Polynomial interpolation from multiples

Joachim von zur Gathen
Faculty of Computer Science, Electrical Engineering
and Mathematics, Universität Paderborn
33095 Paderborn, Germany
gathen@upb.de
http://www-math.upb.de/~gathen/

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@comp.mq.edu.au
http://www.comp.mq.edu.au/~igor/

October 2, 2003

Abstract

We are given an unknown polynomial $f \in \mathbb{Z}[x]$ by a black box which on input $a \in \mathbb{Z}$ returns a value $r_a \cdot f(a)$ for some unknown nonzero rational numbers r_a. If we have appropriate upper bounds on the numerator and denominator of r_a and the degree of f, then the coefficients of f can be computed in probabilistic polynomial time.

Keywords: Hidden polynomial, black box polynomial, approximate computation, short vectors, integer lattices.

1 Introduction

There are several ways of representing a univariate polynomial over a ring. The two most important date structures are the list of coefficients, and a list of values, together with a bound on the degree. The transformations between these two representations, namely evaluation and interpolation, play a basic role in many applications. In more general domains, including the rings of interest in number theory, interpolation becomes the Chinese Remainder Algorithm.

An interesting variation of the classical task of interpolation assumes that not the exact values are given, but only approximations to them. This may mean that each value may be "a little incorrect", or that some but not all values are correct. The usefulness of this problem first appeared in coding theory, with the classical Reed-Solomon codes and the more recent tool of list decoding. A number-theoretic version of importance in cryptography is the *hidden number problem*. It is, of course, necessary to have enough information in the incorrect values to allow reconstruction of the true object.

In this paper, we want to reconstruct a polynomial from approximate values all of which may be incorrect, in some controlled fashion. The case where the difference to the true values is bounded (and we work over a finite prime field), has been solved by Shparlinski (2002b). In this paper, we consider the interpolation task when the ratio to the true value is bounded appropriately.

More precisely, we want to compute the coefficients of a polynomial $f \in \mathbb{Z}[x]$ of degree n for which we are given a *multiplicatively approximate black box* $\mathrm{MABB}(A, \alpha, \beta)$ which on input $a \in \mathbb{Z}$, in time $(n \log(A|a| + 1))^{O(1)}$ returns a rational multiple $g_a = r_a \cdot f(a)$ of $f(a)$ for some unknown nonzero $r_a \in \mathbb{Q}$. Here A, α, and β are positive real numbers such that we can write $r_a = k_a/m_a$ with integers k_a, m_a and

(1.1) $$\gcd(k_a, m_a) = 1,\ 0 < |k_a| \le A|a|^{\alpha},\ 0 < |m_a| \le A|a|^{\beta}.$$

The gcd condition is convenient but obviously not necessary. We assume that the response time of the $\mathrm{MABB}(A, \alpha, \beta)$ is polynomial in the bit length of $|g_a|$ (thus queries with large values of a are more expensive).

We design a probabilistic polynomial time interpolation algorithm which works for an $\mathrm{MABB}(A, \alpha, \beta)$ with any $\alpha + \beta < 1/(n+2)$.

We also consider the same problem for polynomials

$f \in \mathbb{F}_p[x]$ over a finite prime field $\mathbb{F}_p$ of p elements with a *modular multiplicatively approximate black box*, MMABB(α, β, p) , which on input $a \in \mathbb{Z}$ returns a multiple $g_a = r_a \cdot f(a) \in \mathbb{F}_p$ of the value $f(a) \in \mathbb{F}_p$ with some factor $r_a \in \mathbb{F}_p^*$ such that $r_a \equiv k_a/m_a \bmod p$ for some integers k_a, m_a satisfying

(1.2)
$$\gcd(k_a, m_a) = 1, \quad 0 < |k_a| \le p^\alpha, \quad 0 < |m_a| \le p^\beta.$$

We obtain similar results for this problem, but the bound on the possible values of α and β is less generous.

