $f = h^2$ for a lacunary polynomial $f \in \mathbb{F}_q[x]$. Shparlinski uses random evaluations and tests for quadratic residues. How to determine whether a lacunary polynomial is *any* perfect power is posed as an open question.

1.2. Our contributions

Given a lacunary polynomial $f \in \mathbb{Z}[x]$ with $\tau(f) \geq 2$ and degree n , we first present an algorithm to compute an integer $r > 1$ such that $f = h^r$ for some $h \in \mathbb{Z}[x]$, or determine that no such r exists. The algorithm requires $\tilde{O}(t \log^2 \|f\|_\infty \log^2 n)$ machine operations,² and is probabilistic of the Monte Carlo type. That is, for any input, on any execution the probability of producing an incorrect answer is strictly less than $1/2$, assuming the ability to generate random bits at unit cost. This possibility of error can be made arbitrarily small with repeated executions. Moreover, the error is one-sided, so we prove specifically that deciding whether a given multivariate rational polynomial encoded in the lacunary representation is a perfect power is in the complexity class coRP.

A similar algorithm is presented to answer Shparlinski's open question on perfect powers of lacunary polynomials over finite fields, at least for the case of large characteristic. That is, when the characteristic p of a finite field F is greater than $\deg f$, we provide a Monte Carlo algorithm that determines if there exists an $h \in F[x]$ and r such that $f = h^r$, and finds r if it exists, which requires $\tilde{O}(t \log^2 n)$ operations in F .

An implementation of our algorithm over \mathbb{Z} in NTL indicates excellent performance on sparse inputs when compared to a fast implementation based on previous technology (a variable-precision Newton iteration to find a power-series r th root of f , followed by a Monte Carlo correctness check).

Actually computing h such that $f = h^r$ is a somewhat trickier problem, at least insofar as bounds on the sparsity of h have not been completely resolved. Conjectures of Schinzel (1987) and recent work of Zannier (2007) suggest that, provided the characteristic of F is zero or sufficiently large, h is lacunary as well. To avoid this lack of sufficient theoretical understanding, we develop an algorithm which requires time polynomial in both the representation size of the input f (i.e., $\tau(f)$, $\log n$ and $\log \|f\|_\infty$) and the representation size of the output (i.e., $\tau(h)$ and $\log \|h\|_\infty$). This algorithm works by projecting f into a sequence of small cyclotomic fields. Images of the desired h in these fields are discovered by factorization over an algebraic extension. Finally, a form of interpolation of the sparse exponents is used to recover the global h . Thanks to an efficient perfect-root certification, this algorithm is deterministic and polynomial-time, however we do not claim it will be efficient in practice. Instead, we also present and analyze a simpler alternative based on a kind of sparse Newton iteration. Subject to what we believe is a reasonable conjecture, this is shown to be very fast.

It may be helpful to point out the differences between the detection algorithm in Section 2 and the computation algorithms in Section 3. While the former is probabilistic of the Monte Carlo type and does not actually produce the perfect r th root h of f if it exists, it provably works in polynomial-time even if h is dense. The computation algorithms, by contrast, are deterministic but rely on the unknown root h being sparse.

The remainder of the paper is arranged as follows. In Section 2 we present the main theoretical tool for our algorithm to determine if $f = h^r$, and to find r . We also show how to reduce the multivariate problem to the univariate one. In Section 3 we show how to compute h such that $f = h^r$ (given that such h and r exist). Finally, in Section 4, we present an experimental implementation of some of our algorithms in the C++ library NTL.

An earlier version of some of this work was presented in the ISSAC 2008 conference (Giesbrecht and Roche, 2008).

2. Testing for perfect powers

In this section we describe a method to determine if a lacunary polynomial $f \in F[x]$ is a perfect power. That is, do there exist $h \in F[x]$ and $r > 1$ such that $f = h^r$? The polynomial h need not be lacunary, though some conjectures suggest it may well have to be. We will find r , but not h .

We first describe algorithms to test if an $f \in F[x]$ is an r th power of some polynomial $h \in F[x]$, where f and r are both given and r is assumed to be prime. We present and analyze variants that work

² We employ soft-Oh notation: for functions σ and φ we say $\sigma \in \tilde{O}(\varphi)$ if $\sigma \in O(\varphi \log^c \varphi)$ for some constant $c \geq 0$.

over finite fields \mathbb{F}_q and over \mathbb{Z} . In fact, these algorithms for given r are for *black-box* polynomials: they only need to evaluate f at a small number of points. That this evaluation can be done quickly is a property of lacunary and other classes of polynomials.

For lacunary f we then show that, in fact, if h exists at all then r must be small unless $f = x^n$. And if f is a perfect power, then there certainly exists a prime r such that f is an r th power. So in fact the restrictions that r is small and prime are sufficient to cover all nontrivial cases, and our method is complete.

2.1. Detecting given r th powers

Our main tool in this work is the following theorem which says that, with reasonable probability, a polynomial is an r th power if and only if the modular image of an evaluation in a specially constructed finite field is an r th power.

Theorem 2.1. *Let $q \in \mathbb{Z}$ be a prime power and $r \in \mathbb{N}$ a prime dividing $q - 1$. Suppose that $f \in \mathbb{F}_q[x]$ has degree $n \leq 1 + \sqrt{q}/2$ and is not a perfect r th power in $\mathbb{F}_q[x]$. Then*

$$R_f^{(r)} = \#\{c \in \mathbb{F}_q : f(c) \in \mathbb{F}_q \text{ is an } r\text{th power}\} \leq \frac{3q}{4}.$$

Proof. The r th powers in \mathbb{F}_q form a subgroup H of \mathbb{F}_q^* of index r and size $(q - 1)/r$ in \mathbb{F}_q^* . Also, $a \in \mathbb{F}_q^*$ is an r th power if and only if $a^{(q-1)/r} = 1$. We use the method of “completing the sum” from the theory of character sums. We refer to Lidl and Niederreiter (1983), Chapter 5, for an excellent discussion of character sums. By a multiplicative character we mean a homomorphism $\chi : \mathbb{F}_q^* \rightarrow \mathbb{C}$ which necessarily maps \mathbb{F}_q^* onto the unit circle. As usual we extend our multiplicative characters χ so that $\chi(0) = 0$, and define the trivial character $\chi_0(a)$ to be 0 when $a = 0$ and 1 otherwise.

For any $a \in \mathbb{F}_q^*$,

$$\frac{1}{r} \sum_{\chi^r = \chi_0} \chi(a) = \begin{cases} 1 & \text{if } a \in H, \\ 0 & \text{if } a \notin H, \end{cases}$$

where χ ranges over all the multiplicative characters of order r on \mathbb{F}_q^* —that is, all characters that are isomorphic to the trivial character on the subgroup H . Thus

$$\begin{aligned} R_f^{(r)} &= \sum_{a \in \mathbb{F}_q^*} \left(\frac{1}{r} \sum_{\chi^r = \chi_0} \chi(f(a)) \right) = \frac{1}{r} \sum_{\chi^r = \chi_0} \sum_{a \in \mathbb{F}_q^*} \chi(f(a)) \\ &\leq \frac{q}{r} + \frac{1}{r} \sum_{\substack{\chi^r = \chi_0 \\ \chi \neq \chi_0}} \left| \sum_{a \in \mathbb{F}_q} \chi(f(a)) \right|. \end{aligned}$$

Here we use the obvious fact that

$$\sum_{a \in \mathbb{F}_q^*} \chi_0(f(a)) \leq \sum_{a \in \mathbb{F}_q} \chi_0(f(a)) = q - d \leq q,$$

where d is the number of distinct roots of f in \mathbb{F}_q . We next employ the powerful theorem of Weil (1948) on character sums with polynomial arguments (see Theorem 5.41 of Lidl and Niederreiter (1983)), which shows that if f is not a perfect r th power of another polynomial, and χ has order $r > 1$, then

$$\left| \sum_{a \in \mathbb{F}_q} \chi(f(a)) \right| \leq (n - 1)q^{1/2} \leq \frac{q}{2},$$

using the fact that we insisted $n \leq 1 + \sqrt{q}/2$. Summing over the $r - 1$ non-trivial characters of order r , we deduce that

$$R_f^{(r)} \leq \frac{q}{r} + \frac{r - 1}{r} \cdot \frac{q}{2} \leq \frac{3q}{4},$$

since $r \geq 2$. \square

2.2. Certifying specified powers over $\mathbb{F}_q[x]$

Theorem 2.1 allows us to detect when a polynomial $f \in \mathbb{F}_\rho[x]$ is a perfect r th power, for known r dividing $\rho - 1$: choose random $\alpha \in \mathbb{F}_\rho$ and evaluate $\xi = f(\alpha)^{(\rho-1)/r} \in \mathbb{F}_\rho$. Recall that $\xi = 1$ if and only if $f(\alpha)$ is an r th power.

- If f is an r th power, then clearly $f(\alpha)$ is an r th power and we always have $\xi = 1$.
- If f is not an r th power, **Theorem 2.1** demonstrates that for at least $1/4$ of the elements of \mathbb{F}_ρ , $f(\alpha)$ is not an r th power. Thus, for α chosen randomly from \mathbb{F}_ρ we would expect $\xi \neq 1$ with probability at least $1/4$.

