ADVANCES IN APPLIED MATHEMATICS 12, 76–81 (1991)

# The Interpolation Problem for $k$-Sparse Sums of Eigenfunctions of Operators

DIMA YU. GRIGORIEV

*Leningrad Department of the V. A. Steklov Mathematical Institute of the Academy of Sciences of the USSR, Fontanka 27, Leningrad 191011, USSR*

MAREK KARPINSKI*

*Department of Computer Science, University of Bonn, 5300 Bonn 1, Federal Republic of Germany*

AND

MICHAEL F. SINGER†

*Department of Mathematics, Box 8205, North Carolina State University, Raleigh, North Carolina 27695*

In [DG 89], the authors show that many results concerning the problem of efficient interpolation of $k$-sparse multivariate polynomials can be formulated and proved in the general setting of $k$-sparse sums of characters of abelian monoids. In this note we describe another conceptual framework for the interpolation problem. In this framework, we consider $R$-algebras of functions $\mathscr{A}_1, \dots, \mathscr{A}_n$ on an integral domain $R$, together with $R$-linear operators $\mathscr{D}_i$: $\mathscr{A}_i \to \mathscr{A}_i$. We then consider functions $f$ from $R^n$ to $R$ that can be expressed as the sum of $k$ terms, each term being an $R$-multiple of an $n$-fold product $f_1(x_1) \cdot \cdots \cdot f_n(x_n)$, where each $f_i$ is an eigenfunction for $\mathscr{D}_i$. We show how these functions can be thought of as $k$-sums of characters on an associated abelian monoid. This allows one to use the results of [DG 89] to solve interpolation problems for $k$-sparse sums of functions which, at first glance, do not seem to be characters.

Let $R$, $\mathscr{A}_1, \dots, \mathscr{A}_n$, and $\mathscr{D}_1, \dots, \mathscr{D}_n$ be as above. For each $\lambda \in R$ and $1 \le i \le n$, define the $\lambda$-eigenspace $\mathscr{A}_i^\lambda$ of $\mathscr{D}_i$ by

$$\mathscr{A}_i^\lambda = \{f \in \mathscr{A}_i | \mathscr{D}_i f = \lambda f\}.$$

*Supported in part by Leibniz Center for Research in Computer Science, by the DFG Grant KA 673/2-1, and by the SERC Grant GR-E 68297.
†Supported in part by NSF Grant DMS-8803109.



0196-8858/91 $7.50

For every $1 \le i \le n$ we fix some subset $S_i \subset R$. Furthermore, we suppose that

(a) for each $i$, $1 \le i \le n$, and each $\lambda \in S_i$, we are given an eigenfunction $0 \ne f_i^\lambda \in \mathscr{A}_i^\lambda$ such that $\mathscr{A}_i^\lambda = Rf_i^\lambda$, and,

(b) a point $a_0 \in R$ is given such that for each $i$, $1 \le i \le n$, and each $\lambda \in S_i$, we have $f_i^\lambda(a_0) \ne 0$.

Let $X_1, \dots, X_n$ be variables and let $\mathscr{A}$ be the $R$-algebra of functions from $R^n$ to $R$ generated by products of the form $g_1(X_1) \cdot \cdots \cdot g_n(X_n)$, where $g_i \in \mathscr{A}_i$, $1 \le i \le n$. We can extend the operators $\mathscr{D}_i$ to operators on $\mathscr{A}$ (which we denote again by $\mathscr{D}_i$) by setting

$$\begin{aligned}\mathscr{D}_i(&g_1(X_1) \cdot \cdots \cdot g_n(X_n)) \\ &= g_1(X_1) \cdot \cdots \cdot g_{i-1}(X_{i-1})(\mathscr{D}_i g_i)(X_i) g_{i+1}(X_{i+1}) \cdot \cdots \cdot g_n(X_n).\end{aligned}$$

For all integer $k \ge 1$, we say that a function $f \in \mathscr{A}$ is $k$-sparse (with respect to $\mathscr{D}_1, \dots, \mathscr{D}_n$ and $S_1, \dots, S_n$) if $f = \sum_{1 \le j \le k} c_j f_j$, where $c_j \in R$ and each $f_j = \prod_{1 \le i \le n} f_i^{\lambda^{i,j}}(X_i)$ for some $\lambda^{i,j} \in S_i$. Consider the following examples:

EXAMPLE 1. Let $R = \mathbb{Z}$, the integers, and, for each $i$, $1 \le i \le n$, let $\mathscr{A}_i \subset \mathbb{Q}[X]$ consists of all polynomials with rational coefficients that map the integers to the integers. For $1 \le i \le n$, set $\mathscr{D}_i = X\Delta$, where $(\Delta f) = f(X) - f(X-1)$ and let $S_i = \mathbb{Z}_{\ge 0}$, the non-negative integers. For each $\lambda \in S_i$ we can take $f_i^\lambda = \binom{X}{\lambda} = (X(X-1) \cdot \cdots \cdot (X - \lambda + 1))/\lambda!$. Note that $f_i^0 = 1$. Finally, let $a_0 = -1$. In this case

$$\mathscr{A} = \left\{ f \,|\, f = \sum_{\Lambda} c_\Lambda \binom{X_1}{\lambda_1} \cdot \cdots \cdot \binom{X_n}{\lambda_n} \right\},$$

where this sum is over a finite set of $\Lambda = (\lambda_1, \dots, \lambda_n)$, $\lambda_i \in S_i$, and $c_\Lambda \in \mathbb{Z}$. One can show that $\mathscr{A}$ coincides with the subring of $\mathbb{Q}[X_1, \dots, X_n]$ consisting of all polynomials mapping $\mathbb{Z}^n \to \mathbb{Z}$ (for $n = 1$, this can be found in [S 65]; one can prove the result for $n > 1$ using the ideas in [S 65] and double induction, first on $n$ and then on the degree of a polynomial in $X_n$).

EXAMPLE 2. Let $R$ be an integral domain with $\mathbb{Z} \subset R$ and for each $i$, let $\mathscr{A}_i = R[X]$. Let $p_1, \dots, p_n$ be pairwise distinct primes, let $(\mathscr{D}_i f)(X) = f(p_i X)$ for $f \in \mathscr{A}_i$ and let $a_0 = 1$. For each $i$, $1 \le i \le n$, let $S_i = \{p_i^j \,|\, j \in \mathbb{Z}_{\ge 0}\}$ and let $f_i^{p_i^j} = X^j$. In this case $\mathscr{A} = R[X_1, \dots, X_n]$ and $k$-sparse functions correspond to $k$-sparse polynomials.

EXAMPLE 3. Let $R = \mathbb{C}$, the complex numbers and let $\mathscr{A}_i = R[e^X, e^{-X}]$ for each $i$, $1 \le i \le n$. For each $i$, $1 \le i \le n$, set $\mathscr{D}_i = d/dX$ and let $S_i = \mathbb{Z}$. For each $0 \ne \lambda \in S_i$, we can take $f_i^\lambda = e^{\lambda X}$ and let $a_0 = 0$. In this case

$$\mathscr{A} = \left\{ f \mid f = \sum_\Lambda c_\Lambda e^{\lambda_1 X_1 + \cdots + \lambda_n X_n} \right\},$$

where this sum is over a finite set of $\Lambda$ in $\mathbb{Z}^n$ and $c_\Lambda \in \mathbb{Z}$; that is, $\mathscr{A}$ is the set of finite fourier series. A similar example can be constructed over $\mathbb{R}$, the real numbers.

EXAMPLE 4. One can combine Examples 2 and 3. Let $n = 2$. Let $\mathscr{A}_1 = R[X]$ with $\mathscr{D}_1 = p_1 X$ as in Example 2 and let $\mathscr{A}_2 = R[e^X, e^{-X}]$ with $\mathscr{D}_2 = d/dX$. Let $S_1 = \{p_1^j \mid j \in \mathbb{Z}_{\ge 0}\}$, $f_1^{p_1^j} = X^j$, and $S_2 = \mathbb{Z}$, $f_2^\lambda = e^{\lambda X}$. In this case,

$$\mathscr{A} = \left\{ f \mid f = \sum c_{i,j} X_1^i e^{j X_2} \right\},$$

where the sum is over a finite subset of $\mathbb{Z}_{\ge 0} \times \mathbb{Z}$.

EXAMPLE 5. Let $A$ be an infinite cyclic monoid generated by $a$ and let $K$ be a field. Let $R = K[A] = \{r \mid r = \sum_{i \ge 0} c_i a^i\}$, where the sum is finite and $c_i \in K$. With the obvious addition and multiplication, $R$ is an integral domain. If $\chi$ is a character on $A$, then $\chi$ defines a function on $R$ satisfying $\chi(\sum c_i a^i) = \sum c_i \chi(a^i)$. Let $n = 1$ and let $\mathscr{A}_1 = \{f \mid f = \sum d_j \chi_j$ where $\chi_j$ is a character of $A$ and $d_j \in K\}$. For $f = \sum d_j \chi_j \in \mathscr{A}$, and $r \in R$, we let $f(r) = \sum d_j \chi_j(r)$. In this way $\mathscr{A}$ is an $R$-algebra of functions on $R$. Let $(\mathscr{D}_1 f)(\chi) = f(a\chi)$ and $S_1 = K - \{0\}$. For each $\lambda \in S_1$ we may take $f_1^\lambda$ to be the character defined by $f_1^\lambda(a) = \lambda$. Finally, we let $a_0 = a^0$. In this case $\mathscr{A} = \mathscr{A}_1$, and $k$-sparse functions correspond to $k$-sums of characters (cf. [DG 89, Introduction]).