The corresponding additive problem, where a black box produces a shift $s_a + f(a)$ for some integer s_a, has been solved in Shparlinski (2001) over $\mathbb{F}_p$, with a rather generous error bound on the size of s_a (roughly speaking, $|s_a|$ could be up to $p\exp(-\log^{1/2} p)$).

Loosely speaking, the problem we consider in this paper, as well as the above mentioned additive problem, are variants of the *hidden number problem* which has its origin in pioneering works of Boneh & Venkatesan (1996, 1997) and which has proved to be an invaluable tool for cryptography and computer science; see Shparlinski (2003) and also surveys given in Shparlinski (2002a,b).

It is no surprise that, as in most other works on the hidden number problem, our main tool is a lattice basis reduction algorithm.

Venkatesan Guruswami and Avi Wigderson have remarked that if the fudge factors r_a are always integers with a polynomial bound on their value, then we can divide by all integers up to the bound (which evenly divide the approximate value) and obtain a list which contains sufficiently many correct values so that the list decoding approach of Guruswami & Sudan (1999) recovers the polynomial. However in this paper, as well as in Shparlinski (2001), these factors may be chosen from exponentially large sets.

2 Lattices, linear homogeneous equations, and polynomials

Here we collect several well-known facts which form the background of our algorithm.

We review several related results and definitions on lattices which can be found in Grötschel *et al.* (1993). For more details and more recent references, we recommend to consult the brilliant surveys of Nguyen & Stern (2000, 2001).

Let $\{b_1, \ldots, b_s\}$ be a set of linearly independent vectors in $\mathbb{R}^r$. The set

$$L = \{z \colon z = c_1 b_1 + \ldots + c_s b_s,\ c_1, \ldots, c_s \in \mathbb{Z}\}$$

is called an *s-dimensional lattice* with *basis* $\{b_1, \ldots, b_s\}$. If $s = r$, the lattice L is of *full rank*.

To each lattice L one can naturally associate its *volume*

$$\mathrm{vol}\,(L) = \left(\det\left(\langle b_i, b_j\rangle\right)_{i,j=1}^{s}\right)^{1/2},$$

where $\langle a, b\rangle$ denotes the inner product, which does not depend on the choice of the basis $\{b_1, \ldots, b_s\}$.

For a vector u, let $\|u\|$ denote its *Euclidean norm*. The famous Minkowski theorem, see Theorem 5.3.6 in Section 5.3 of Grötschel *et al.* (1993), gives the upper bound

$$\min\{\|z\| \colon z \in L \setminus \{0\}\} \le s^{1/2}\mathrm{vol}\,(L)^{1/s} \tag{2.3}$$

on the shortest nonzero vector in any s-dimensional lattice L via its volume. In fact $s^{1/2}$ can be replaced by the slightly smaller *Hermite constant* $\gamma_s^{1/2}$, see Nguyen & Stern (2000, 2001).

The Minkowski bound (2.3) motivates a natural question: how to find the shortest vector in a lattice. Unfortunately, there are several indications that this problem is **NP**-complete (when the dimension grows), see Nguyen & Stern (2000, 2001). However, for a relaxed task of finding a short vector, the celebrated *LLL algorithm* of Lenstra *et al.* (1982) provides a desirable solution.

To simplify our calculations we use the *LLL* algorithm in its original form. Later developments of Schnorr (1987) and quite recently by Ajtai *et al.* (2001) lead to some (rather slight) improvements of our results.

We also assume that the basis $\{b_1, \ldots, b_s\}$ of L consists of vectors in $\mathbb{Z}^r$ (rather than in $\mathbb{R}^r$), so one can talk about the bit size of the basis and the notion of a polynomial-time algorithm.

LEMMA 2.1. *There exists a deterministic polynomial-time algorithm which, given a basis for an s-dimensional lattice L, finds a nonzero vector $v \in L$ with*

$$\|v\| \le 2^{(s-1)/2} \min\{\|z\| \colon z \in L \setminus \{0\}\}.$$

It is also useful to remember that when s is small (for example, constant), then in polynomial time one can find a nonzero vector $v \in L$ with $\|v\| = \min\{\|z\| \colon z \in L \setminus \{0\}\}$, see Ajtai *et al.* (2001); Nguyen & Stern (2000, 2001).