For a polynomial $f \in \mathbb{F}_q[z]$ over an arbitrary finite field $\mathbb{F}_q[x]$, $q - 1$ is not necessarily divisible by r , so we will work in a suitable extension. First, we can safely assume $r \nmid q$ under the requirement that the characteristic of \mathbb{F}_q is strictly greater than $\deg f$, since in any case we must have $r \leq \deg f$. Then from Fermat’s Little Theorem, we know that $r \mid (q^{r-1} - 1)$ and so we construct an extension field $\mathbb{F}_{q^{r-1}}$ over \mathbb{F}_q and proceed as above. We now present and analyze this more formally.

Algorithm IsPerfectRthPowerGF

Input: A prime power $q, f \in \mathbb{F}_q[x]$ of degree n such that $\text{char}(\mathbb{F}_q) < n \leq 1 + \sqrt{q}/2, r \in \mathbb{N}$ a prime dividing n , and $\epsilon \in \mathbb{R}_{>0}$

Output: **true** if f is the r th power of a polynomial in $\mathbb{F}_q[x]$; **false** otherwise.

- 1: Find an irreducible $\Gamma \in \mathbb{F}_q[z]$ of degree $r - 1$, successful with probability at least $\epsilon/2$
 - 2: $\rho \leftarrow q^{r-1}$
 - 3: Define $\mathbb{F}_\rho = \mathbb{F}_q[z]/(\Gamma)$
 - 4: $m \leftarrow 2.5(1 + \lceil \log_2(1/\epsilon) \rceil)$
 - 5: **for** i from 1 to m **do**
 - 6: Choose random $\alpha \in \mathbb{F}_\rho$
 - 7: $\xi \leftarrow f(\alpha)^{(\rho-1)/r} \in \mathbb{F}_\rho$
 - 8: **if** $\xi \neq 1$ **then**
 - 9: **return false**
 - 10: **return true**
-

Notes on IsPerfectRthPowerGF.

To accomplish Step 1, a number of fast probabilistic methods are available to find irreducible polynomials. We employ the algorithm of Shoup (1994). This algorithm requires $O((r^2 \log r + r \log q) \log r \log \log r)$ operations in \mathbb{F}_q . It is probabilistic of the Las Vegas type, and we assume that it always stops within the number of operations specified, and returns the correct answer with probability at least $1/2$ and “Fail” otherwise (it never returns an incorrect answer). The algorithm is actually presented in Shoup (1994) as *always* finding an irreducible polynomial, but requiring *expected* time as above; by not iterating indefinitely our restatement allows for a Monte Carlo analysis in what follows. To obtain an irreducible Γ with failure probability at most $\epsilon/2$ we run (our modified) Shoup’s algorithm $1 + \lceil \log_2(1/\epsilon) \rceil$ times.

The restriction that $n \leq 1 + \sqrt{q}/2$ (or equivalently that $q \geq 4(n - 1)^2$) is not at all limiting. If this condition is not met, simply extend \mathbb{F}_q with an extension of degree $v = \lceil \log_q(4(n - 1)^2) \rceil$ and perform the algorithm over \mathbb{F}_{q^v} . At worst, each operation in \mathbb{F}_{q^v} requires $O(M(\log n))$ operations in \mathbb{F}_q .

Here we define $M(r)$ as a number of operations in F to multiply two polynomials of degree $\leq r$ over F , for any field F , or the number of bit operations to multiply two integers with at most r bits. Using classical arithmetic $M(r)$ is $O(r^2)$, while using the fast algorithm of Cantor and Kaltofen (1991) we may assume that $M(r)$ is $O(r \log r \log \log r)$.

Theorem 2.2. *Let q, f, n, r, ϵ be as in the input to the algorithm IsPerfectRthPowerGF. If f is a perfect r th power the algorithm always reports this. If f is not a perfect r th power then, on any invocation, this is reported correctly with probability at least $1 - \epsilon$.*

Proof. It is clear from the above discussion that the algorithm always works when f is perfect power. When f is not a perfect power, each iteration of the loop will obtain $\xi \neq 1$ (and hence a correct output) with probability at least $1/4$. By iterating the loop m times we ensure that the probability of failure is at most $\epsilon/2$. Adding this to the probability that Shoup’s algorithm (for Step 1) fails yields a total probability of failure of at most ϵ . \square

Theorem 2.3. *On inputs as specified, the algorithm `IsPerfectRthPowerGF` requires $O((rM(r) \log r \log q) \cdot \log(1/\epsilon))$ operations in \mathbb{F}_q plus the cost to evaluate $\alpha \mapsto f(\alpha)$ at $O(\log(1/\epsilon))$ points $\alpha \in \mathbb{F}_{q^{r-1}}$.*

Proof. As noted above, Shoup’s (1994) algorithm requires $O((r^2 \log r + r \log q) \log r \log \log r)$ field operations per iteration, which is within the time specified. The main cost of the loop in Steps 5–9 is computing $f(\alpha)^{(e-1)/r}$, which requires $O(\log q)$ or $O(r \log q)$ operations in \mathbb{F}_q using repeated squaring, plus one evaluation of f at a point in \mathbb{F}_q . Each operation in \mathbb{F}_q requires $O(M(r))$ operations in \mathbb{F}_q , and we repeat the loop $O(\log(1/\epsilon))$ times. \square

Corollary 2.4. *Given $f \in \mathbb{F}_q[x]$ of degree n with $\tau(f) = t$, and $r \in \mathbb{N}$ a prime dividing n , we can determine if f is an r th power with*

$$O((rM(r) \log r \log q + tM(r) \log n) \cdot \log(1/\epsilon))$$

operations in \mathbb{F}_q , provided $n > \text{char}(\mathbb{F}_q)$. When f is an r th power, the output is always correct, while if f is not an r th power, the output is correct with probability at least $1 - \epsilon$.

2.3. Certifying specified powers over $\mathbb{Z}[x]$

For an integer polynomial $f \in \mathbb{Z}[x]$, we proceed by working in the homomorphic image of \mathbb{Z} in \mathbb{F}_p (and then in an extension of that field). We must ensure that the homomorphism preserves the perfect power property we are interested in with high probability. For any polynomial $g \in \mathbb{F}[x]$, let $\text{disc}(g) = \text{res}(g, g')$ be the discriminant of g (the resultant of g and its first derivative). It is well known that g is squarefree if and only if $\text{disc}(g) \neq 0$. Also define $\text{lcoeff}(g)$ as the leading coefficient of g , the coefficient of the highest power of x in g . Finally, for $g \in \mathbb{Z}[x]$ and p a prime, denote by $g \bmod p$ the unique polynomial in $\mathbb{F}_p[x]$ with all coefficients in g reduced modulo p .

Lemma 2.5. *Let $f \in \mathbb{Z}[x]$ and $\tilde{f} = f / \gcd(f, f')$ its squarefree part. Let p be a prime such that $p \nmid \text{disc}(\tilde{f})$ and $p \nmid \text{lcoeff}(f)$. Then f is a perfect power in $\mathbb{Z}[x]$ if and only if $f \bmod p$ is a perfect power in $\mathbb{F}_p[x]$.*

Proof. Clearly if f is a perfect power, then $f \bmod p$ is a perfect power in $\mathbb{Z}[x]$. To show the converse, assume that $f = f_1^{s_1} \cdots f_m^{s_m}$ for distinct irreducible $f_1, \dots, f_m \in \mathbb{Z}[x]$, so $\tilde{f} = f_1 \cdots f_m$. Clearly $f \equiv f_1^{s_1} \cdots f_m^{s_m} \pmod p$ as well, and because $p \nmid \text{lcoeff}(f)$ we know $\deg(f_i \bmod p) = \deg f_i$ for $1 \leq i \leq m$. Since $p \nmid \text{disc}(\tilde{f})$, $\tilde{f} \bmod p$ is squarefree (see von zur Gathen and Gerhard (2003), Lemma 14.1), and each of the $f_i \bmod p$ must be pairwise relatively prime and squarefree for $1 \leq i \leq m$. Now suppose $f \bmod p$ is a perfect r th power modulo p . Then we must have $r \mid s_i$ for $1 \leq i \leq m$. But this immediately implies that f is a perfect power in $\mathbb{Z}[x]$ as well. \square

Given any polynomial $g = g_0 + g_1x + \cdots + g_mx^m \in \mathbb{Z}[x]$, we define the height or coefficient ∞ -norm of g as $\|g\|_\infty = \max_i |g_i|$. Similarly, we define the coefficient 1-norm of g as $\|g\|_1 = \sum_i |g_i|$, and 2-norm as $\|g\|_2 = (\sum_i |g_i|^2)^{1/2}$. With f, \tilde{f} as in Lemma 2.5, \tilde{f} divides f , so we can employ the factor bound of Mignotte (1974) to obtain

$$\|\tilde{f}\|_\infty \leq 2^n \|f\|_2 \leq 2^n \sqrt{n+1} \cdot \|f\|_\infty.$$

Since $\text{disc}(\tilde{f}) = \text{res}(\tilde{f}, \tilde{f}')$ is the determinant of matrix of size at most $(2n - 1) \times (2n - 1)$, Hadamard’s inequality implies

$$|\text{disc}(\tilde{f})| \leq (2^n (n + 1)^{1/2} \|f\|_\infty)^{n-1} (2^n (n + 1)^{3/2} \|f\|_\infty)^n < 2^{2n^2} (n + 1)^{2n} \cdot \|f\|_\infty^{2n}.$$

Also observe that $|\text{lcoeff}(f)| \leq \|f\|_\infty$. Thus, the product $\text{disc}(\tilde{f}) \cdot \text{lcoeff}(f)$ has at most

$$\mu = \left\lceil \frac{\left\lceil \log_2 \left(2^{2n^2} (n+1)^{2n} \|f\|_\infty^{2n+1} \right) \right\rceil}{\left\lfloor \log_2 \left(4(n-1)^2 \right) \right\rfloor} \right\rceil$$

prime factors greater than $4(n-1)^2$ (we require the lower bound $4(n-1)^2$ to employ [Theorem 2.1](#) without resorting to field extensions). Choose an integer $\gamma \geq 4(n-1)^2$ such that the number of primes between γ and 2γ is at least $4\mu + 1$. By [Rosser and Schoenfeld \(1962\)](#), Corollary 3, the number of primes in this range is at least $3\gamma / (5 \ln \gamma)$ for $\gamma \geq 21$.

