Publ. I.R.M.A. Strasbourg, 1990, 413/S–21
Actes 21^e Séminaire Lotharingien, p. 14–18

On zero-testing and interpolation of sums of characters

Andreas Dress [*]
Fakultät für Mathematik
Universität Bielefeld

Johannes Grabmeier
IBM Deutschland GmbH
Wissenschaftliches Zentrum Heidelberg

We study the problem of zero-testing and interpolation of sums of characters. This generalizes and unifies the previous work of [GK87], [BT88], [CDGK88] and [GKS88], where the question of zero-testing and interpolation of k-sparse multivariate polynomials over fields of characteristic 0 and over finite fields were studied. Proofs, more details and further results can be found in [DG89].

Let A be an abelian monoid with neutral element 1_A and let K be a field. According to the well known Artin-Dedekind Lemma the set $Hom(A,(K,*))$ of all *characters*, i.e. monoid homomorphisms with $1_A \mapsto 1_K$ from A into the multiplicative monoid $(K,*)$ of K is a linearly independent subset of the K-space of all maps from A into K. For any subset $X \subseteq Hom(A,(K,*))$ of characters and every positive integer k define the set X_k of *k-sums* of characters from X by

$$X_k := \{f : A \to K \mid \exists\, f_1,\ldots,f_k \in K, \chi_1,\ldots,\chi_k \in X,\ f = \sum_{\kappa=1}^{k} f_\kappa \chi_\kappa\}.$$

We assume $\#X \geq k$ and $\chi_\kappa \neq \chi_\sigma$ for $\kappa \neq \sigma$ in $f = \sum_{\kappa=1}^{k} f_\kappa \chi_\kappa$.

[*] Part of this work was prepared during a visit at the Scientific Center Heidelberg, IBM Germany, which is gratefully acknowledged.

For given X and k we are interested in procedures by which for any such $f = \sum_\chi f_\chi \chi$ in X_k its support

$$supp(f) := \{\chi \in X \mid f_\chi \neq 0\}$$

and its coefficients f_χ can be determined from as few as possible evaluations of f. A first step to solve this *interpolation problem* is, of course, the study of (small) subsets T of A which allow to distinguish any non-trivial k-sum of characters from X from the zero map. We will refer to such subsets as *zero-test sets* for X_k. Any zero-test set for X_{2k} distinguishes two different k-sums of characters. However, if an algorithm to carry out this task, is required to be efficient in some sense, the evaluations of f at the elements of such a set may not be sufficient.

The case of A being a cyclic monoid, generated by some $a \in A$, and $X = Hom(A, (K, *))$ is solved by the following two results:

Lemma *Let A be a cyclic monoid generated by an element $a \in A$. Then for $X = Hom(A, (K, *))$ and each natural number k the set*

$$\{1, a, a^2, \dots, a^{k-1}\}$$

is a minimal zero-test set for X_k.

Theorem *Let A be a cyclic monoid generated by an element $a \in A$ and let f be a sum of atmost k characters from $X = Hom(A, (K, *))$. Then the following holds:*

i) The rank of the matrix $M_k := (f(a^{i+j}))_{0 \leq i,j < k}$ coincides with the cardinality of $supp(f)$.

ii) If $\tilde{k} := \#supp(f)$ $(\leq k)$ and if

$$\begin{pmatrix} e_{\tilde{k}} \\ e_{\tilde{k}-1} \\ \vdots \\ e_1 \end{pmatrix} := M_{\tilde{k}}^{-1} \cdot \begin{pmatrix} -f(a^{\tilde{k}}) \\ -f(a^{\tilde{k}+1}) \\ \vdots \\ -f(a^{2\tilde{k}-1}) \end{pmatrix}$$

then the equation

$$X^{\tilde{k}} + e_1 X^{\tilde{k}-1} + \dots + e_{\tilde{k}-1} X + e_{\tilde{k}} = 0$$

has $\tilde{k}$ different solutions $c_1, \ldots, c_{\tilde{k}}$ in K and one has

$$supp(f) = \{\chi_{c_\kappa} \mid 1 \leq \kappa \leq \tilde{k}\}.$$

If there exists an element a in an arbitrary abelian monoid A which distinguishes all characters in X, i.e. $\chi(a) \neq \xi(a)$ for $\chi \neq \xi$, then the results for cyclic monoids can be applied. Important examples are the following ones:

Let A equal U^n for some submonoid U of the monoid $(K, *)$ and X is the subset of all maps

$$\chi^\alpha = \chi^{(\alpha_1, \cdots, \alpha_n)} : U^n \to K$$

where

$$\chi^\alpha((x_1, \ldots, x_n)) := x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$$

for $\alpha_1, ..., \alpha_n \in \mathbb{N}_0 := \{0, 1, ...\}$ and $x_1, ..., x_n \in U$.

In case U is infinite the characters from $X := \{\chi^\alpha, \ \alpha \in \mathbb{N}_0^n\}$ correspond to the monomials in n indeterminates and k-sum characters correspond to k-sparse polynomials.

