A Zero-Test and an Interpolation Algorithm for the Shifted Sparse Polynomials

Dima Grigoriev [*]
Dept. of Computer Science
University of Bonn
5300 Bonn 1

Marek Karpinski [†]
Dept. of Computer Science
University of Bonn
5300 Bonn 1
and
International Computer Science Institute
Berkeley, California

Abstract

Recall that a polynomial $f \in F[X_1, \ldots, X_n]$ is t -sparse, if $f = \sum \alpha_I X^I$ contains at most t terms. In [BT 88], [GKS 90] (see also [GK 87] and [Ka 89]) the problem of interpolation of t-sparse polynomial given by a black-box for its evaluation has been solved. In this paper we shall assume that F is a field of characteristic zero. One can consider a t-sparse polynomial as a polynomial represented by a straight-line program or an arithmetic circuit of the depth 2 where on the first level there are multiplications with unbounded fan-in and on the second level there is an addition with fan-in t.

In the present paper we consider a generalization of the notion of sparsity, namely we say that a polynomial $g(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ is *shifted t-sparse* if for a suitable nonsingular $n \times n$ matrix A and a vector B the polynomial $g(A(X_1, \ldots, X_n)^T + B)$ is t-sparse. One could consider g as being represented by a straight-line program of the depth 3 where on the first level (with the fan-in $n+1$) a linear transformation $A(X_1, \ldots, X_n)^T + B$ is computed. One could also consider a shifted t-sparse polynomial as t-sparse with respect to other coordinates $(Y_1, \ldots, Y_n)^T = A(X_1, \ldots, X_n)^T + B$.

[*] On leave from Steklov Mathematical Institute, Fontanka 27, St. Petersburg, 191011 Russia

[†] Supported in part by Leibniz Center for Research in Computer Science, by the DFG Grant KA 673/4-1 and by the SERC Grant GR-E 68297

We assume that a shifted t-sparse polynomial g is given by a black-box and the problem we consider is to construct a transformation $A(X_1, \dots, X_n)^T + B$. As the complexity of the designed below algorithm (see the Theorem in which we describe the variety of all possible A, B and the corresponding t-sparse representations of $g(A(X_1, \dots, X_n)^T + B)$) depends on d^{n^4} where d is the degree of g, we could first interpolate g within time $d^{O(n)}$ and suppose that g is given explicitly. It would be interesting to get rid of d in the complexity bounds as it is usually done in the interpolation of sparse polynomials ([BT 88], [GKS 90], [Ka 89]). The main technical tool we rely on is the criterium of t-sparsity based on Wronskian ([GKS 91], [GKS 92]), the latter criterium has a *parametrical* nature (so we can select t-sparse polynomials from a given *parametrical* family of polynomials) unlike the approach in [BT 88] using BCH-codes.

We could directly consider (see the Theorem) the multivariate polynomials (section 3), but to make the exposition clearer before that we first study (see the proposition) the one-variable case (section 2). First at all we recall (section 1) the criterium of t-sparsity and based on it interpolation method for t-sparse multivariable polynomials.

In the last section 4 we design a zero-test algorithm for shifted t-sparse polynomials with the complexity independent on d.

1 A Criterium of t-sparsity and the Interpolation

Let $p_1, \ldots, p_n$ be pairwise distinct primes and denote by D a linear operator mapping $D : X_1 \to p_1 X_1, \ldots, D : X_n \to p_n X_n$. We recall a criterium of t-sparsity (cf. also [BT 88]).

Lemma 1. ([GKS 91], [GKS 92]) *A polynomial $f \in F[X_1, \ldots, X_n]$ is t-sparse if and only if the Wronskian*

$$W_f(X_1, \ldots, X_n) = \det \begin{pmatrix} f & Df & \ldots & D^t f \\ Df & D^2 f & \ldots & D^{t+1} f \\ \vdots & \vdots & & \vdots \\ D^t f & D^{t+1} f & \ldots & D^{2t} f \end{pmatrix} \in F[X_1, \ldots, X_n]$$

vanishes identically.