Now let $\gamma \geq \max\{21\mu \ln \mu, 226\}$. It is easily confirmed that if $\mu \leq 6$ and $\gamma \geq 226$, then $3\gamma / (5 \ln \gamma) > 4\mu + 1$. Otherwise, if $\mu \geq 7$, then $\ln(21 \ln \mu) < 2 \ln \mu$, so

$$\frac{\gamma}{\ln \gamma} \geq \frac{21\mu \ln \mu}{\ln \mu + \ln(21 \ln \mu)} > 7\mu,$$

and therefore $3\gamma / (5 \ln \gamma) > 21\mu / 5 > 4\mu + 1$.

Thus, if $\gamma \geq \max\{21\mu \ln \mu, 226\}$, then a random prime not equal to r in the range $\gamma \dots 2\gamma$ divides $\text{lcoeff}(f) \cdot \text{disc}(f)$ with probability at most $1/4$. Primes p of this size have only $\log_2 p \in O(\log n + \log \log \|f\|_\infty)$ bits.

Algorithm IsPerfectRthPowerZ

Input: $f \in \mathbb{Z}[x]$ of degree n ; $r \in \mathbb{N}$ a prime dividing n ; $\epsilon \in \mathbb{R}_{>0}$;

Output: **true** if f is the r th power of a polynomial in $\mathbb{Z}[x]$; **false** otherwise

- 1: $\mu \leftarrow \left\lceil \left\lceil \log_2 \left(2^{2n^2} (n+1)^{2n} \|f\|_\infty^{2n+1} \right) \right\rceil / \left\lfloor \log_2 \left(4(n-1)^2 \right) \right\rfloor \right\rceil$
- 2: $\gamma \leftarrow \max\{\lceil 21\mu \ln \mu \rceil, 4(n-1)^2, 226\}$
- 3: **for** i from 1 to $\lceil \log_2(1/\epsilon) \rceil$ **do**
- 4: $p \leftarrow$ random prime in the range $\gamma \dots 2\gamma$
- 5: **if** NOT **IsPerfectRthPowerGF**($p, f \bmod p, r, 1/4$) **then**
- 6: **return false**
- 7: **return true**

Theorem 2.6. Let $f \in \mathbb{Z}[x]$ of degree n , $r \in \mathbb{N}$ dividing n and $\epsilon \in \mathbb{R}_{>0}$. If f is a perfect r th power, the algorithm **IsPerfectRthPowerZ** always reports this. If f is not a perfect r th power, on any invocation of the algorithm, this is reported correctly with probability at least $1 - \epsilon$.

Proof. If f is an r th power then so is $f \bmod p$ for any prime p , and so is any $f(\alpha) \in \mathbb{F}_p$. Thus, the algorithm always reports that f is an r th power. Now suppose f is not an r th power. If $p \mid \text{disc}(f)$ or $p \mid \text{lcoeff}(f)$ it may happen that $f \bmod p$ is an r th power. This happens with probability at most $1/4$ and we will assume that the worst happens in this case. When $p \nmid \text{disc}(f)$ and $p \nmid \text{lcoeff}(f)$, the probability that **IsPerfectRthPowerGF** incorrectly reports that f is an r th power is also at most $1/4$, by our choice of parameter ϵ in the call to **IsPerfectRthPowerGF**. Thus, on any iteration of steps 3–6, the probability of finding that f is an r th power is at most $1/2$. The probability of this happening $\lceil \log_2(1/\epsilon) \rceil$ times is at most ϵ . \square

Theorem 2.7. On inputs as specified, the algorithm **IsPerfectRthPowerZ** requires

$$O\left(rM(r) \log r \cdot M(\log n + \log \log \|f\|_\infty) \cdot (\log n + \log \log \|f\|_\infty) \cdot \log(1/\epsilon)\right),$$

or $O(r^2(\log n + \log \log \|f\|_\infty)^2 \cdot \log(1/\epsilon))$ bit operations, plus the cost to evaluate $(\alpha, p) \mapsto f(\alpha) \bmod p$ at $O(\log(1/\epsilon))$ points $\alpha \in \mathbb{F}_p$ for primes p with $\log p \in O(\log n + \log \log \|f\|_\infty)$.

Proof. The number of operations required by each iteration is dominated by Step 5, for which $O(rM(r) \log r \log p)$ operations in \mathbb{F}_p is sufficient by [Theorem 2.3](#). Since $\log p \in O(\log n + \log \log \|f\|_\infty)$ we obtain the final complexity as stated. \square

We obtain the following corollary for t -sparse polynomials in $\mathbb{Z}[x]$. This follows since the cost of evaluating a t -sparse polynomial $f \in \mathbb{Z}[x]$ modulo a prime p is $O(t \log \|f\|_\infty \log p + t \log nM(\log p))$ bit operations.

Corollary 2.8. *Given $f \in \mathbb{Z}[x]$ of degree n , with $\tau(f) = t$, and $r \in \mathbb{N}$ a prime dividing n , we can determine if f is an r th power with*

$$O^{\sim} \left((r^2 \log^2 n + t \log^2 n + t \log \|f\|_\infty \log n) \cdot \log(1/\epsilon) \right)$$

bit operations. When f is an r th power, the output is always correct, while if f is not an r th power, the output is correct with probability at least $1 - \epsilon$.

2.4. An upper bound on r

In this subsection we show that if $f = h^r$ and $f \neq x^n$ then r must be small. Over $\mathbb{Z}[x]$ we show that $\|h\|_2$ is small as well. A sufficiently strong result over many fields is demonstrated by Schinzel (1987), Theorem 1, where it is shown that if f has sparsity $t \geq 2$ then $t \geq r + 1$ (in fact a stronger result is shown involving the sparsity of h as well). This holds when either the characteristic of the ground field of f is zero or greater than $\deg f$.

Here we give a (much) simpler result for polynomials in $\mathbb{Z}[x]$, which bounds $\|h\|_2$ and is stronger at least in its dependency on t though it also depends upon the coefficients of f .

Theorem 2.9. *Suppose $f \in \mathbb{Z}[x]$ with $\deg f = n$ and $\tau(f) = t$, and $f = h^r$ for some $h \in \mathbb{Z}[x]$ of degree s and $r \geq 2$. Then $\|h\|_2 \leq \|f\|_1^{1/r}$.*

Proof. Let $p > n$ be prime and $\zeta \in \mathbb{C}$ a p th primitive root of unity. Then

$$\|h\|_2^2 = \sum_{0 \leq i \leq s} |h_i|^2 = \frac{1}{p} \sum_{0 \leq i < p} |h(\zeta^i)|^2.$$

(this follows from the fact that the Discrete Fourier Transform (DFT) matrix is orthogonal). In other words, the average value of $|h(\zeta^i)|^2$ for $i = 0 \dots p - 1$ is $\|h\|_2^2$, and so there exists a $k \in \{0, \dots, p - 1\}$ with $|h(\zeta^k)|^2 \geq \|h\|_2^2$. Let $\theta = \zeta^k$. Then clearly $|h(\theta)| \geq \|h\|_2$. We also note that $f(\theta) = h(\theta)^r$ and $|f(\theta)| \leq \|f\|_1$, since $|\theta| = 1$. Thus,

$$\|h\|_2 \leq |h(\theta)| = |f(\theta)|^{1/r} \leq \|f\|_1^{1/r}. \quad \square$$

The following corollary is particularly useful.

Corollary 2.10. *If $f \in \mathbb{Z}[x]$ is not of the form x^n , and $f = h^r$ for some $h \in \mathbb{Z}[x]$, then*

- (i) $r \leq 2 \log_2 \|f\|_1$,
- (ii) $\tau(h) \leq \|f\|_1^{2/r}$.

Proof. Part (i) follows since $\|h\|_2 \geq \sqrt{2}$. Part (ii) follows because $\|h\|_2 \geq \sqrt{\tau(h)}$. \square

These bounds relate to the sparsity of f since $\|f\|_1 \leq \tau(f) \|f\|_\infty$.

2.5. Perfect power detection algorithm

We can now complete the perfect power detection algorithm, when we are given only the t -sparse polynomial f (and not r).

Algorithm IsPerfectPowerZ

Input: $f \in \mathbb{Z}[x]$ of degree n and sparsity $t \geq 2$, $\epsilon \in \mathbb{R}_{>0}$

Output: **true** and r if $f = h^r$ for some $h \in \mathbb{Z}[x]$; **false** otherwise.