We now return to the general situation. We are interested in computational questions involving $k$-sparse functions in $\mathscr{A}$. We assume that a function $f \in \mathscr{A}$ is given by a black box that allows us to calculate $f(a_0, \ldots, a_0)$ and $(\mathscr{D}_i^j f)(a_0, \ldots, a_0)$ for $1 \le i \le n$ and all $j \ge 1$ ($\mathscr{D}_i^j f = \mathscr{D}_i(\mathscr{D}_i(\cdots(\mathscr{D}_i f)\cdots)$, where $\mathscr{D}_i$ is iterated $j$ times). In Example 1, this is equivalent to being able to calculate $f(-m_1, \ldots, -m_n)$ for all $m_i \in \mathbb{Z}_{>0}$. In Example 2, this means we can calculate $f(p_1^{m_1}, \ldots, p_n^{m_n})$ for all $m_i \in \mathbb{Z}_{>0}$. In these two examples our assumption would be satisfied if we had black boxes to calculate the values of $f$ in $\mathbb{Z}^n$. In Example 3, our assumption implies that we can calculate $(\partial^{m_1 + \cdots + m_n} f / \partial X_1^{m_1} \cdots \partial X_n^{m_n})(0)$ for all $m_i \in \mathbb{Z}_{>0}$. In general we shall show that the techniques of [DG 89] can be used to decide, given a black box (as above) for a $k$-sparse function

$f \in \mathscr{A}$, if $f$ is identically zero and to interpolate this function, i.e., to find the $\lambda_{i,j}$ and $c_j$. To do this we must interpret $f$ as a $k$-sparse sum of monomial characters on a monoid.

Let $A$ be the subalgebra of the algebra of $R$-endomorphisms of $\mathscr{A}$, $\mathrm{END}_R(\mathscr{A})$, generated over $R$ by $\mathscr{D}_1, \ldots \mathscr{D}_n$. We consider $A$ as a multiplicative monoid. Let $F$ be the quotient field of $R$. Each element $f \in \mathscr{A}$ yields a function $\tilde{f}$ on $A$ defined by

$$\tilde{f}\left(\sum r_J \mathscr{D}_1^{j_1}, \ldots, \mathscr{D}_n^{j_n}\right) = \sum r_J\left(\mathscr{D}_1^{j_1}, \ldots, \mathscr{D}_n^{j_n} f\right)(a_0).$$

Note that $\tilde{f}_i^\lambda(\mathscr{D}_i) = (\mathscr{D}_i f_i^\lambda)(a_0) = \lambda f_i^\lambda(a_0)$ and $\tilde{f}_i^\lambda(\mathscr{D}_j) = 0$ if $i \neq j$. If $f \in \mathscr{A}$ satisfies $f(a_0) \neq 0$, we define

$$\hat{f} = \frac{1}{f(a_0)} \tilde{f}.$$

If $f = f_i^\lambda$, then one sees that $\hat{f}_i^\lambda(\mathscr{D}_i) = \lambda$, $\hat{f}_i^\lambda(\mathscr{D}_j) = 0$ if $i \neq j$, and $\hat{f}_i^\lambda(1) = 1$, so $\hat{f}_i^\lambda$ is an $F$-valued character of $A$. Note that distinct values of $\lambda$ yield distinct characters.

A $k$-sparse

$$f = \sum_{1 \leq j \leq k} c_j \prod_{1 \leq i \leq n} f_i^{\lambda_{i,j}}$$

on $\mathscr{A}$ corresponds to a $k$-sparse sum of monomial characters

$$\tilde{f} = \sum_{1 \leq j \leq k} c_j \left( \prod_{1 \leq i \leq n} f_i^{\lambda_{i,j}}(a_0) \right) \prod_{1 \leq i \leq n} \hat{f}_i^{\lambda_{i,j}}$$

on $A$. Therefore deciding if $f$ is identically zero and interpolating are equivalent to the same problems for $\tilde{f}$. Note that if $f$ and $g$ both belong to $\mathscr{A}_i^\lambda$, then $\hat{f} = \hat{g}$. Because of this, we have restricted $\mathscr{A}_i^\lambda$ (in condition (a) above) to be a cyclic $R$-module. Without this restriction we could not recover a $k$-sparse representation of $f$ from $\tilde{f}$.