An interpolation method from [BT 88] (see also [KY 88]) actually considers the Wronskian $W_f(1, \ldots, 1)$ at the point $(1, \ldots, 1)$ and is based on the following

Lemma 2. ([BT 88]) *If f is exactly t-sparse (i.e., f contains exactly t terms), then the reduced Wronskian does not vanish*

$$\bar{W}_f(1, \ldots, 1) = \det \begin{pmatrix} f(1, \ldots, 1) & (Df)(1, \ldots, 1) & \ldots & (D^{t-1} f)(1, \ldots, 1) \\ \vdots & \vdots & & \vdots \\ (D^{t-1} f)(1, \ldots, 1) & (D^t f)(1, \ldots, 1) & \ldots & (D^{2t-2} f)(1, \ldots, 1) \end{pmatrix} \neq 0$$

at the point $(1, \ldots, 1)$.

Thus, if $f = \sum \alpha_I X^I$ is exactly t-sparse and if a (characteristic) polynomial $\chi(Z) = \sum\limits_{0 \le j \le t} \gamma_j Z^j \in \mathbb{Z}[\mathbb{Z}]$ has as its t roots p^I for all exponent vectors I occuring in f (where for $I = (i_1, \ldots, i_n)$ we denote $p^I = p_1^{i_1} \cdots p_n^{i_n}$), then $\sum\limits_{0 \le j \le t} \gamma_j D^j f = 0$ and hence

$$\begin{pmatrix} f & Df & \ldots & D^t f \\ \vdots & \vdots & & \vdots \\ D^t f & D^{t+1} f & \ldots & D^{2t} f \end{pmatrix} (\gamma_0, \ldots, \gamma_t)^T = 0 \, .$$

Therefore, a linear system

$$\begin{pmatrix} f(1, \ldots, 1) & (Df)(1, \ldots, 1) & \ldots & (D^t f)(1, \ldots, 1) \\ \vdots & \vdots & & \vdots \\ (D^t f)(1, \ldots, 1) & (D^{t+1} f)(1, \ldots, 1) & \ldots & (D^{2t} f)(1, \ldots, 1) \end{pmatrix} (Y_0, \ldots, Y_t)^T = o$$

has (up to a constant multiple) a unique (by lemma 2) solution $(Y_0, \ldots, Y_t) = (\gamma_0, \ldots, \gamma_t)$ which gives the coefficients of χ, thereby its roots p^I and finally I.

2 One-variable Shifted Sparse Polynomials

A polynomial $g \in F[X]$ is called *shifted t-sparse* if for an appropriate b a polynomial $g(X-b)$ is t-sparse (so the origin is shifted from 0 to b). If t is the least possible, we say that g is *minimally shifted t-sparse*, this notion relates also to the multivariable case. Let $F = \mathbb{Q}$. Usually we take b from the algebraic closure $\bar{\mathbb{Q}}$ (we could also consider b from $\mathbb{R}$). Assume that the bit-size of the (rational) coefficients of g does not exceed M.

Consider a new variable Y and an $\mathbb{Q}(\mathbb{Y})$-linear transformation of the ring $\mathbb{Q}(\mathbb{Y})[\mathbb{X}]$ mapping $D_1 : X \rightarrow p_1 X + (p_1 - 1)Y$. Denote

$$\mathcal{W}_g(X,Y) = \det \begin{pmatrix} g & D_1 g & \ldots & D_1^t g \\ \vdots & \vdots & & \vdots \\ D_1^t g & D_1^{t+1} g & \ldots & D_1^{2t} g \end{pmatrix} \in \mathbb{Q}[\mathbb{X}, \mathbb{Y}]$$

Lemma 3. *g is shifted t-sparse if and only if for some $Y = b$ a polynomial $\mathcal{W}_g(X,b)$ vanishes identically. Moreover in this case a polynomial $g(X-b)$ is t-sparse.*

Proof. If $g(X-b)$ is t-sparse, then the expansion $g = \sum_j \beta_j (X+b)^j$ into the powers of $(X+b)$ contains at most t terms. Lemma 1 implies that $\mathcal{W}_g(X,b)$ vanishes identically. The other direction follows also from lemma 1 which completes the proof.