The set of integer solutions $z = (z_1, \ldots, z_r) \in \mathbb{Z}^r$ of a linear homogeneous Diophantine equation

$$\sum_{i=1}^{r} z_i c_i = 0$$

forms a lattice of dimension $r - 1$ (unless $c_1 = \cdots = c_r = 0$). The same is also true for the solutions $z \in \mathbb{Z}^r$ of a linear homogeneous congruence

$$\sum_{i=1}^{r} z_i c_i \equiv 0 \bmod p$$

modulo a prime p, except that in this case the set of integer solutions forms a lattice of dimension r.

Finally, for any polynomial $f \in \mathbb{K}[x]$ of degree at most n over any field $\mathbb{K}$ we have the well-known *Newton relations*

$$\sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} f(x+i) = 0. \tag{2.4}$$

Moreover, if $\deg f = n$ and the characteristic of $\mathbb{K}$ is greater than $n+1$ or zero then, because f can also be viewed as a linear recurrence sequence of order exactly $n+1$, any other linear relation between all $(n+2)$-tuples of consecutive values of f has coefficients proportional to those in (2.4). That is, if for some coefficients $C_0, \ldots, C_{n+1} \in \mathbb{K}$

$$\sum_{i=0}^{n+1} (-1)^i C_i f(x+i) = 0$$

for all positive integer x, then

$$C_i = \lambda (-1)^i \binom{n+1}{i}, \quad \text{for } 0 \le i \le n+1,$$

and some $\lambda \in \mathbb{K}$.

3 Polynomials over $\mathbb{Z}$

There is some nonuniqueness inherent in our problem. Namely, when the black box chooses all its fudge factors r_a as even integers, then we can in principle not tell whether the original polynomial is f or $2f$. Therefore we can at best expect a constant multiple of the original polynomial as output.

We call an integer polynomial *primitive* if the greatest common divisor of its coefficients is 1, and its leading term is positive. Each nonzero integer polynomial has a unique constant multiple which is primitive, and we make this our target, thus removing the non-uniqueness just mentioned.

As usual we define the *height* of a polynomial $f = \sum_{i=0}^{n} f_i x^i \in \mathbb{Z}[x]$ as

$$\mathcal{H}(f) = \max_{0 \le j \le n} |f_j|.$$

We consider the family $\mathcal{P}_n(H)$ of primitive polynomials of degree n and of height at most H:

$$\mathcal{P}_n(H) = \left\{ f(x) = \sum_{i=0}^{n} f_i x^i \in \mathbb{Z}[x] : \begin{array}{r} \gcd(f_0, \ldots, f_n) = 1, \\ f_n \ge 1, \mathcal{H}(f) \le H \end{array} \right\}.$$

THEOREM 3.1. *Let n and H be positive integers, and let α, β, δ be nonnegative real numbers with $0 < \delta < 1$ and $\alpha + \beta \le (1-\delta)/(n+2)$. There is a deterministic algorithm which, for any $f \in \mathcal{P}_n(H)$, computes the coefficients of f in time polynomial in $n, \log H, \log A$, and δ^{-1} using an MABB(A, α, β) for f.*

Proof. For each factor r_a we always write $r_a = k_a/m_a$ with k_a and m_a of the form (1.1).

Let $f \in \mathcal{P}_n(H)$ and $c = (c_0, \ldots, c_{n+1}) \in \mathbb{Z}^{n+2}$ be the vector of coefficients in (2.4), that is,

$$c_i = (-1)^i \binom{n+1}{i}, \quad 0 \le i \le n+1.$$

For a vector $b = (b_0, \ldots, b_{n+1}) \in \mathbb{Z}^{n+2}$, we consider the polynomial

$$h_b = \sum_{i=0}^{n+1} b_i f(x+i) \in \mathbb{Z}[x].$$

In particular, we have $h_c = 0$. Moreover, as discussed in Section 2, $h_b = 0$ if and only if the vectors b and c are proportional.