In Example 2, the submonoid $U$ of $A$ generated by $\mathscr{D}_1, \ldots \mathscr{D}_n$ is abelian of rank $n$, so the comments in the second paragraph of Section 2 of [DG 89] apply and we can conclude that we can reduce to a cyclic monoid. In general, we cannot guarantee the existence of such a submonoid of $A$ but we can guarantee the existence of $k$-distinction sets for the set of monomial characters, if the ring $R$ is infinite or contains $\mathrm{GF}(p^{\lceil \log_p(s^2 n/2) \rceil})$ if $R$ is finite of characteristic $p \neq 0$ (cf. [GKS 89; DG 89]).

LEMMA. *For any $k, n$, one can construct vectors $\Omega_1, \ldots, \Omega_{t_0}$, in $R^n$ with $t_0 = \lceil k^2n/2 \rceil$, such that for any vectors $\Lambda_1, \ldots, \Lambda_k \in R^n$ there exists a $j$, $1 \le j \le t_0$, for which $\Lambda_l \cdot \Omega_j \ne \Lambda_r \cdot \Omega_j$ for all $1 \le l < r \le k$. Furthermore, if* $\mathrm{char}(R) = 0$ *then the entries of $\Omega_1, \ldots, \Omega_{t_0}$ can be natural numbers less than $k^2n$. If* $\mathrm{char}(R) = p$ *and* $\mathrm{GF}(p^{\lceil \log_p(k^2n/2) \rceil}) \subset R$ *then the entries of $\Omega_1, \ldots, \Omega_{t_0}$ can be chosen from* $\mathrm{GF}(p^{\lceil \log_p(k^2n/2) \rceil})$.

*Proof.* Consider first the case $\mathrm{char}(R) = 0$. Let $q$ be a prime number with $\lceil k^2n/2 \rceil \le q \le k^2n$ (which exists by Bertrand's postulate) and define an integer matrix

$$\Omega = (\omega_{ij})_{1 \le i \le n,\, 1 \le j \le t_0},$$

where $0 \le \omega_{ij} \le q$ and such that $\omega_{ij} \equiv j^i \pmod{q}$. Note that each $n \times n$ submatrix of $\Omega$ is nonsingular because such a matrix is a Vandermonde matrix mod $q$. As $\Omega_1, \ldots, \Omega_{t_0}$ we can take the elements of $\Omega$. For each pair $1 \le l < r \le s$, there exist at most $(n-1)$ vectors among $\Omega_1, \ldots, \Omega_{t_0}$ which are orthogonal to $(\Lambda_l - \Lambda_r)$. Therefore, among $\Omega_1, \ldots, \Omega_{t_0}$ one can find a vector not orthogonal to all the differences $\Lambda_l - \Lambda_r$ (cf. Lemma 2.3 [DG 89]).

If $\mathrm{char}(R) = p$, the proof is similar using the matrix

$$(\alpha_j^i)_{1 \le i \le n,\, 1 \le j \le t_0},$$

where $\alpha_j \in R$ are pairwise distinct. If $\mathrm{GF}(p^{\lceil \log_p(k^2n/2) \rceil}) \subset R$ we can chose $\alpha_j$ from the latter field. $\square$

From this lemma, we see that the elements $D_1, \ldots, D_{t_0}$, where

$$D_i = \sum_{j=1}^{n} \omega_{ij} \mathscr{D}_j,$$

form a $k$-distinction set. Therefore one can use the techniques of Section 1 of [DG 89] to develop zero testing and interpolation algorithms in our setting. Conversely, Example 5 shows that results developed in this setting can be transferred to results about characters on infinite cycle monoids. For example, in Example 3, the matrix $M_k$ of Theorem 1 of [DG 89] arises naturally as a Wronskian matrix associated with solutions of a linear differential equation. This observation perhaps explains the somewhat mysterious appearance of ideas from BCH codes in this subject.

## REFERENCES

[DG 89] A. DRESS AND J. GRABMEIER, The interpolation problem for $k$-sparse polynomials and character sums, *Adv. Appl. Math.*, **12** (1991), 57–75.

[GKS 88] D. YU. GRIGORIEV, M. KARPINSKI AND M. SINGER, "Fast Parallel Algorithms for Sparse Multivariate Polynomial Interpolation over Finite Fields," University of Bonn, Research Report No. 8523-CS, 1988.

[S 65] J. P. SERRE, "Algèbre Local-Multiplicités, Lecture Notes in Mathematics, Vol. 11, Springer-Verlag, New York, 1965.