- 1: $\mathcal{P} \leftarrow \{\text{primes } r \mid n \text{ and } r \leq 2 \log_2(t \|f\|_\infty)\}$
 - 2: **for** $r \in \mathcal{P}$ **do**
 - 3: **if** IsPerfectRthPowerZ($f, r, \epsilon/\#\mathcal{P}$) **then**
 - 4: **return true** and r
 - 5: **return false**
-

Theorem 2.11. *If $f \in \mathbb{Z}[x] = h^r$ for some $h \in \mathbb{Z}[x]$, the algorithm `IsPerfectPowerZ` always returns “True” and returns r correctly with probability at least $1 - \epsilon$. Otherwise, it returns “False” with probability at least $1 - \epsilon$. The algorithm requires $O^*(t \log^2 \|f\|_\infty \log^2 n \log(1/\epsilon))$ bit operations.*

Proof. From the preceding discussions, we can see that if f is a perfect power, then it must be a perfect r th power for some $r \in \mathcal{P}$. So the algorithm must return true on some iteration of the loop. However, it may incorrectly return true *too early* for an r such that f is not actually an r th power; the probability of this occurring is the probability of error when f is not a perfect power, and is less than $\epsilon/\#\mathcal{P}$ at each iteration. So the probability of error on any iteration is at most ϵ , which is what we wanted.

The complexity result follows from the fact that each $r \in O(\log t + \log \|f\|_\infty)$ and using Corollary 2.8. \square

For polynomials in $\mathbb{F}_q[x]$ we use Schinzel’s bound that $r \leq t - 1$ and obtain the following algorithm.

Algorithm `IsPerfectPowerGF`

Input: A prime power $q, f \in \mathbb{F}_q[x]$ of degree n and sparsity t such that $n < \text{char}(\mathbb{F}_q)$, and $\epsilon \in \mathbb{R}_{>0}$

Output: **true** and r if $f = h^r$ for some $h \in \mathbb{F}_q[x]$; **false** otherwise.

- 1: $\mathcal{P} \leftarrow \{\text{primes } r \mid n \text{ and } r \leq t\}$
 - 2: **for** $p \in \mathcal{P}$ **do**
 - 3: **if** `IsPerfectRthPowerGF`($f, r, \epsilon/\#\mathcal{P}$) **then**
 - 4: **return true** and r
 - 5: **return false**
-

Theorem 2.12. *If $f = h^r$ for $h \in \mathbb{F}_q[x]$, the algorithm `IsPerfectPowerGF` always returns “True” and returns r correctly with probability at least $1 - \epsilon$. Otherwise, it returns “False” with probability at least $1 - \epsilon$. The algorithm requires $O^*(t^3(\log q + \log n))$ operations in \mathbb{F}_q .*

Proof. The proof is equivalent to that of Theorem 2.11, using the complexity bounds in Corollary 2.4. \square

2.6. Detecting multivariate perfect powers

In this subsection we examine the problem of detecting multivariate perfect powers. That is, given a lacunary $f \in \mathbb{F}[x_1, \dots, x_\ell]$ of total degree n as in (1.1), we want to determine if $f = h^r$ for some $h \in \mathbb{F}[x_1, \dots, x_\ell]$ and $r \in \mathbb{N}$. This is done simply as a reduction to the univariate case.

First, given $f \in \mathbb{F}[x_1, \dots, x_\ell]$, define the squarefree part $\tilde{f} \in \mathbb{F}[x_1, \dots, x_\ell]$ as the squarefree polynomial of highest total degree which divides f .

Lemma 2.13. *Let $f \in \mathbb{F}[x_1, \dots, x_\ell]$ be of total degree $n > 0$ and let $\tilde{f} \in \mathbb{F}[x_1, \dots, x_\ell]$ be the squarefree part of f . Define*

$$\Delta = \text{disc}_x(\tilde{f}(y_1x, \dots, y_\ell x)) = \text{res}_x(\tilde{f}(y_1x, \dots, y_\ell x), \tilde{f}'(y_1x, \dots, y_\ell x)) \in \mathbb{F}[y_1, \dots, y_\ell]$$

and

$$\Lambda = \text{lcoeff}_x(f(y_1x, \dots, y_\ell x)) \in \mathbb{F}[y_1, \dots, y_\ell]$$

for independent indeterminates x, y_1, \dots, y_ℓ . Assume that $a_1, \dots, a_\ell \in \mathbb{F}$ with $\Delta(a_1, \dots, a_\ell) \neq 0$ and $\Lambda(a_1, \dots, a_n) \neq 0$. Then $f(x_1, \dots, x_\ell)$ is a perfect power if and only if $f(a_1x, \dots, a_\ell x) \in \mathbb{F}[x]$ is a perfect power.

Proof. Clearly if f is a perfect power, then $f(a_1x, \dots, a_\ell x)$ is a perfect power. To prove the converse, assume that

$$f = f_1^{s_1} f_2^{s_2} \dots f_m^{s_m}$$

for irreducible $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_\ell]$. Then

$$f(y_1x, \dots, y_mx) = f_1(y_1x, \dots, y_mx)^{s_1} \dots f_m(y_1x, \dots, y_mx)^{s_m}$$

and each of the $f_i(y_1x, \dots, y_mx)$ are irreducible. Now, since $\Lambda(a_1, \dots, a_m) \neq 0$, we know the $\deg(f(a_1x, \dots, a_\ell x)) = \deg f$ (the total degree of f). Thus, $\deg f_i(a_1x, \dots, a_\ell x) = \deg f_i$ for $1 \leq i \leq \ell$ as well. Also, by our assumption, $\text{disc}(f(a_1x, \dots, a_\ell x)) \neq 0$, so all of the $f_i(a_1x, \dots, a_\ell x)$ are squarefree and pairwise relatively prime for $1 \leq i \leq k$, and

$$f(a_1x, \dots, a_\ell x) = f_1(a_1x, \dots, a_\ell x)^{s_1} \cdots f_m(a_1x, \dots, a_\ell x)^{s_m}.$$

Assume now that $f(a_1x, \dots, a_\ell x)$ is an r th perfect power. Then r divides s_i for $1 \leq i \leq m$. This immediately implies that f itself is an r th perfect power. \square

It is easy to see that the total degree of Δ is less than $2n^2$ and the total degree of Λ is less than n , and that both Δ and Λ are non-zero. Thus, for randomly chosen a_1, \dots, a_ℓ from a set $\mathcal{S} \subseteq F$ of size at least $8n^2 + 4n$ we have $\Delta(a_1, \dots, a_\ell) = 0$ or $\Lambda(a_1, \dots, a_\ell) = 0$ with probability less than $1/4$, by Zippel (1979) or Schwartz (1980). This can be made arbitrarily small by increasing the set size and/or by repetition. We then run the appropriate univariate algorithm over $F[x]$ (depending upon the field) to identify whether or not f is a perfect power, and if so, to find r . Note that, for integer polynomials, $f(a_1x, \dots, a_\ell x)$ need not be explicitly computed over $\mathbb{Z}[x]$; this can be delayed until a finite field is chosen in the `IsPerfectRthPowerZ` algorithm, in order to preserve polynomial time.

3. Computing perfect roots

Once we have determined that $f \in F[x]$ is equal to h^r for some $h \in F[x]$, the next task is to actually compute h . Unfortunately, as noted in the introduction, there are no known bounds on $\tau(h)$ which are polynomial in $\tau(f)$.

The question of how sparse the polynomial root of a sparse polynomial must be (or equivalently, how dense any power of a dense polynomial must be) relates to some questions first raised by Erdős (1949) on the number of terms in the square of a polynomial. Schinzel extended this work to the case of perfect powers and proved that $\tau(h^r)$ tends to infinity as $\tau(h)$ tends to infinity (Schinzel, 1987). Some conjectures of Schinzel suggest that $\tau(h)$ should be $O(\tau(f))$. A recent breakthrough of Zannier (2007) shows that $\tau(h)$ is bounded by a function which does not depend on $\deg f$, but this bound is unfortunately not polynomial in $\tau(f)$.

However, our own (limited) investigations, along with more extensive ones by Coppersmith and Davenport (1991), and later Abbott (2002), suggest that, for any $h \in F[x]$, where the characteristic of F is not too small, $\tau(h) \in O(\tau(h^r) + r)$. We skirt this problem in two ways: our first algorithm is output-sensitive, and the second relies on a modest conjecture.

3.1. Computing r th roots in polynomial-time (without conditions)

In this subsection we present an algorithm for computing an h such that $f = h^r$ given $f \in \mathbb{Z}[x]$ and $r \in \mathbb{Z}$ or showing that no such h exists. The algorithm is deterministic and requires time polynomial in $t = \tau(f)$, $\log \deg f$, $\log \|f\|_\infty$ and a given upper bound μ on $m = \tau(h)$. Neither its correctness nor complexity is conditional on any conjecture. We will only demonstrate that this algorithm requires polynomial time. A more detailed analysis is performed on the (more efficient) algorithm of the next subsection (though that complexity is subject to a modest conjecture).

The basic idea of the algorithm here is that we can recover all the coefficients in \mathbb{Q} as well as modular information about the exponents of h from a homomorphism into a small cyclotomic field over \mathbb{Q} . Doing this for a relatively small number of cyclotomic fields yields h .