We let

$$B = \left\lceil \left((n+2)^{2n+2} (2A)^{2n+4} H \right)^{1/\delta} \right\rceil,$$

and consider nonzero vectors $b = (b_0, \ldots, b_{n+1}) \in [-B, B]^{n+2}$. We let

$$\mathcal{B} = \{ b \in [-B, B]^{n+2} : b \text{ not proportional to } c \}.$$

In particular, h_b is not identically zero for any $b \in \mathcal{B}$. A Taylor expansion at i of the ith summand of h_b gives

$$h_b = \sum_{j=0}^{n} \sum_{i=0}^{n+1} b_i \frac{f^{(j)}(i)}{j!} x^j = \sum_{j=0}^{n} \sum_{i=0}^{n+1} b_i \sum_{\nu=j}^{n} \binom{\nu}{j} f_\nu i^{\nu-j} x^j.$$

Estimating each term trivially we obtain for $b \in \mathcal{B}$

$$\mathcal{H}(h_b) \le (n+2)(n+1)^{n+1} 2^n B \mathcal{H}(f) \le (n+2)^{n+2} 2^n B H.$$

Hence for $b \in \mathcal{B}$, the absolute value of any zero of h_b is less than $\mathcal{H}(h_b) + 1 < (n+2)^{2n+2} B H$.

We now set $a = (n+2)^{2n+2} B H$ and query the approximate black box for f with inputs $a+i$ to receive the values

$$g_{a+i} = r_{a+i} \cdot f(a+i) = \frac{k_{a+i}}{m_{a+i}} \cdot f(a+i) \quad \text{for } 0 \le i \le n+1.$$

All values g_{a+i} are nonzero because $a \ge \mathcal{H}(f) + 1$. We consider the $(n+1)$-dimensional lattice

$$L = \left\{ z = (z_0, \ldots, z_{n+1}) \in \mathbb{Z}^{n+2} : \sum_{i=0}^{n+1} z_i g_{a+i} = 0 \right\},$$

and the integers

$$K = \prod_{j=0}^{n+1} k_{a+j}, \quad M = \prod_{j=0}^{n+1} m_{a+j},$$

and

$$K_i = \frac{k_{a+i}}{m_{a+i}} M, \quad M_i = \frac{m_{a+i}}{k_{a+i}} K \quad \text{for } 0 \le i \le n+1.$$

Then

(3.5)

$$|K_i| \le A^{n+2}(a+i)^{\alpha+\beta(n+1)}, \ |M_i| \le A^{n+2}(a+i)^{\alpha(n+1)+\beta}$$

for $0 \le i \le n+1$. We see that L contains the "short" vector $u = (u_0, \ldots, u_{n+1})$ with

$$u_i = c_i M_i \quad \text{for } 0 \le i \le n+1.$$

By (3.5) its norm satisfies

$$\begin{aligned} \|u\| &\le A^{n+2}(a+n+1)^{\alpha(n+1)+\beta} \left(\sum_{i=0}^{n+1} c_i^2 \right)^{1/2} \\ &\le A^{n+2}(a+n+1)^{\alpha(n+1)+\beta} \sum_{i=0}^{n+1} |c_i| \\ &= 2^{n+1} A^{n+2}(a+n+1)^{\alpha(n+1)+\beta} \end{aligned}$$

and thus the algorithm of Lemma 2.1 returns a vector $v = (v_0, \ldots, v_{n+1}) \in L$ with

$$\|v\| \le 2^{(n+1)/2}\|u\| \le 2^{3(n+1)/2} A^{n+2}(a+n+1)^{\alpha(n+1)+\beta}.$$

