THE INTERPOLATION PROBLEM FOR k-SPARSE SUMS OF EIGENFUNCTIONS OF OPERATORS

DIMA YU. GRIGORIEV
STEKLOV INSTITUTE OF MATHEMATICS
SOV. ACAD. OF SCIENCES
LENINGRAD 191011

MAREK KARPINSKI *
DEPT. OF COMPUTER SCIENCE
UNIVERSITY OF BONN
5300 BONN 1

MICHAEL F. SINGER †
DEPT. OF MATHEMATICS
N.C. STATE UNIVERSITY
RALEIGH, NC 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 $\mathcal{A}_1, \ldots, \mathcal{A}_n$ on an integral domain R, together with R-linear operators $\mathcal{D}_i : \mathcal{A}_i \to \mathcal{A}_i$. 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 $f_1(x_1) \cdot \ldots \cdot f_n(x_n)$ where each f_i is an eigenfunction for $\mathcal{D}_i$. 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 $R, \mathcal{A}_1, \ldots, \mathcal{A}_n$, and $\mathcal{D}_1, \ldots, \mathcal{D}_n$ be as above. For each $\lambda \in R$ and $1 \le i \le n$, define the λ-eigenspace $\mathcal{A}_i^\lambda$ of $\mathcal{D}_i$ by

$$\mathcal{A}_i^\lambda = \{f \in \mathcal{A}_i \mid \mathcal{D}_i f = \lambda f\}.$$

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 $0 \ne f_i^\lambda \in \mathcal{A}_i^\lambda$ such that $\mathcal{A}_i^\lambda = R f_i^\lambda$, and,

*Supported in part by Leibnis 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.

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 $f_i^\lambda(a_0) \neq 0$.

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

$$\mathcal{D}_i(g_1(X_1) \cdot \ldots \cdot g_n(X_n)) = g_1(X_1) \cdot \ldots \cdot g_{i-1}(X_{i-1})(\mathcal{D}_i g_i)(X_i) g_{i+1}(X_{i+1}) \cdot \ldots \cdot g_n(X_n).$$

For an integer $k \ge 1$, we say that a function $f \in \mathcal{A}$ is k-sparse (with respect to $\mathcal{D}_1, \ldots, \mathcal{D}_n$ and $S_1, \ldots, S_n$) 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 $\mathcal{A}_i \subset \mathbf{Q}[X]$ consists of all polynomials with rational coefficients that map the integers to the integers. For $1 \le i \le n$, set $\mathcal{D}_i = X\triangle$ where $(\triangle f) = f(X) - f(X-1)$ and let $S_i = \mathbb{Z}_{\ge 0}$, the non-negative integers. For each $0 \neq \lambda \in S_i$ we can take $f_i^\lambda = \binom{X}{\lambda} = \frac{X(X-1)\ldots(X-\lambda+1)}{\lambda!}$ and also $f_i^0 = 1$. In this case

$$\mathcal{A} = \{f \mid f = c_0 + \sum_{\Lambda} c_\Lambda \binom{X_1}{\lambda_1} \cdot \ldots \cdot \binom{X_n}{\lambda_n}\}$$

where this sum is over a finite set of $\Lambda = (\lambda_1, \ldots, \lambda_n)$ and $c_\Lambda \in \mathbb{Z}$. One can show that $\mathcal{A}$ coincides with the subring of $\mathbf{Q}[X_1, \ldots, X_n]$ 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). $\square$

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

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

$$\mathcal{A} = \{f \mid f = \sum_{\Lambda} c_\Lambda e^{\lambda_1 X_1 + \ldots + \lambda_n X_n}\}$$

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

Example 4. One can combine examples 2 and 3. Let $n = 2$. Let $\mathcal{A}_1 = R[X]$ with $\mathcal{D}_1 = p_1 X$ as in example 2 and let $\mathcal{A}_2 = R[e^X, e^{-X}]$ with $\mathcal{D}_2 = \frac{d}{dX}$. 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,