Assume that (the unknown) $h \in \mathbb{Z}[x]$ has the form

$$h = \sum_{1 \leq i \leq m} b_i x^{d_i} \quad \text{for } b_1, \dots, b_m \in \mathbb{Z} \setminus \{0\}, \text{ and } 0 \leq d_1 < d_2 < \dots < d_m,$$

and that $p > 2$ is a prime distinct from r such that

$$p \nmid \prod_{1 \leq i < j \leq m} (d_j - d_i), \quad \text{and} \quad p \nmid \prod_{1 \leq i \leq m} (d_i + 1). \tag{3.1}$$

Let $\zeta_p \in \mathbb{C}$ be a p th primitive root of unity, and $\Phi_p = 1 + z + \dots + z^{p-1} \in \mathbb{Z}[z]$ its minimal polynomial, the p th cyclotomic polynomial (which is irreducible in $\mathbb{Q}[z]$). Computationally we represent $\mathbb{Q}(\zeta_p)$ as

$\mathbb{Q}[z]/(\Phi_p)$, with $\zeta_p \equiv z \pmod{\Phi_p}$. Observe that $\zeta_p^k = \zeta_p^{k \text{ rem } p}$ for any $k \in \mathbb{Z}$, where $k \text{ rem } p$ is the least non-negative residue of k modulo p . Thus

$$h(\zeta_p) = h_p(\zeta_p) \quad \text{for } h_p = \sum_{1 \leq i \leq m} b_i x^{d_i \text{ rem } p} \in \mathbb{Z}[x],$$

and h_p is the unique representation of $h(\zeta_p)$ as a polynomial of degree less than $p - 1$. This follows from the conditions (3.1) on our choice of prime p because

- No pair of distinct exponents d_i and d_j of h is equivalent modulo p (since $p \nmid (d_i - d_j)$);
- All the exponents reduced modulo p are strictly less than $p - 1$ (since our conditions imply $d_i \not\equiv (p - 1) \pmod{p}$ for $1 \leq i \leq m$).

This also implies that the coefficients of h_p are exactly the same as those of h , albeit in a different order. Now observe that we can determine h_p quite easily from the roots of

$$\Gamma_p(y) = y^r - f(\zeta_p) \in \mathbb{Q}(\zeta_p)[y].$$

These roots can be found by factoring the polynomial $\Gamma_p(y)$ in $\mathbb{Q}(\zeta_p)[y]$, and the roots in \mathbb{C} must be $\omega^i h(\zeta_p) \in \mathbb{C}$ for $0 \leq i < r$, where ω is a primitive r th root of unity. When $r > 2$, and since we chose p distinct from r , the only r th root of unity in $\mathbb{Q}(\zeta_p)$ is 1. Thus $\Gamma_p(y)$ has exactly one linear factor, and this must be equal to $y - h(\zeta_p) = y - h_p(\zeta_p)$, precisely determining h_p . When $r = 2$, we have

$$\Gamma_p(y) = (y - h(\zeta_p))(y + h(\zeta_p)) = (y - h_p(\zeta_p))(y + h_p(\zeta_p))$$

and we can only determine $h_p(\zeta_p)$ (and h_p and, for that matter, h) up to a factor of ± 1 . However, the exponents of h_p and $-h_p$ are the same, and the ambiguity is only in the coefficients (which we resolve later).

Finally, we need to perform the above operations for a sequence of cyclotomic fields $\mathbb{Q}(\zeta_{p_1}), \mathbb{Q}(\zeta_{p_2}), \dots, \mathbb{Q}(\zeta_{p_k})$ such that the primes in $\mathcal{P} = \{p_1, \dots, p_k\}$ allow us to recover all the exponents in h . Each prime $p \in \mathcal{P}$ gives the set of exponents of h reduced modulo that prime, as well as all the coefficients of h in \mathbb{Z} . That is, from each of the computations with $p \in \mathcal{P}$ we obtain

$$\mathcal{C} = \{b_1, \dots, b_m\} \quad \text{and} \quad \mathcal{E}_p = \{d_1 \text{ rem } p, d_2 \text{ rem } p, \dots, d \text{ rem } p\},$$

but with no clear information about the order of these sets. In particular, it is not obvious how to correlate the exponents modulo the different primes directly. To do this we employ the clever sparse interpolation technique of Garg and Schost (2008) (based on a method of Grigoriev and Karpinski (1987) for a different problem), which interpolates the symmetric polynomial in the exponents:

$$g = (x - d_1)(x - d_2) \cdots (x - d_m) \in \mathbb{Z}[x].$$

For each $p \in \mathcal{P}$ we compute the symmetric polynomial modulo p ,

$$g_p = (x - (d_1 \text{ rem } p))(x - (d_2 \text{ rem } p)) \cdots (x - (d_m \text{ rem } p)) \equiv g \pmod{p},$$

for which we do not need to know the order of the exponent residues. We then determine $g \in \mathbb{Z}[x]$ by the Chinese remainder theorem and factor g over $\mathbb{Z}[x]$ to find the $d_1, \dots, d_m \in \mathbb{Z}$. Thus the product of all primes in $p \in \mathcal{P}$ must be at least $2\|g\|_\infty$ to recover the coefficients of g uniquely. It is easily seen that $2\|g\|_\infty \leq 2n^m$.

As noted above, the computation with each $p \in \mathcal{P}$ recovers all the exponents of h in \mathbb{Z} , so using only one prime $p \in \mathcal{P}$, we determine the j th exponent of h as the coefficient of $x^{d_j \text{ rem } p}$ in h_p for $1 \leq j \leq m$. If $r = 2$ we can choose either of the roots of $\Gamma_p(y)$ (they differ by only a sign) to recover the coefficients of h .

Finally, once we have a candidate root h , we certify that $f = h^r$ by taking logarithmic derivatives to obtain

$$\frac{f'}{f} = \frac{rh'h^{r-1}}{h^r},$$

which simplifies to $f'h = rh'f$. This equation only involves two sparse multiplications and is therefore confirmed in polynomial time, and along with checking leading coefficients implies that in fact $f = h^r$.

The above discussion is summarized in the following algorithm.

Algorithm ComputeRootAlgebraic

Input: $f \in \mathbb{Z}[x]$ as in (1.2) with $\deg f = n$, and $r, \mu \in \mathbb{N}$

Output: $h \in \mathbb{Z}[x]$ such that $f = h^r$ and $\tau(h) \leq \mu$, provided such an h exists

- 1: $\gamma \leftarrow$ smallest integer ≥ 21 such that $3\gamma / (5 \ln \gamma) \geq (\mu^2 + 2\mu) \log_2 n$
 - 2: $\mathcal{P} \leftarrow \{p \in \{\gamma, \dots, 2\gamma\} \text{ and } p \text{ prime}\}$
 - 3: **for** $p \in \mathcal{P}$ **do**
 - 4: Represent $\mathbb{Q}(\zeta_p)$ by $\mathbb{Q}[x]/(\Phi_p)$, where $\Phi_p \leftarrow 1 + z + \dots + z^{p-1}$ and $\zeta_p \equiv z \pmod{\Phi_p}$
 - 5: Compute $f(\zeta_p) = \sum_{1 \leq i \leq t} c_i \zeta_p^{e_i \text{ rem } p} \in \mathbb{Z}[\zeta_p]$
 - 6: Factor $\Gamma_p(y) \leftarrow y^r - f(\zeta_p) \in \mathbb{Q}(\zeta_p)[y]$ over $\mathbb{Q}(\zeta_p)[y]$
 - 7: **if** $\Gamma_p(y)$ has no roots in $\mathbb{Z}[\zeta_p]$ **then**
 - 8: **return** “ f is not an r th power of a μ -sparse polynomial”
 - 9: Let $h_p(\zeta_p) \in \mathbb{Z}[\zeta_p]$ be a root of $\Gamma_p(y)$
Write $h_p(x) = \sum_{1 \leq i \leq m_p} b_{ip} x^{d_{ip}}$, for $b_{ip} \in \mathbb{Z}$ and distinct $d_{ip} \in \mathbb{N}$ for $1 \leq i \leq m_p$
 - 10: **if** $\deg h_p = p - 1$ **then**
 - 11: $m_p \leftarrow 0$; Continue with next prime $p \in \mathcal{P}$ at Step 3
 - 12: $g_p \leftarrow (x - d_{1p})(x - d_{2p}) \dots (x - d_{m_p p}) \in \mathbb{Z}_p[x]$
 - 13: $m \leftarrow \max\{m_p : p \in \mathcal{P}\}$
 - 14: $\mathcal{P}_0 \leftarrow \{p \in \mathcal{P} : m_p = m\}$
 - 15: Reconstruct $g \in \mathbb{Z}[x]$ from $\{g_p\}_{p \in \mathcal{P}_0}$ by the Chinese Remainder Algorithm
 - 16: $\{d_1, d_2, \dots, d_k\} \leftarrow$ distinct integer roots of g
 - 17: **if** $k < m$ **then**
 - 18: **return** “ f is not an r th power of a μ -sparse polynomial”
 - 19: Choose any $p \in \mathcal{P}_0$. For $1 \leq j \leq m$, let $b_j \in \mathbb{Z}$ be the coefficient of $x^{d_j \text{ rem } p}$ in h_p
 - 20: $h \leftarrow \sum_{1 \leq j \leq m} b_j x^{d_j}$
 - 21: **if** $f^r h = r h^r f$ **and** $\text{lc}(f) = \text{lc}(h)^r$ **then**
 - 22: **return** h
 - 23: **else**
 - 24: **return** “ f is not an r th power of a μ -sparse polynomial”
-

Theorem 3.1. *The algorithm ComputeRootAlgebraic works as stated. It requires a number of bit operations polynomial in $t = \tau(f)$, $\log \deg f$, $\log \|f\|$, and μ .*

Proof. We assume throughout the proof that there does exist an $h \in \mathbb{Z}[x]$ such that $f = h^r$ and $\tau(h) \leq \mu$. If it does not, this will be caught in the test in Steps 21–24 by the above discussion, if not before.