We have

$$\begin{aligned} |v_i K_i| &\le 2^{3(n+1)/2} A^{2n+4}(a+n+1)^{(\beta+\alpha)(n+2)} \\ &\le (2A)^{2n+4} a^{(\beta+\alpha)(n+2)} \\ &\le (2A)^{2n+4} a^{1-\delta} \\ &= (2A)^{2n+4} \left((n+2)^{2n+2} BH\right)^{1-\delta} \\ &\le (n+2)^{2n+2}(2A)^{2n+4} HB^{1-\delta} \le B \end{aligned}$$

for $0 \le i \le n+1$. Since

$$0 = \sum_{i=0}^{n+1} v_i M g_{a+i} = \sum_{i=0}^{n+1} v_i K_i f(a+i),$$

it follows that $(v_0 K_0, \ldots, v_{n+1} K_{n+1})$ is proportional to c, say $v_i K_i = \lambda c_i$ for some nonzero $\lambda \in \mathbb{Q}$ and all $i \le n+1$. We now calculate the unique interpolation polynomial $g \in \mathbb{Q}[x]$ of degree at most n with $g(a+i) = g_{a+i} v_i / c_i$ for $0 \le i \le n$. (The value for $i = n+1$ is ignored.) Since

$$g(a+i) = g_{a+i} v_i / c_i = \lambda g_{a+i} / K_i = \lambda f(a+i)/M$$

for $0 \le i \le n$, g is a nonzero constant multiple of f. Finding f from g is trivial. The cost estimate is immediate. □

4 Polynomials over finite fields

Here we show that the approach of Section 3 works for polynomials over $\mathbb{F}_p$ for a prime p.

To avoid the nonuniqueness problem in the case of polynomials over $\mathbb{F}_p$ it is more natural to consider monic polynomials rather than primitive ones. As in any ring, multiplication by integers is well-defined, so that $ay \in \mathbb{F}_p$ for any $a \in \mathbb{Z}$ and $y \in \mathbb{F}_p$. Similarly, we have $h(a) \in \mathbb{F}_p$ for $a \in \mathbb{Z}$ and $h \in \mathbb{F}_p[x]$.

We consider the family $\mathcal{M}_{n,p}$ of monic polynomials of degree n:

$$\mathcal{M}_{n,p} = \Big\{ f(x) = \sum_{i=0}^{n} f_i x^i \in \mathbb{F}_p[x] \colon f_n = 1 \Big\}.$$

THEOREM 4.1. *Let n be a positive integer, and let $\alpha, \beta, \delta, \varepsilon$ be nonnegative real numbers with $0 < \delta, \varepsilon < 1$ and $\alpha + \beta = (1-\delta)/(n+2)^2$. Then for any prime*

$$p > 2^{(2n+6)(n+2)/\delta} \varepsilon^{-1/\delta}$$

there is a probabilistic algorithm which for any $f \in \mathcal{M}_{n,p}$ computes with probability at least $1-\varepsilon$ the coefficients of f in time polynomial in $n, \log p, \delta^{-1}$ and $\log \varepsilon^{-1}$ using an MMABB(α, β, p) for f.

Proof. For each factor r_a we always write $r_a = k_a/m_a$ with k_a and m_a are of the form (1.2).

The assumptions imply that $p > n+1$. We define the vector $c \in \mathbb{Z}^{n+2}$ and the polynomials $h_b \in \mathbb{F}_p[x]$ for $b \in \mathbb{Z}^{n+2}$ in exactly the same way as in the proof of Theorem 3.1. In particular, we have $h_c = 0$, and $h_b = 0$ if and only if the vectors b and c are proportional modulo p. We let

$$B = \left\lfloor \frac{1}{6} (\varepsilon p)^{1/(n+2)} \right\rfloor$$

and consider nonzero vectors $b = (b_0, \ldots, b_{n+1}) \in [-B, B]^{n+2}$. We let

$$\mathcal{B} = \{ b \in [-B, B]^{n+2} \colon b \text{ not proportional } c \text{ over } \mathbb{F}_p \},$$

and for $b \in \mathcal{B}$, we consider $\mathcal{A}_b = \{ a \in \mathbb{Z} \colon h_b(a) = 0 \}$. We have $\#\mathcal{A}_b \le n$, and $\mathcal{A} = \bigcup_{b \in \mathcal{B}} \mathcal{A}_b$ has at most

$$n(2B+1)^{n+2} < n 3^{n+2} B^{n+2} \le 6^{n+2} B^{n+2} \le \varepsilon p$$

elements. We choose a uniformly at random from $\mathbb{F}_p$, so that $\mathrm{Prob}(a \in \mathcal{A}) < \varepsilon$. We now query the approximate black box for f with the inputs $a+i$ to receive the values $g_{a+i} = r_{a+i} \cdot f(a+i)$ for $0 \le i \le n+1$.