Observe that for almost every b the polynomial $g(X-b)$ has exactly $(d+1)$ terms, where $d = \deg(g)$, since in the polynomial $g(X-Y) \in \mathbb{Q}[\mathbb{X}, \mathbb{Y}]$ the coefficient in the power X^S is a polynomial in Y of degree exactly $d - S$, $0 \leq S \leq d$.

Lemma 3 provides an algorithm for finding t such that g is minimal shifted t-sparse which runs in time $d^{O(1)}$ (trying successively $t = 1, 2, \ldots$), moreover this algorithm finds all $Y = Y_0$ such that $g(X - Y_0)$ is t-sparse. Namely, one writes down a polynomial system in Y equating to zero all the coefficients in the powers of X, thus the system contains $d^{O(1)}$ equations of degrees at most $d^{O(1)}$. So, one can prove the following proposition.

Proposition. *There is an algorithm which for one-variable polynomial g finds the minimal t and all Y_0 for which $g(X-Y_0)$ is t-sparse in time $(Md)^{O(1)}$. The number of such Y_0 does not exceed $d^{O(1)}$.*

One of the purposes of the sparse analysis is to get rid of d in the complexity bounds. We can write down a system in b with a less (for small t) number of equations, when b is supposed to belong to $\mathbb{R}$. So, assume that the expansion $g = \sum_j \beta_j (X+b)^j$ contains at most t terms for some $b \in \mathbb{R}$. Then for any fixed $Y = Y_0 \in \mathbb{R}$ a polynomial $(D_1^K g)(X, Y_0) = \sum_j \beta_j (p_1^K (X+Y_0) - Y_0 + b)^j$ for $K \geq 0$. Therefore the polynomial $\mathcal{W}_g(X, Y_0)$ has at most $2^{O(t^4)}$ real roots because of [Kh 91] since one can consider $(2t+1)t$ powers of linear polynomials $(p_1^K(X+Y_0) - Y_0 + b)^j, \quad 0 \leq K \leq 2t$ as the elements of a Pfaffian chain [Kh 91].

Thus Y satisfies the conditions of lemma 3 if and only if it satisfies the following system of polynomial equations (cf. lemma 5 below)

$$\mathcal{W}_g(0, Y) = \mathcal{W}_g(1, Y) = \ldots = \mathcal{W}_g(2^{O(t^4)}, Y) = 0\ .$$

Each of the polynomials from the latter system can be represented by a black-box for its evaluation. As each of these polynomials $\mathcal{W}_g(s, Y)$ contains $(2t+1)t$ powers $(p_1^K(s+Y) - Y + b)^j, \quad 0 \leq K \leq 2t$ the system has at most $2^{O(t^4)}$ real solutions (by the same argument relying on [Kh 91] as above), thus the number of such $Y = Y_0$ that $g(X - Y_0)$ is t-sparse is less than $2^{O(t^4)}$.

3 Multivariate Shifted Sparse Polynomials

Consider now $n^2 + n$ new variables $Z_{i,j}, Y_i, \quad 1 \leq i, j \leq n$ and a $\mathbb{Q}(\{\mathbb{Z}_{ij}, \mathbb{Y}_i\}_{1\leq i,j\leq n})$-linear transformation D_n of the ring $\mathbb{Q}(\{\mathbb{Z}_{ij}, \mathbb{Y}_i\}_{1\leq i,j\leq n})[\mathbb{X}_1, \ldots, \mathbb{X}_n]$ mapping

$$D_n X = Z P Z^{-1}(X - Y) + Y$$

where vectors $X = (X_1, \ldots, X_n)^T, Y = (Y_1, \ldots, Y_n)^T$, matrices $Z = (Z_{ij})$, $P = \begin{pmatrix} p_1 & & 0 \\ & \ddots & \\ 0 & & p_n \end{pmatrix}$. Similarly, as above denote

$$\mathcal{W}_g(X, Y, Z) = \det \begin{pmatrix} g & D_n g & \ldots & D_n^t g \\ \vdots & \vdots & & \vdots \\ D_n^t g & D_n^{t+1} g & \ldots & D_n^{2t} g \end{pmatrix} \in \mathbb{Q}(\mathbb{Z})[\mathbb{X}, \mathbb{Y}] .$$