In Steps 1–2 we construct a set of primes \mathcal{P} which is guaranteed to contain sufficiently many good primes to recover g , where primes are good in the sense that for all $p \in \mathcal{P}$

$$\beta = r \cdot \prod_{1 \leq i < j \leq m} (d_j - d_i) \cdot \prod_{1 \leq i \leq m} (d_i + 1) \not\equiv 0 \pmod{p}.$$

It is easily derived that $\beta < n^{\mu^2}$, which has fewer than $\log_2 \beta \leq \mu^2 \log_2 n$ prime factors, so there are at most $\mu^2 \log_2 n$ bad primes. We also need to recover g in Step 15, and $\|g\|_\infty \leq n^\mu$, for which we need at least $1 + \log_2 \|g\| \leq 2\mu \log_2 n$ good primes. Thus if \mathcal{P} has at least $(\mu^2 + 2\mu) \log_2 n$ primes, there are a sufficient number of good primes to reconstruct g in Step 15.

By Rosser and Schoenfeld (1962), Corollary 3, for $\gamma \geq 21$ we have that the number of primes in $\{\gamma, \dots, 2\gamma\}$ is at least $3\gamma / (5 \ln \gamma)$, which is at least $(\mu^2 + 2\mu) \log_2 n$ by our choice of γ in Step 1, and $\gamma \in O(\mu^2 \log(n))$. Numbers of this size can easily be tested for primality.

Since we assume that a root h exists, $\Gamma_p(y)$ will always have exactly one root $h_p \in \mathbb{Z}[\zeta_p]$ when $r > 2$, and exactly two roots in $\mathbb{Z}[\zeta_p]$ when $r = 2$ (differing only by sign).

Two conditions cause the primes to be identified as bad. If the map $h \mapsto h(\zeta_p)$ causes some exponents of h to collide modulo p , this can only reduce the number of non-zero exponents m_p in

h_p , and so such primes will not show up in the list of good primes \mathcal{P}_0 , as selected in Step 14. Also, if any of the exponents of h are equivalent to $p - 1$ modulo p we will not be able to reconstruct the exponents of h from h_p , and we identify these as bad in Step 11 (by artificially marking $m_p = 0$, which ensures they will not be added to \mathcal{P}_0).

Correctness of the remainder of the algorithm follows from the previous discussion.

The complexity is clearly polynomial for all steps except for factoring in $\mathbb{Q}(\zeta_p)[y]$ (Step 6), which can be performed in polynomial time with the algorithm of, for example, Landau (1985). \square

As stated, the algorithm `ComputeRootAlgebraic` is not actually output-sensitive, as it requires an a priori bound μ on $\tau(h)$. To avoid this, we could start with any small value for μ , say $\tau(f)$, and after each failure double this bound. Provided that the input polynomial f is in fact an r th perfect power, this process will terminate after a number of steps polynomial in the lacunary size of the output polynomial h . There are also a number of other small improvements that could be made to increase the algorithm's efficiency, which we have omitted here for clarity.

3.2. Faster root computation subject to conjecture

Algorithm `ComputeRootAlgebraic` is output sensitive as the cost depends on the sparsity of the root h . As discussed above, there is considerable evidence that, roughly speaking, the root of a sparse polynomial must always be sparse, and so the preceding algorithm may be unconditionally polynomial-time.

In fact, with suitable sparsity bounds we can derive a more efficient algorithm based on Newton iteration. This approach is simpler as it does not rely on advanced techniques such as factoring over algebraic extension fields. It is also more general as it applies to fields other than \mathbb{Z} and to powers r which are not prime.

Unfortunately, this algorithm is not purely output-sensitive, as it relies on a conjecture regarding the sparsity of powers of h . We first present the algorithm and prove its correctness. Then we give our modest conjecture and use it to prove the algorithm's efficiency.

Our algorithm is essentially a Newton iteration, with special care taken to preserve sparsity. We start with the image of h modulo x , using the fact that $f(0) = h(0)^r$, and at Step $i = 1, 2, \dots, \lceil \log_2(\deg h + 1) \rceil$, we compute the image of h modulo x^i .

Here, and for the remainder of this section, we will assume that $f, h \in \mathbb{F}[x]$ with degrees n and s respectively such that $f = h^r$ for $r \in \mathbb{N}$ at least 2, and that the characteristic of \mathbb{F} is either zero or greater than n . As usual, we define $t = \tau(f)$.

Algorithm `ComputeRootNewton`

Input: $f \in \mathbb{F}[x]$, $r \in \mathbb{N}$ such that f is a perfect r th power

Output: $h \in \mathbb{F}[x]$ such that $f = h^r$

- 1: $u \leftarrow$ highest power of x dividing f
 - 2: $f_u \leftarrow$ coefficient of x^u in f
 - 3: $g \leftarrow f / (f_u x^u)$
 - 4: $h \leftarrow 1, \quad k \leftarrow 1$
 - 5: **while** $kr \leq \deg g$ **do**
 - 6: $\ell \leftarrow \min\{k, (\deg g) / r + 1 - k\}$
 - 7: $a \leftarrow \frac{(hg - h^{r+1}) \text{ rem } x^{k+\ell}}{rx^k}$
 - 8: $h \leftarrow h + (a/g \text{ mod } x^\ell) \cdot x^k$
 - 9: $k \leftarrow k + \ell$
 - 10: $b \leftarrow$ any r th root of f_u in \mathbb{F}
 - 11: **return** $bhx^{u/r}$
-

Theorem 3.2. *If $f \in \mathbb{F}[x]$ is a perfect r th power, then `ComputeRootNewton` returns an $h \in \mathbb{F}[x]$ such that $h^r = f$.*

Proof. Let u, f_u, g be as defined in Steps 1–3. Thus $f = f_u g x^u$. Now let \hat{h} be some r th root of f , which we assume exists. If we similarly write $\hat{h} = \hat{h}_v \hat{g} x^v$, with $\hat{h}_v \in F$ and $\hat{g} \in F[x]$ such that $\hat{g}(0) = 1$, then $\hat{h}^r = \hat{h}_v^r \hat{g}^r x^{vr}$. Therefore f_u must be a perfect r th power in F , $r|u$, and g is a perfect r th power in $F[x]$ of some polynomial with constant coefficient equal to 1.

Denote by h_i the value of h at the beginning of the i th iteration of the while loop. So $h_1 = 1$. We claim that at each iteration through Step 6, $h_i^r \equiv g \pmod{x^k}$. From the discussion above, this holds for $i = 1$. Assuming the claim holds for all $i = 1, 2, \dots, j$, we prove it also holds for $i = j + 1$.

From Step 8, $h_{j+1} = h_j + (a/g \pmod{x^l})x^k$, where a is as defined on the j th iteration of Step 7. We observe that

$$h_j h_j^r \equiv h_j^{r+1} + r h_j^r (a/g \pmod{x^l}) x^k \pmod{x^{k+\ell}}.$$

From our assumption, $h_j^r \equiv f \pmod{x^k}$, and $l \leq k$, so we have

$$h_j h_j^{r+1} \equiv h_j^{r+1} + r a x^k \equiv h_j^{r+1} + h_j f - h_j^{r+1} \equiv h_j f \pmod{x^{k+\ell}}.$$

Therefore $h_{j+1}^r \equiv f \pmod{x^{k+\ell}}$, and so by induction the claim holds at each step. Since the algorithm terminates when $kr > \deg g$, we can see that the final value of h is an r th root of g . Finally, $(bhx^{u/r})^r = f_u g x^u = f$, so the theorem holds. \square

Algorithm `ComputeRootNewton` will only be efficient if the low-order terms of the polynomial power h^{r-1} can be efficiently computed on Step 7. Since we know that h and the low-order terms of h^{r-1} are sparse, we need only a guarantee that the *intermediate powers* will be sparse as well. This is stated in the following modest conjecture.

Conjecture 3.3. For $r, s \in \mathbb{N}$, if the characteristic of F is zero or greater than rs , and $h \in F[x]$ with $\deg h = s$, then

$$\tau(h^i \pmod{x^{2s}}) < \tau(h^r \pmod{x^{2s}}) + r, \quad i = 1, 2, \dots, r - 1.$$

This corresponds to intuition and experience, as the system is still overly constrained with only s degrees of freedom. Computationally, the conjecture has also been confirmed for all of the numerous examples we have tested, although a more thorough investigation of its truth would be interesting. A weaker inequality would suffice to prove polynomial time, but we use the stated bounds as we believe these give more accurate complexity measures.

The application of [Conjecture 3.3](#) to `ComputeRootNewton` is given by the following simple lemma, which essentially tells us that the “error” introduced by examining higher-order terms of h_1^r is not too dense.

Lemma 3.4.³ Let $k, \ell \in \mathbb{N}$ such that $\ell \leq k$ and $k + \ell \leq s$, and suppose $h_1 \in F[x]$ is the unique polynomial with degree less than k satisfying $h_1^r \equiv f \pmod{x^k}$. Then

$$\tau(h_1^{r+1} \pmod{x^{k+\ell}}) \leq 2t(t + r).$$

Proof. Let $h_2 \in F[x]$ be the unique polynomial of degree less than ℓ satisfying $h_1 + h_2 x^k \equiv h \pmod{x^{k+\ell}}$. Since $h^r = f$,

$$f \equiv h_1^r + r h_1^{r-1} h_2 x^k \pmod{x^{k+\ell}}.$$

Multiplying by h_1 and rearranging gives

$$h_1^{r+1} \equiv h_1 f - r h_1 h_2 x^k \pmod{x^{k+\ell}}.$$

Because $h_1 \pmod{x^k}$ and $h_2 \pmod{x^\ell}$ each have at most $\tau(h)$ terms, which by [Conjecture 3.3](#) is less than $t - r$, the total number of terms in $h_1^{r+1} \pmod{x^{k+\ell}}$ is less than $2t(t - r)$. \square

We are now ready to prove the efficiency of the algorithm, assuming the conjecture.