Because f is not identically zero, at least one value $g_{a+i} \in \mathbb{F}_p$ is nonzero. We consider the $(n+1)$-dimensional lattice

$$L = \Big\{ z = (z_0, \ldots, z_{n+1}) \in \mathbb{Z}^{n+2} \colon \sum_{i=0}^{n+1} z_i g_{a+i} = 0 \Big\}.$$

We also denote

$$K = \prod_{j=0}^{n+1} k_{a+j}, \quad M = \prod_{j=0}^{n+1} m_{a+j}$$

and

$$K_i = \frac{k_{a+i}}{m_{a+i}} M, \quad M_i = \frac{m_{a+i}}{k_{a+i}} K, \quad 0 \le i \le n+1.$$

In particular

$$|K_i| \le p^{\alpha+(n+1)\beta}, \quad |M_i| \le p^{(n+1)\alpha+\beta} \tag{4.6}$$

for $0 \le i \le n+1$. We see that L contains the "short" vector $u = (u_0, \ldots, u_{n+1}) \in L$ with

$$u_i = c_i M_i \quad \text{for } 0 \le i \le n+1.$$

By (4.6) its norm satisfies

$$\begin{aligned} \|u\| &\le p^{\alpha(n+1)+\beta} \left(\sum_{i=0}^{n+1} c_i^2 \right)^{1/2} \\ &\le p^{\alpha(n+1)+\beta} \sum_{i=0}^{n+1} |c_i| \\ &= 2^{n+1} p^{\alpha(n+1)+\beta}, \end{aligned}$$

and the algorithm of Lemma 2.1 returns a vector $v = (v_0, \ldots, v_{n+1}) \in L$ with

$$\|v\| \le 2^{(n+2)/2} \|u\| \le 2^{2n+2} p^{\alpha(n+1)+\beta}.$$

The assumption in the theorem implies that $B \ge 1$, and therefore

$$B \ge \frac{B+1}{2} \ge \frac{1}{12} p^{1/(n+2)} \varepsilon^{1/(n+2)} \ge 2^{2n+2} p^{(1-\delta)/(n+2)}.$$

We have

$$|v_i K_{a+i}| \le 2^{2n+2} p^{(\alpha+\beta)(n+2)} \le 2^{2n+2} p^{(1-\delta)/(n+2)} \le B$$

for all $i \le n+1$. Now we assume that $a \notin \mathcal{A}$. Since

$$0 = \sum_{i=0}^{n+1} v_i M g_{a+i} = \sum_{i=0}^{n+1} v_i K_i f(a+i),$$

it follows that $(v_0 K_0, \ldots, v_{n+1} K_{n+1})$ is proportional modulo p to c, say $v_i K_i = \lambda c_i$ for some integer λ with $\lambda \not\equiv 0 \bmod p$ and all $i \le n+1$. Since $p > n+1$, each c_i with $i \le n+1$ is nonzero modulo p. We now calculate the unique interpolation polynomial $g \in \mathbb{F}_p[x]$ of degree at most n with $g(a+i) = g_{a+i} v_i / c_i \in \mathbb{F}_p$ for $0 \le i \le n$. (The value for $i = n+1$ is ignored.) Since

$$g(a+i) = g_{a+i} v_i / c_i = \lambda g_{a+i} / K_i = \lambda f(a+i)/M$$

for $i \le n$, g is a nonzero constant multiple of f, and $f = \mathrm{lc}(g)^{-1} \cdot g$, where $\mathrm{lc}(g)$ is the leading coefficient of g. The cost estimate is immediate. □

5 Remarks

Our algorithm works with $\alpha + \beta = O(n^{-1})$ over $\mathbb{Z}$ and with $\alpha + \beta = O(n^{-2})$ over $\mathbb{F}_p$. The example of two polynomials xg and $(x+1)g$ where $\deg g = n-1$ shows that it is impossible to solve this problem with $\alpha > 1$. Indeed, the black box output $a(a+1)g(a)$ is consistent with both polynomials. It is an open question by how much our bound on $\alpha + \beta$ can be relaxed. Is there a polynomial-time method when $\alpha + \beta = O(n^{-1})$ over $\mathbb{F}_p$? Finally, can the lower bound on p in Theorem 4.1 be lowered?