Lemma 4. *g is shifted t-sparse if and only if for some Z_0, Y_0 such that $det Z_0 \neq 0$, the polynomial $\mathcal{W}_g(X, Y_0, Z_0)$ vanishes identically. Moreover, in this case a polynomial $g(Z_0 X + Y_0)$ is t-sparse.*

The proof is similar to the proof of lemma 3 taking into account that

$$(D_n g)(ZX + Y) = g(ZPZ^{-1}(ZX + Y - Y) + Y) = g(ZPX + Y) .$$

As in section 2 lemma 4 provides a test for minimal shifted t-sparsity trying successively $t = 1, 2, \ldots$ running in time $d^{O(n^4)}$ (see [CG 83] for solving system of polynomial equations and inequalities). Moreover, the algorithm finds algebraic conditions (equations and inequality $\det Z \neq 0$) on all Z, Y for which $g(ZX + Y)$ is t-sparse.

So, these Z, Y form a constructive set $U \subset \bar{\mathbb{Q}}^{n^2+n}$ given by a system $h_1 = \ldots = h_k = 0$, $\det Z \neq 0$ where $h_1, \ldots, h_k \in \mathbb{Q}[\{\mathbb{Z}_{\beth\gimel}, \mathbb{Y}_\beth\}_{\nVdash \leq \beth, \gimel \leq \ltimes}]$, then $\deg(h_1), \ldots, \deg(h_k) \leq d^{O(1)}$, $k \leq d^{O(1)}$. Applying the algorithm from [CG 83] one can find the irreducible over $\mathbb{Q}$ components $\bar{U} = \bigcup_l U^{(l)}$ of the closure (in the Zariski topology) $\bar{U}$. For each component $U^{(l)}$ the algorithm from [CG 83] produces firstly, some polynomials $h_1^{(l)}, \ldots, h_{N(l)}^{(l)} \in \mathbb{Q}[\{\mathbb{Z}_{\beth\gimel}, \mathbb{Y}_\beth\}]$ such that $U^{(l)} = \{h_1^{(l)} = \ldots = h_{N(l)}^{(l)} = 0\}$ and secondly, a general point of $U^{(l)}$, namely the following fields isomorphism

$$\mathbb{Q}(\mathbb{U}^{(\lessdot)}) \simeq \mathbb{Q}(\mathbb{T}_{\nVdash}, \ldots, \mathbb{T}_{\gtrdot})[\theta]$$

where $\mathbb{Q}(\mathbb{U}^{(\lessdot)})$ is the field of rational functions on $U^{(l)}$, $m = \dim(U^{(l)})$, linear forms $T_1, \ldots, T_m$ in variables $\{Z_{ij}, Y_i\}_{1 \leq i,j \leq n}$ constitute a transcendental basis of $\mathbb{Q}(\mathbb{U}^{(\lessdot)})$ and θ is algebraic over $\mathbb{Q}(\mathbb{T}_{\nVdash}, \ldots, \mathbb{T}_{\gtrdot})$. The algorithm produces a minimal polynomial $\phi(Z) \in \mathbb{Q}(\mathbb{T}_{\nVdash}, \ldots, \mathbb{T}_{\gtrdot})[\mathbb{Z}]$ of θ, the linear forms $T_S(\{Z_{ij}, Y_i\})$, $1 \leq S \leq m$, a linear form $\theta(\{Z_{ij}, Y_i\})$, and the expressions for the coordinate functions $Z_{i,j}(T_1, \ldots, T_m, \theta), Y_i(T_1, \ldots, T_m, \theta)$ as rational functions in $T_1, \ldots, T_m, \theta$. The degrees of the polynomials $h_1^{(l)}, \ldots, h_{N(l)}^{(l)}$ do not exceed $d^{O(n^2)}$, the bit-size of any of the (rational) coefficients occuring in these polynomials can be bounded by $M^{O(1)}d^{O(n^2)}$ and the algorithm runs in time $M^{O(1)}d^{O(n^4)}$.

Denote $\tilde{U}^{(l)} = U^{(l)} \setminus \{\det Z = 0\}$ (some of $\tilde{U}^{(l)}$ can be empty), remark that $U = \bigcup\limits_{l} \tilde{U}^{(l)}$.