³ Subject to the validity of [Conjecture 3.3](#).

Theorem 3.5.³ If $f \in \mathbb{F}[x]$ has degree n and t nonzero terms, then `ComputeRootNewton` uses $O((t+r)^4 \log r \log n)$ operations in \mathbb{F} and an additional $O((t+r)^4 \log r \log^2 n)$ bit operations, not counting the cost of root-finding in the base field \mathbb{F} on Step 10.

Proof. First consider the cost of computing h^{r+1} in Step 7. This will be accomplished by repeatedly squaring and multiplying by h , for a total of at most $2 \lfloor \log_2(r+1) \rfloor$ multiplications. As well, each intermediate product will have at most $\tau(f)+r < (t+r)^2$ terms, by [Conjecture 3.3](#). The number of field operations required, at each iteration, is $O((t+r)^4 \log r)$, for a total cost of $O((t+r)^4 \log r \log n)$.

Furthermore, since $k + \ell \leq 2^i$ at the i th step, for $1 \leq i < \log_2 n$, the total cost in bit operations is less than

$$\sum_{1 \leq i < \log_2 n} (t+r)^4 \log_2 ri \in O((t+r)^4 \log r \log^2 n).$$

In fact, this is the most costly step. The initialization in Steps 1–3 uses only $O(t)$ operations in \mathbb{F} and on integers at most n . And the cost of computing the quotient on Step 8 is proportional to the cost of multiplying the quotient and dividend, which is at most $O(t(t+r))$. \square

When $\mathbb{F} = \mathbb{Q}$, we must account for coefficient growth. We use the normal notion of the size of a rational number: for $\alpha \in \mathbb{Q}$, write $\alpha = a/b$ for a, b relatively prime integers. Then define $\mathcal{H}(\alpha) = \max\{|a|, |b|\}$. And for $f \in \mathbb{Q}[x]$ with coefficients $c_1, \dots, c_t \in \mathbb{Q}$, write $\mathcal{H}(f) = \max \mathcal{H}(c_i)$.

Thus, the size of the lacunary representation of $f \in \mathbb{Q}[x]$ is proportional to $\tau(f)$, $\deg f$, and $\log \mathcal{H}(f)$. Now we prove the bit complexity of our algorithm is polynomial in these values, when $\mathbb{F} = \mathbb{Q}$.

Theorem 3.6.³ Suppose $f \in \mathbb{Q}[x]$ has degree n and t nonzero terms, and is a perfect r th power. `ComputeRootNewton` computes an r th root of f using $O^{\sim}(t(t+r)^4 \cdot \log n \cdot \log \mathcal{H}(f))$ bit operations.

Proof. Let $h \in \mathbb{Q}[x]$ such that $h^r = f$, and let $c \in \mathbb{Z}_{>0}$ be minimal such that $ch \in \mathbb{Z}[x]$. Gauß’s Lemma tells us that c^r must be the least positive integer such that $c^r f \in \mathbb{Z}[x]$ as well. Then, using [Theorem 2.9](#), we have

$$\mathcal{H}(h) \leq \|ch\|_{\infty} \leq \|ch\|_2 \leq (t\|c^r f\|_{\infty})^{1/r} \leq t^{1/r} \mathcal{H}(f)^{(t+1)/r}.$$

(The last inequality comes from the fact that the lcm of the denominators of f is at most $\mathcal{H}(f)^t$.)

Hence $\log \mathcal{H}(h) \in O((t \log \mathcal{H}(f))/r)$. Clearly the most costly step in the algorithm will still be the computation of h_i^{r+1} at each iteration through Step 7. For simplicity in our analysis, we can just treat h_i (the value of h at the i th iteration of the while loop in our algorithm) as equal to h (the actual root of f), since we know $\tau(h_i) \leq \tau(h)$ and $\mathcal{H}(h_i) \leq \mathcal{H}(h)$.

[Lemma 3.4](#) and [Conjecture 3.3](#) tell us that $\tau(h^i) \leq 2(t+r)^2$ for $i = 1, 2, \dots, r$. To compute h^{r+1} , we will actually compute $(ch)^{r+1} \in \mathbb{Z}[x]$ by repeatedly squaring and multiplying by ch , and then divide out c^{r+1} . This requires at most $\lfloor \log_2 r + 1 \rfloor$ squares and products.

Note that $\|(ch)^{2i}\|_{\infty} \leq (t+r)^2 \|(ch)^i\|_{\infty}^2$ and $\|(ch)^{i+1}\|_{\infty} \leq (t+r)^2 \|(ch)^i\|_{\infty} \|ch\|_{\infty}$. Therefore

$$\|(ch)^i\|_{\infty} \leq (t+r)^{2r} \|ch\|_{\infty}^r, \quad i = 1, 2, \dots, r,$$

and thus $\log \|(ch)^i\|_{\infty} \in O(r(t+r) + t \log \mathcal{H}(f))$, for each intermediate power $(ch)^i$.

Thus each of the $O((t+r)^4 \log r)$ field operations at each iteration costs $O(M(t \log \mathcal{H}(f) + \log r(t+r)))$ bit operations, which then gives the stated result. \square

The method used for Step 10 depends on the field \mathbb{F} . For $\mathbb{F} = \mathbb{Q}$, we just need to find two integer perfect roots, which can be done in “nearly linear” time by the algorithm of [Bernstein \(1998\)](#). Otherwise, we can use any of the well-known fast root-finding methods over $\mathbb{F}[x]$ to compute a root of $x^r - f_u$.

3.3. Computing multivariate roots

For the problem of computing perfect polynomial roots of multivariate polynomials, we again reduce the problem to a univariate one, this time employing the well-known Kronecker substitution method.

Suppose $f, h \in \mathbb{F}[x_1, \dots, x_\ell]$ and $r \in \mathbb{N}$ such that $f = h^r$. It is easily seen that each partial degree of f is exactly r times the corresponding partial degree in h , that is, $\deg_{x_i} f = r \deg_{x_i} h$, for all $i \in \{1, \dots, \ell\}$.

Now suppose f and r are given and we wish to compute h . First use the relations above to compute $d_i = \deg_{x_i} f / r + 1$ for each $i \in \{1, \dots, \ell\}$. (If any $\deg_{x_i} f$ is not a multiple of r , then f must not be an r th power.)

Now use the Kronecker substitution and define

$$\hat{f} = f(y, y^{d_1}, y^{d_1 d_2}, \dots, y^{d_1 \cdots d_{\ell-1}}) \quad \text{and} \quad \hat{h} = h(y, y^{d_1}, y^{d_1 d_2}, \dots, y^{d_1 \cdots d_{\ell-1}}),$$

where y is a new variable. Clearly $\hat{f} = \hat{h}^r$, and since each $d_i > \deg_{x_i} h$, h is easily recovered from the lacunary representation of \hat{h} in the standard way: for each non-zero term cy^e in \hat{h} , compute the digits of e in the mixed radix representation corresponding to the sequence $d_1, d_2, \dots, d_{\ell-1}$. That is, decompose e (uniquely) as $e = e_1 + e_2 d_1 + e_3 d_1 d_2 + \dots + e_\ell d_1 \cdots d_{\ell-1}$ with each $e_i \in \mathbb{N}$ such that $e_i < d_i$. Then the corresponding term in h is $c x_1^{e_1} \cdots x_\ell^{e_\ell}$.

Therefore we simply use either algorithm above to compute \hat{h} as the r th root of \hat{f} over $\mathbb{F}[y]$, then invert the Kronecker map to obtain $h \in \mathbb{F}[x_1, \dots, x_\ell]$. The conversion steps are clearly polynomial-time, and notice that $\log \deg \hat{f}$ is at most ℓ times larger than $\log \deg f$. Therefore the lacunary sizes of \hat{f} and \hat{h} are polynomial in the lacunary sizes of f and h , and the algorithms in this section yield polynomial-time algorithms to compute perfect r th roots of multivariate lacunary polynomials.

4. Implementation

To investigate the practicality of our algorithms, we implemented `IsPerfectPowerZ` using Victor Shoup’s NTL. This is a high-performance C++ for fast dense univariate polynomial computations over $\mathbb{Z}[x]$ or $\mathbb{F}_q[x]$.

NTL does not natively support a lacunary polynomial representation, so we wrote our own using vectors of coefficients and of exponents. In fact, since `IsPerfectPowerZ` is a black-box algorithm, the only sparse polynomial arithmetic we needed to implement was for evaluation at a given point.

The only significant diversion between our implementation and the algorithm specified in Section 2 is our choice of the ground field. Rather than working in a degree- $(r - 1)$ extension of \mathbb{F}_p , we simply find a random p in the same range such that $(r - 1) \mid p$. It is more difficult to prove that we can find such a p quickly (using e.g. the best known bounds on Linnik’s Constant), but in practice this approach is very fast because it avoids computing in field extensions.

As a point of comparison, we also implemented the Newton iteration approach to computing perfect polynomial roots, which appears to be the fastest known method for dense polynomials. This is not too dissimilar from the techniques from the previous section on computing a lacunary r th root, but without paying special attention to sparsity. We work modulo a randomly chosen prime p to compute an r th perfect root h , and then use random evaluations of h and the original input polynomial f to certify correctness. This yields a Monte Carlo algorithm with the same success probability as ours, and so provides a suitable and fair comparison.