It is easy to see that our method can also be applied to interpolating linear recurrence sequences instead of polynomials, which satisfy a given linear recurrence relation

$$\sum_{i=0}^{n+1} c_i u(x+i) = 0.$$

The cost of the corresponding algorithm depends on the size of the coefficients in the above relation. To justify the algorithm one can use bounds on the number of zeros of linear recurrence sequences over $\mathbb{Z}$ and in finite fields; see Everest *et al.* (2002), or the original papers Evertse & Schlickewei (1999); van der Poorten & Schlickewei (1991); Schlickewei *et al.* (1999); Schmidt (2000).

One can obtain an algorithm which interpolates a t-sparse polynomial with only $t+1$ queries to an MABB(A, α, β) or an MMABB(α, β, p); the whole algorithm however remains polynomial in n, not in t and $\log n$ as one would desire for t-sparse polynomials.

One can also consider polynomials with rational coefficients for which there is black box returning rational multiples of their values with controlled numerator and denominator.

Our method, combined with the method of Shparlinski (2001), can be applied to the more general problem of recovering k polynomials $f_1, \ldots, f_k$ from polynomially many vectors $R_a \cdot (f_1(a), \ldots, f_k(a))^T + s_a$ for some "small" matrices R_a and vectors s_a.

Finally, our method can be extended to polynomials $f(x_1, \ldots, x_m)$ in $m \ge 2$ variables by making *Kronecker queries* of the form $f\left(a, a^{d+1}, \ldots, a^{(d+1)^{m-1}}\right)$ and thus reducing this case to the univariate case.

We conclude by mentioning that it would be interesting to consider an analog of our problem over a residue ring of the integers modulo an integer. One of our crucial ingredients, namely the fact that the number of roots of a polynomial is bounded by its degree, does not apply anymore. However, over such rings one can try to use a much weaker bound of Konyagin (1979).

Instead of recovering a hidden polynomial, we can ask to construct a number x given by a black box

returning $r_p x \bmod p$ on input p, for a prime p and a small rational number r_p. One will have additional constraints, such as bounds on $|x|$ and on the primes. This problem is now under consideration.

Acknowledgement. The authors thank Venkatesan Guruswami and Avi Wigderson for useful discussions and in particular for attracting our attention to the possible application of list decoding as in Guruswami & Sudan (1999), to the special case where the fudge factors are polynomially bounded in value.

References

Miklós Ajtai, Ravi Kumar & D. Sivakumar (2001). A Sieve Algorithm for the Shortest Lattice Vector Problem. In *Proceedings of the Thirty-third Annual ACM Symposium on the Theory of Computing,* Hersonissos, Crete, Greece, 601–610. ACM Press, 1515 Broadway, New York, New York 10036. ISBN 1-58113-349-9.

Dan Boneh & Ramarathnam Venkatesan (1996). Hardness of Computing the Most Significant Bits of Secret Keys in Diffie-Hellman and Related Schemes. In *Advances in Cryptology: Proceedings of CRYPTO '96,* Santa Barbara CA, N. Koblitz, editor, number 1109 in Lecture Notes in Computer Science, 129–142. Springer-Verlag, Springer-Verlag. ISBN 3-540-61512-1. ISSN 0302-9743. URL `http://link.springer.de/link/service/series/0558/tocs/t1109.htm`.

Dan Boneh & Ramarathnam Venkatesan (1997). Rounding in lattices and its cryptographic applications. *Proceedings of the 8th Annual ACM-SIAM Symposium on Descrete Algorithms, ACM* 675–681. URL `http://crypto.stanford.edu/~dabo/abstracts/nonuniform.html`.