For any point $(Z_0, Y_0) \in \tilde{U}^{(l)}$ the polynomial $g(Z_0X + Y_0)$ is exactly t-sparse, therefore by lemma 2 the following linear system

$$\begin{pmatrix} g(X_0, Y_0, Z_0) & D_n g(X_o, Y_0, Z_0) & \ldots & D_n^t g(X_0, Y_0, Z_0) \\ \vdots & \vdots & & \vdots \\ D_n^t g(X_0, Y_0, Z_0) & D_n^{t+1} g(X_0, Y_0, Z_0) & \ldots & D_n^{2t} g(X_0, Y_0, Z_0) \end{pmatrix} (\gamma_0, \ldots, \gamma_{t-1}, 1) = 0$$

has a unique solution, where the vector $X_0 = Z_0^{-1}((1, \ldots, 1)^T - Y_0)$. As $\gamma_0, \ldots, \gamma_{t-1} \in \mathbb{Z}$ (see section 1) and $\gamma_0, \ldots, \gamma_{t-1}$ can be represented as the rational functions in $(Z, Y) \in \tilde{U}^{(l)}$, we conclude taking into account the irreducibility of $U^{(l)}$ that $\gamma_0, \ldots, \gamma_{t-1}$ are constants on $\tilde{U}^{(l)}$. Thus, the exponent vectors I (see section 1) are the same for all the points $(Z, Y) \in \tilde{U}^{(l)}$.

So, for $(Z, Y) \in \tilde{U}^{(l)}$ one can write t-sparse representation of the polynomial

$$g = \sum_I C_I(Z, Y)(Z^{-1}(X - Y))^I \tag{1}$$

where the coefficients $C_I(Z, Y)$ depend on Z, Y. The equality (1) is equivalent to a system of equalities

$$g(ZX^{(0)} + Y) = \sum_I C_I(Z, Y)(Z^{-1}(X^{(0)} - Y))^I$$

where $X^{(0)}$ runs over all the vectors from $\{0, \ldots, d\}^n$. Adding to the latter system the system $\det Z \neq 0$, $h_1^{(l)} = \ldots = h_{N(l)}^{(l)} = 0$ determining $\tilde{U}^{(l)}$ we come to a parametrical (with the parameters $\{Z_{ij}, Y_i\}$) linear in C_I system which one can solve invoking the algorithm from [H 83] (see also [CG 84]) in time $M^{O(1)}d^{O(n^4)}$. This algorithm yields some disjoint decomposition of $\tilde{U}^{(l)} = \bigcup\limits_S U_S^{(l)}$ where each $U_S^{(l)}$ is a constructive set and also yields the rational functions $\bar{C}_{I,S}^{(l)}(\{Z_{ij}, Y_i\}) \in \mathbb{Q}(\{\mathbb{Z}_{\mathbb{ij}}, \mathbb{Y}_{\mathbb{i}}\})$ such that $C_I = \bar{C}_{I,S}^{(l)}(\{Z_{ij}, Y_i\})$ for every point $\{Z_{ij}, Y_i\} \in U_S^{(l)}$ (thus each C_I is a piecewise-rational function on $\tilde{U}^{(l)}$).

The algorithm yields also polynomials $h_{S,0}^{(l)}, \ldots, h_{S,N_S^{(l)}}^{(l)} \in \mathbb{Q}[\{\mathbb{Z}_{\mathbb{ij}}, \mathbb{Y}_{\mathbb{i}}\}]$ such that $U_S^{(l)} = \{h_{S,0}^{(l)} \neq 0,\ h_{S,1}^{(l)} = \ldots = h_{S,N_S^{(l)}}^{(l)} = 0\}$. From [H 83] (see also [CG 84]) we get the bounds on the degrees $\deg(h^{(l)}_{S,q}), \deg(\bar{C}^{(l)}_{I,S}) \leq d^{O(n^2)}$ and the bound $M^{O(1)}d^{O(n^2)}$ for the bit-size of every (rational) coefficients of all the yielded rational functions.

Thus, we have proved the following theorem (cf. proposition above).