We ran two sets of tests comparing these algorithms. The first set, depicted in Fig. 1, does not take advantage of sparsity at all; that is, the polynomials are dense and have close to the maximal number of terms. It appears that the worst-case running time of our algorithm is actually a bit better than the Newton iteration method on dense input, but on the average they perform roughly the same. The lower triangular shape comes from the fact that both algorithms can (and often do) terminate early. The visual gap in the timings for the sparse algorithm comes from the fact that exactly half of the input polynomials were perfect powers. It appears our algorithm terminates more quickly when the polynomial is not a perfect power, but usually takes close to the full amount of time otherwise.

The second set of tests, depicted in Fig. 2, held the number of terms of the perfect power, $\tau(f)$, roughly fixed, letting the degree n grow linearly. Here we can see that, for sufficiently sparse f , our algorithm performs significantly and consistently better than the Newton iteration. In fact, we can see that, with some notable but rare exceptions, it appears that the running time of our algorithm is largely independent of the degree when the number of terms remains fixed. The outliers we see

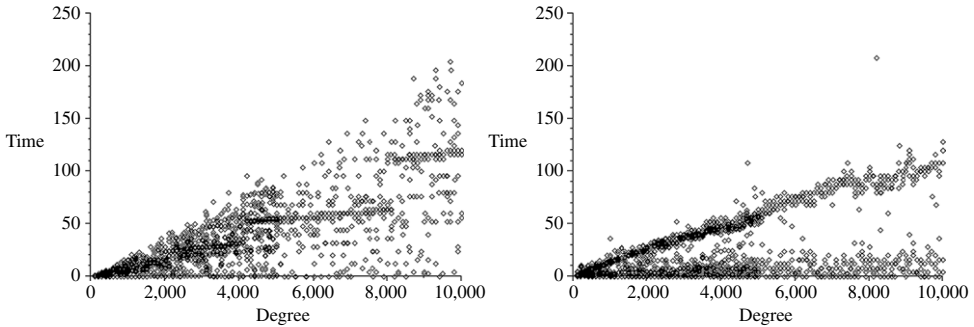


Fig. 1. Comparison of Newton iteration (left) vs. our `IsPerfectPowerZ` (right). Inputs are dense.

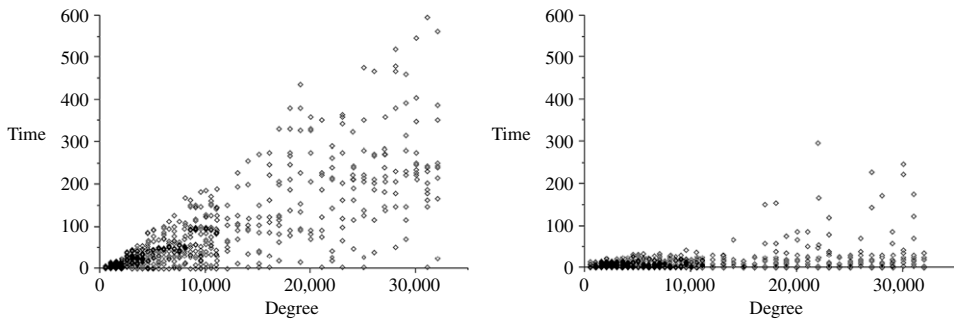


Fig. 2. Comparison of Newton iteration (left) vs. our `IsPerfectPowerZ` (right). Inputs are sparse, with sparsity fixed around 500.

probably come from inputs that were unluckily dense (it is not trivial to produce examples of h^f with a given fixed number of nonzero terms, so the sparsity did vary to some extent).

Perhaps most surprisingly, although the choices of parameters for these two algorithms only guaranteed a probability of success of at least $1/2$, in fact over literally millions of tests performed with both algorithms and a wide range of input polynomials, not a single failure was recorded. This is of course due to the loose bounds employed in our analysis, indicating a lack of understanding at some level, but it also hints at the possibility of a deterministic algorithm, or at least one which is probabilistic of the Las Vegas type.

Both implementations are available as C++ code downloadable from the second author's website.

Acknowledgements

The authors would like to thank Éric Schost and Pascal Koiran for pointing out that the logarithmic derivative could be used for a certificate of correctness in Algorithm `ComputeRootAlgebraic`. The authors would also like to thank Erich Kaltofen and Igor Shparlinski for their helpful comments.

References

- Abbott, J., 2002. Sparse squares of polynomials. *Math. Comp.* 71 (237), 407–413 (electronic).
- Bach, E., Sorenson, J., 1993. Sieve algorithms for perfect power testing. *Algorithmica* 9 (4), 313–328.
- Ben-Or, M., Tiwari, P., 1988. A deterministic algorithm for sparse multivariate polynomial interpolation. In: Proc. STOC 1988. ACM Press, New York, NY, pp. 301–309.
- Bernstein, D.J., 1998. Detecting perfect powers in essentially linear time. *Math. Comp.* 67 (223), 1253–1283.
- Cantor, D., Kaltofen, E., 1991. Fast multiplication of polynomials over arbitrary algebras. *Acta Inform.* 28, 693–701.
- Coppersmith, D., Davenport, J., 1991. Polynomials whose powers are sparse. *Acta Arith.* 58 (1), 79–87.
- Cucker, F., Koiran, P., Smale, S., 1999. A polynomial time algorithm for Diophantine equations in one variable. *J. Symbolic Comput.* 27 (1), 21–29.

- Erdős, P., 1949. On the number of terms of the square of a polynomial. *Nieuw Arch. Wiskunde* (2) 23, 63–65.
- Garg, S., Schost, E., Interpolation of polynomials given by straight-line programs. Preprint, 2008.
- von zur Gathen, J., Gerhard, J., 2003. *Modern Computer Algebra*. Cambridge University Press, Cambridge, New York, Melbourne.
- von zur Gathen, J., Karpinski, M., Shparlinski, I., Counting curves and their projections. In: *ACM Symposium on Theory of Computing*, 1993, pp. 805–812.
- Giesbrecht, M., Roche, D.S., 2008. On lacunary polynomial perfect powers. In: *ISSAC'08: Proc. International Symposium on Symbolic and Algebraic Computation*. ACM, pp. 103–110.
- Grigoriev, D., Karpinski, M., The matching problem for bipartite graphs with polynomially bounded permanents is in NC. In: *Foundations of Computer Science, FOCS*, 1987, pp. 166–172.
- Kaltofen, E., 1987. Single-factor hensel lifting and its application to the straight-line complexity of certain polynomials. In: *STOC '87: Proceedings of the Nineteenth Annual ACM Conference on Theory of Computing*. ACM, New York, NY, USA, pp. 443–452.
- Kaltofen, E., Koiran, P., 2006. Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields. In: *ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation*. ACM Press, New York, NY, USA, pp. 162–168.
- Kaltofen, E., Lee, W-s., 2003. Early termination in sparse interpolation algorithms. *J. Symbolic Comput.* 36 (3–4), 365–400. *International Symposium on Symbolic and Algebraic Computation (ISSAC'2002)* (Lille).
- Karpinski, M., Shparlinski, I., 1999. On the computational hardness of testing square-freeness of sparse polynomials. *Electronic Colloquium on Computational Complexity (ECCC)* 6 (027).
- Landau, S., 1985. Factoring polynomials over algebraic number fields. *SIAM J. Comput.* 14, 184–195.
- Lenstra Jr., H.W., 1999. Finding small degree factors of lacunary polynomials. In: *Number Theory in Progress*, Vol. 1 (Zakopane-Kościelisko, 1997). de Gruyter, Berlin, pp. 267–276.
- Lidl, R., Niederreiter, H., 1983. Finite Fields. In: *Encyclopedia of Mathematics and its Applications*, vol. 20. Addison-Wesley, Reading MA.
- Mignotte, M., 1974. An inequality about factors of polynomials. *Math. Comp.* 28, 1153–1157.
- Plaisted, D.A., 1977. Sparse complex polynomials and polynomial reducibility. *J. Comp. Syst. Sci.* 14, 210–221.
- Plaisted, D.A., 1984. New NP-hard and NP-complete polynomial and integer divisibility problems. *Theoret. Comput. Sci.* 31, 125–138.
- Quick, A., Some gcd and divisibility problems for sparse polynomials. Technical Report 191/86, University of Toronto, 1986.
- Rosser, J.B., Schoenfeld, L., 1962. Approximate formulas for some functions of prime numbers. III. *J. Math.* 6, 64–94.
- Schinzel, A., 1987. On the number of terms of a power of a polynomial. *Acta Arith.* 49 (1), 55–70.
- Schwartz, J.T., 1980. Fast probabilistic algorithms for verification of polynomial identities. *J. Assoc. Comput. Mach.* 27, 701–717.
- Shoup, V., 1994. Fast construction of irreducible polynomials over finite fields. *J. Symbolic Comput.* 17 (5), 371–391.
- Shparlinski, I., 2000. Computing Jacobi symbols modulo sparse integers and polynomials and some applications. *J. Algorithms* 36 (2), 241–252.
- Weil, A., 1948. On some exponential sums. *Proc Natl. Acad. Sci. USA* 34, 204–207.
- Yun, D.Y.Y., 1976. On square-free decomposition algorithms. In: *SYMSAC'76: Proceedings of the Third ACM Symposium on Symbolic and Algebraic Computation*. ACM, New York, NY, USA, pp. 26–35.
- Zannier, U., 2007. On the number of terms of a composite polynomial. *Acta Arith.* 127 (2), 157–167.
- Zippel, R., Probabilistic algorithms for sparse polynomials. In: *Proc. EUROSAM 79, Marseille, 1979*, pp. 216–226.