Now let K be a field of characteristic 0 and let $\{p_1, p_2, \ldots, p_n\}$ be a set of n different primes, then any two different monomial characters necessarily differ on $a := (p_1, \ldots, p_n)$. This implies in particular many of the results presented in [GK87] and [BT88].

Similarly, if $U \leq (K, *)$ contains at least one element, say u, of infinite order or of order at least q^n (or $q^n - 1$) for some $q \in \mathbb{N}$ then all monomial characters in $X := X(q, n) = \{\chi^\alpha \mid \alpha \in \mathbf{q}^n\}$ (or in $X := \{\chi^\alpha \mid \alpha \in \mathbf{q}^n \setminus \{(0, 0, ..., 0)\}\}$ respectively) differ on $a := (u, u^q, \ldots, u^{q^{n-1}})$ in view of the uniqueness of q-adic expansion, and this is used in [CDGK88].

To apply the results for cyclic monoids even in cases where no distinguishing element is at hand or does not exist the methods of the paper [GKS88] allow to construct a set which possesses a distinguishing element for each k-subset of characters from X. Therefore a class of cyclic submonoids is used. The key to their result is to use an identity of Cauchy to construct an integral matrix with bounded entries and the property that no square submatrix is singular. In our more general setting the result is as follows:

Theorem *If U is a finite (and therefore cyclic!) subgroup of order e of the multiplicative group of a field K, if $A = U^n$ is the n-fold direct product of U, then for every positive integers k and q satisfying*

$$n \cdot (q-1) \cdot (n + (n-1) \cdot \binom{k}{2}) < e$$

there exists a zero-test set of order at most $(n-1) \cdot k \cdot \binom{k}{2} + k$ for the sums of characters from $X(q,n)_k = \{\chi^\alpha \mid \alpha \in \mathbf{q}^\mathbf{n}\}_k$.

If no reduction to cyclic monoids is possible, all we can do is provide a method for a recursive construction of zero-test sets for direct products of abelian monoids from those of the factors.

Lemma [cf. [CDGK88]] *If A and B are abelian monoids, if for given $X \subseteq Hom(A,(K,*))$ and $Y \subseteq Hom(B,(K,*))$ we have zero-test sets $A_1 = \{1_A\}, A_2, \ldots, A_k \subseteq A$ and $B_1 = \{1_B\}, B_2, \ldots, B_k \subseteq B$ for $X_1, X_2, \ldots, X_k$ and $Y_1, Y_2, \ldots, Y_k$, respectively, then — identifying $Hom(A \times B,(K,*))$ with $Hom(A,(K,*)) \times Hom(B,(K,*))$, as usual — the set*

$$\bigcup_{i \cdot j \leq k} A_i \times B_j \subseteq A \times B$$

is a zero-test set for $(X \times Y)_k$. This lemma generalizes immediately to the situation of more than two factors.

In case $U = \{0,1\} \leq K$ we can use this lemma to obtain the zero-test set

$$\{a^S \in U^n \mid S \subseteq \{1,...,n\},\ \#S \leq \log_2 k,\ a^S_\nu = \begin{cases} 0, & \text{if } \nu \in S; \\ 1, & \text{if } \nu \notin S. \end{cases}\}$$

for X_k and it has cardinality $\sum_{i=0}^{\lfloor \log_2 k \rfloor} \binom{n}{i}$. Furthermore, it can be shown that this zero-test is minimal.

Finally we state a theorem from which an interpolation algorithm for the case of direct products can be derived:

Theorem *Assume that for some field K, some monoid U, some finite set $X \subseteq Hom(A,(K,*))$ of characters, and some subset $D \subseteq A$ with $q := \#D = \#X$ the matrix $(\chi(d))_{d \in D, \chi \in X}$ is invertible. If furthermore for any*

$k, n \in \mathbb{N}$ a zero-test set $T_{n,k} \subseteq A^n$ for $(X^n)_k$, the k-sums of products of characters, is specified, then any k-sum of characters from $(X^n)_k$ of A^n can be reconstructed by an efficient algorithm only using matrix operations from at most $n \cdot (k^2 + q) \cdot \#T_{n-1,k}$ evaluations of f.

References

[BT88] Ben-Or, M., Tiwari, P. A Deterministic Algorithm for Sparse Multivariate Polynomial Interpolation, Proc. STOC ACM, (1988).

[CDGK88] Clausen, M., Dress, A., Grabmeier, J., Karpinski, M. On zero-testing and interpolation of k-sparse multivariate polynomials over finite fields, Theor. Comp. Sc., to appear, 1989.

[DG89] Dress, A., Grabmeier, J. The Interpolation Problem For k-sparse Polynomials and Character Sets, submitted to Adv. Appl. Math.

[GK87] Grigoriev, D.Y., Karpinski, M. The Matching Problem for Bipartite Graphs with Polynomially Bounded Permanents is in NC, Proc. 28^{th} IEEE FOCS (1987), Los Angeles, Oct. 12–14, 1987.

[GKS88] Grigoriev, D.Y., Karpinski, M., Singer, M.F. Fast Parallel Algorithms for Sparse Multivariate Polynomial Interpolation over Finite Fields, preprint, 1988.