Theorem. *There is an algorithm which finds a minimal t and produces a constructive set $U \subset \bar{\mathbb{Q}}^{n^2+n}$ of all $\{Z_{ij}, Y_i\}_{1\leq i,j \leq n}$ such that $g(ZX+Y)$ is t-sparse, in the form $U = \bigcup\limits_l \mathcal{U}^{(l)}$ and for each constructive set $\mathcal{U}^{(l)}$ the algorithm produces polynomials $\mathcal{H}^{(l)}_0, \ldots, \mathcal{H}^{(l)}_{\mathcal{N}^{(l)}} \in \mathbb{Q}[\{\mathbb{Z}_{\beth\gimel}, \mathbb{Y}_{\beth}\}]$ such that $\mathcal{U}^{(l)} = \{\mathcal{H}^{(l)}_0 \neq 0,\ \mathcal{H}^{(l)}_1 = \ldots = \mathcal{H}^{(l)}_{\mathcal{N}^{(l)}} = 0\}$. Also the algorithm produces t exponent vectors and for each exponent vector I a rational function $\mathcal{C}^{(l)}_I(\{Z_{ij}, Y_i\}) \in \mathbb{Q}(\{\mathbb{Z}_{\beth\gimel}, \mathbb{Y}_{\beth}\})$ which provide t-sparse representations of*

$$g = \sum_I \mathcal{C}^{(l)}_I(\{Z_{ij}, Y_i\})(Z^{-1}(X-Y))^I$$

which is valid for every point $(\{Z_{ij}, Y_i\}) \in \mathcal{U}^{(l)}$. The degrees of all produced rational functions $\mathcal{H}^{(l)}_S$, $\mathcal{C}^{(l)}_I$ do not exceed $d^{O(n^2)}$, the bit-size of the coefficients of these rational functions can be bounded by $(Md^{n^2})^{O(1)}$ and the running time of the algorithm is at most $(Md^{n^4})^{O(1)}$.

Again when Z_{ij}, Y_i belong to $\mathbb{R}$ we could write down a polynomial system on Z, Y with a less number of equations. For this purpose we need the following

Lemma 5. *If g is a shifted t-sparse polynomial, then for any Z_0, Y_0 such that* $\det Z_0 \neq 0$ *for at least one of $X^{(0)}_1 = 1, \ldots, n^{O(n)}2^{O(t^4)}$, a polynomial $\mathcal{W}_g(X^{(0)}_1, X_2, \ldots, X_n, Y_0, Z_0) \in \mathbb{R}[\mathbb{X}_{\nvDash}, \ldots, \mathbb{X}_{\ltimes}]$ does not vanish identically, provided that $\mathcal{W}_g(X, Y_0, Z_0) \in \mathbb{R}[\mathbb{X}]$ does not vanish identically.*

Proof. Let for some $Z^{(0)}, Y^{(0)}$ a polynomial $g(Z^{(0)}X + Y^{(0)})$ be t-sparse, i.e.

$$g = \sum_J \beta_J \prod_{1 \leq i \leq n} ((Z^{(0)})^{-1}(X - Y^{(0)}))^{j_i}_i$$

where $J = (j_1, \ldots, j_n)$ and the sum has at most t items (by $((Z^{(0)})^{-1}(X-Y^{(0)}))_i$ we denote i-th coordinate of the vector $(Z^{(0)})^{-1}(X - Y^{(0)})$). Then

$$(D^K_n g)(X, Y_0, Z_0) = \sum_J \beta_J \prod_{1\leq i \leq n} ((Z^{(0)})^{-1}((Z_0 P^K Z_0^{-1}(X-Y_0)+Y_0)-Y^{(0)}))^{j_i}_i \quad \text{for } 0 \leq K \leq 2t.$$

Thus $\mathcal{W}_g(X, Y_0, Z_0)$ is a polynomial in $(2t+1)t$ products of the form like in the latter expression and these products can be considered as the elements of a Pfaffian chain. [Kh 91] entails (cf. also [GKS 93]) that the sum of Betti numbers of the variety $\{\mathcal{W}_g(X, Y_0, Z_0) = 0\} \subset \mathbb{R}^{\ltimes}$ is less than $n^{O(n)}2^{O(t^4)}$. As in particular $(n-1)$-th Betti number $b^{n-1} < n^{O(n)}2^{O(t^4)}$ we conclude the statement of the lemma (cf. [GKS 93]).