Graham Everest, Alf van der Poorten, Igor Shparlinski & Thomas Ward (2002). Exponential functions, linear recurrence sequences, and their applications.

Jan-Hendrik Evertse & Hans Peter Schlickewei (1999). The Absolute Subspace Theorem and linear equations with unknowns from a multiplicative group. *Number Theory in Progress* **1**, 121–142. URL `http://www.math.leidenuniv.nl/~evertse/98-absolute.pdf`.

Martin Grötschel, László Lovász & Alexander Schrijver (1993). *Geometric Algorithms and Combinatorial Optimization.* Number 2 in Algorithms and Combinatorics. Springer-Verlag, Berlin, Heidelberg, 2nd edition. First edition 1988.

V. Guruswami & M. Sudan (1999). Improved decoding of Reed-Solomon codes and algebraic-geometric codes. *IEEE Transactions on Information Theory* **45**, 1757–1767.

S. V. Konyagin (1979). О числе решений сравнения n-й степени с одним неизвестным (On the number of solutions of a univariate congruence of the nth degree). *Matematiceskij Sbornik* **102**, 171–187.

A. K. Lenstra, H. W. Lenstra, Jr. & L. Lovász (1982). Factoring Polynomials with Rational Coefficients. *Mathematische Annalen* **261**, 515–534.

Phong Q. Nguyen & Jacques Stern (2000). Lattice Reduction in Cryptology: An Update. In *Algorithmic Number Theory, Proceedings ANTS-IV,* Leiden, The Netherlands, Wieb Bosma, editor, number 1838 in Lecture Notes in Computer Science, 85–112. Springer-Verlag. ISSN 0302-9743. URL `http://www.di.ens.fr/~stern/publications.html`.

Phong Q. Nguyen & Jacques Stern (2001). The Two Faces of Lattices in Cryptology. In *Cryptography and Lattices, International Conference (CaLC 2001),* Providence RI, Joseph H. Silverman, editor, number 2146 in Lecture Notes in Computer Science, 146–180. Springer-Verlag. ISSN 0302-9743. URL `http://www.di.ens.fr/~pnguyen/pub.html#NgSt01`.

A. J. van der Poorten & H. P. Schlickewei (1991). Zeros of recurrence sequences. *Bulletin of the Australian Mathematical Society* **44**, 215–223. URL `http://www.institut.math.jussieu.fr/~miw/articles/HPS-WMS-MW.html`.

Hans Peter Schlickewei, Wolfgang M. Schmidt & Michel Waldschmidt (1999). Zeros of linear recurrence sequences. *Manuscripta Mathematica* **98**(2), 225–241. URL `http://link.springer.de/link/service/journals/00229/`.

W. Schmidt (1991). *Diophantine approximations and Diophantine equations.* Springer-Verlag, Berlin.

Wolfgang M. Schmidt (2000). Zeros of linear recurrence sequences. *Publicationes Mathematicae (Debrecen)* **56**(3-4), 609–630.

C. P. Schnorr (1987). A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science* **53**, 201–224.

Igor E. Shparlinski (2001). Sparse Polynomial Approximation in Finite Fields. In *Proceedings of the Thirty-third Annual ACM Symposium on the Theory of Computing,* Hersonissos, Crete, Greece, 209–215. ACM Press, 1515 Broadway, New York, New York 10036. ISBN 1-58113-349-9.

Igor E. Shparlinski (2002a). Exponential Sums and lattice Reduction: Applications to Cryptography. *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas* **1**, 286–298. URL `http://www.comp.mq.edu.au/~igor/ExpSums-Lat.ps`.

Igor E. Shparlinski (2002b). Playing "Hide-and-Seek" in Finite Fields: The Hidden Number Problem and Its Applications. *Proceedings of the 7th Spanish Meeting on Cryptology and Information Security* **1**, 49–72. URL `http://www.comp.mq.edu.au/~igor/Hide-Seek.ps`.

I. E. Shparlinski (2003). *Cryptographic applications of analytic number theory.* Birkhäuser Verlag.