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

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

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 this sum is finite and $c_i \in K$. With the obvious addition and multiplication, R is an integral domain. If χ is a character on A, then χ defines a function on R satisfying $\chi(\sum c_i a^i) = \sum c_i \chi(a^i)$. Let $n = 1$ and let $\mathcal{A}_1 = \{f \mid f = \sum d_j \chi_j$ where χ_j is a character of A and $d_j \in K\}$. For $f = \sum d_j \chi_j \in \mathcal{A}$, and $r \in R$, we let $f(r) = \sum d_j \chi_j(r)$. In this way $\mathcal{A}$ is an R-algebra of functions on R. Let $(\mathcal{D}_1 f)(\chi) = f(a\chi)$ and $S_1 = K - \{0\}$. For each $\lambda \in S_1$ we may take f_1^λ to be the character defined by $f_1^\lambda(a) = \lambda$. Finally, we let $a_0 = a^0$. In this case $\mathcal{A} = \mathcal{A}_1$, 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 $\mathcal{A}$. We assume that a function $f \in \mathcal{A}$ is given by a black box that allows to calculate $f(a_0)$ and $(\mathcal{D}_i^j f)(a_0)$ for $1 \leq i \leq n$ and all $j \geq 1$ ($\mathcal{D}_i^j f = \mathcal{D}(\mathcal{D}(\ldots(\mathcal{D}f)\ldots)$ where $\mathcal{D}$ is iterated j times). In example 1, this means that we can 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 $(\frac{\partial^{m_1+\cdots+m_n}}{\partial X_1^{m_1}\ldots\partial X_n^{m_n}} f)(0)$ 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 $f \in \mathcal{A}$, 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 $\mathrm{HOM}_R(\mathcal{A}, \mathcal{A})$ generated over R by $\mathcal{D}_1, \ldots \mathcal{D}_n$. We consider A as a multiplicative monoid. Let F be the quotient field of R. Each element $f \in \mathcal{A}$ yields a function $\hat{f}$ on A defined by

$$\hat{f}(\sum r_J \mathcal{D}_1^{j_1}, \ldots \mathcal{D}_n^{j_n}) = \sum r_J \mathcal{D}_1^{j_1}, \ldots \mathcal{D}_n^{j_n} f)(a_0).$$

For each i, $1 \leq i \leq n$ and each $\lambda \in S_i$ we define an F valued character $\hat{f}_i^\lambda$ on A by

$$\hat{f}_i^\lambda = \frac{1}{f_i^\lambda(a_0)} \hat{f}_i^\lambda.$$

A k-sparse

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

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

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

on A. Therefore deciding if f is identically zero and interpolating are equivalent to the same problems for $\hat{f}$.

In example 2, the submonoid U of A generated by $\mathcal{D}_1, \ldots \mathcal{D}_n$ 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 $\mathrm{GF}(p^{\lceil \log_p(\frac{k^2 n}{2})\rceil})$ if R is finite of characteristic $p \neq 0$ (c.f. [GKS 88], [DG 89]).

Lemma For any k, n, one can construct vectors $\Omega_1, \ldots, \Omega_{t_0}$, in R^n with $t_0 = \lceil \frac{k^2 n}{2} \rceil$, such that for any vectors $\Lambda_1, \ldots, \Lambda_k \in R^n$ there exists a j, $1 \leq j \leq t_0$ for which $\Lambda_l \cdot \Omega_j \neq \Lambda_r \cdot \Omega_j$ for all $1 \leq l < r \leq k$. 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 $\mathrm{GF}(p^{\lceil \log_p(\frac{k^2n}{2})\rceil}) \subset R$ then the entries of $\Omega_1, \ldots, \Omega_{t_0}$ can be chosen from $\mathrm{GF}(p^{\lceil \log_p(\frac{k^2n}{2})\rceil})$.

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

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

where $0 \leq \omega_{ij} \leq q$ and such that $\omega_{ij} \equiv j^i (\mathrm{mod}\ q)$. Note that each $n \times n$ submatrix of Ω 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 Ω. For each pair $1 \leq l < r \leq s$, 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 $\Lambda_l - \Lambda_r$ (c.f. Lemma 2.3 [DG 89]).

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

$$(\alpha_j^i)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq t_0}}$$

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

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

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

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 transfered to results about characters on infinite cyclic 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] Dress, A., Grabmeier, J., *The Interpolation Problem for k-sparse Polynomials and Character Sums*, Advances in Applied Mathematics, to appear.

[GKS 88] Grigoriev, D.Yu., Karpinski, M., Singer, M., *Fast Parallel Algorithms for Sparse Multivariate Polynomial Interpolation over Finite Fields*, University of Bonn, Research Report No. 8523-CS, 1988.

[S 65] Serre, J.P., *Algèbre Local-Multiplicités*, Lecure Notes in Mathematics Vol. 11, Springer Verlag, New York, 1965.