Thus, Y, Z satisfy the conditions of lemma 4 if and only if $\det Z \neq 0$ and they satisfy the following $n^{O(n^2)}2^{O(nt^4)}$ equations.

$$\mathcal{W}_g(X_1^{(0)}, \ldots, X_n^{(0)}, Y, Z) = 0, \qquad X_1^{(o)}, \ldots, X_n^{(0)} \in \{1, \ldots, n^{O(n)}2^{O(t^4)}\}$$

4 Zero-test for shifted sparse polynomials

Let g be shifted t-sparse polynomial. Then (see lemma 5) for at least one of $X_1^{(0)} = 1, \ldots, n^{O(n)}2^{(t^2)}$ a polynomial $g(X_1^{(0)}, X_2, \ldots, X_n) \in \mathbb{Q}[\mathbb{X}_{\neq}, \ldots, \mathbb{X}_{\ltimes}]$ does not vanish identically. Thus for zero-test one can compute $g(X_1^{(0)}, \ldots, X_n^{(0)})$ for $n^{O(n^2)}2^{O(nt^2)}$ points $(X_1^{(0)}, \ldots, X_n^{(0)}) \in \{1, \ldots, n^{O(n)}2^{O(t^2)}\}^n$. Then g vanishes identically if and only if all the results of computation vanish. Thus, the complexity of zero-test does not depend on d.

Acknowledgement. The authors would like to thank C. Schnorr for initiating the question about the shifted sparse polynomials.

References

[BT 88] Ben-Or, M. & Tiwari, P., *A deterministic algorithm for sparse multivariate polynomial interpolation*, Proc. 20 STOC ACM, 1988, pp. 301-309.

[CG 83] Chistov, A. & Grigoriev, D., *Subexponential-time solving systems of algebraic equations*, Preprints LOMI E-9-83, E-10-83, Leningrad, 1983.

[CG 84] Chistov, A. & Grigoriev, D., *Complexity of quantifier elimination in the theory of algebraically closed fields*, Lect. Notes Comp. Sci. **176**, 1984, pp. 17-31.

[GK 87] Grigoriev, D. & Karpinski, M., *The matching problem for bipartite graphs with polynomially bounded permanents is in NC*, Proc. 28 FOCS IEEE, 1987, pp. 166-172.

[GKS 90] Grigoriev, D., Karpinski, M. & Singer, M., *Fast parallel algorithms for sparse multivariate polynimial interpolation over finite fields*, SIAM J. Comput. **19**, N 6, 1990, pp. 1059-1063.

[GKS 91] Grigoriev, D., Karpinski, M. & Singer, M., *The interpolation problem for k-sparse sums of eigenfunctions of operators*, Adv. Appl. Math. **12**, 1991, pp. 76-81.

[GKS 92] Grigoriev, D., Karpinski, M. & Singer, M., *Computational complexity of sparse rational interpolation* , to appear in SIAM J. Comput.

[GKS 93] Grigoriev, D., Karpinski, M. & Singer, M., *Computational complexity of sparse real algebraic function interpolation*, to appear in Proc. Int. Conf. Eff. Meth. Alg. Geom., Nice, April 1992 (Progr. in Math. Birkhäuser).

[H 83] Heintz, J., *Definability and fast quantifier elimination in algebraically closed fields*, Theor. Comp. Sci. **24**, 1983, pp. 239-278.

[Ka 89] Karpinski, M., *Boolean Circuit Complexity of Algebraic Interpolation Problems*, Technical Report TR-89-027, International Computer Science Institute, Berkeley, 1989; in Proc. CSL'88, Lecture Notes in Computer Science **385**, 1989, pp. 138-147.

[Kh 91] Khovanski, A., *Fewnomials*, Transl. Math. Monogr., AMS 88, 1991.

[KY 88] Kaltofen, E. & Yagati, L., *Improved sparse multivariate interpolation*, Report 88-17, Dept. Comput. Sci., Rensselaer Polytechnic Institute, 1988.