On zero-testing and interpolation of sparse character sums (preliminary version)

Andreas Dress *
Fakultät für Mathematik
Universität Bielefeld

Johannes Grabmeier
IBM Deutschland GmbH
Wissenschaftliches Zentrum Heidelberg

Abstract

Motivated by an amazing result of D. Y. Grigoriev and M. Karpinski, the interpolation problem for k-sparse multivariate polynomials has received some attention in recent years. In this note we want to show that essentially all of the results obtained so far hold more generally for k-sparse sums of characters of abelian monoids, thereby providing a useful unified approach to this active field of research. As it turns out the basic ingredients of this approach are the construction of distinction sets for characters and zero–test sets for k-sparse character sums.

Contents

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

0 Introduction

The basic ideas of the paper [GK87] were the starting point for the papers [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. In this note we want to provide a unified approach to this active field of research, based on the observation that the fundamental ideas in these papers are valid in the more general context of k-sparse sums of characters of abelian monoids.

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 by

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

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, that is, subsets $T \subseteq A$ such that for any $f \in X_k \setminus \{0\}$ there exists some $a \in T$ with $f(a) \neq 0$. We will refer to such subsets as *zero-test sets* for X_k. Obviously, any such zero-test set for X_k must contain at least k elements unless $\#X < k$, compare the proof of Lemma 1.1. However, as we will see later on, only in the most simple case of cyclic groups zero-test sets of this cardinality can be guaranteed.

The relation between zero-test sets and subsets of A which may be suitable for interpolation, that is, which allow to distinguish any two different k-sums of characters, is simple and obvious.

Lemma 0.1 *A subset $T \subseteq A$ has the property that the associated restriction map $K^A \to K^T : f \mapsto f|_T$ is injective on $X_k \subseteq K^A$ if and only if T is a zero-test set for X_{2k}.*

Hence, in principle, for any zero-test set T for X_{2k} it should be possible to compute for any map $f = \sum_{\chi \in X} f_\chi \chi$ in X_k its support and its coefficients from its restriction $f|_T$. Again, this holds indeed for the particularly simple minimal zero-test sets one has in cyclic groups. In general there does not seem to exist a universally applicable interpolation algorithm which for any field K, any monoid A, any set $X \subseteq Hom(A, (K, *))$ of K-valued characters of A, and any zero-test set $T \subseteq A$ for X_{2k} allows to reconstruct the support and the coefficients of f for any $f \in X_k$ systematically from its restriction to T, except, of course, the trivial, but surely not efficient algorithm, which for all possible choices of $\chi_1, ..., \chi_k \in X$ and $f_1, ..., f_k \in K$ compares $f(a)$ with $\sum_{\kappa=1}^{k} f_\kappa \chi_\kappa(a)$ for all $a \in T$. Therefore it appears to be worthwhile to discuss in some detail what can be done in this direction.

The examples we have in mind are in particular the cases where A equals U^n for some submonoid U of the monoid $(K, *)$ and X is a 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 the case of $K := \mathbb{Q}$ (or any other infinite field) and $U := K$ the characters from $X := \{\chi^\alpha,\ \alpha \in \mathbb{N}_0^n\}$ correspond to the monomials in n indeterminates as k-sum characters correspond to k-sparse polynomials. In case U is finite it has turned out to be particular interesting to study the above problems for such *monomial characters* of type χ^α whose *local degrees* $\alpha_1, ..., \alpha_n$, are bounded by a natural number q, that is we choose

$$X = X(q, n) := \{\chi^\alpha \mid \alpha \in \mathbf{q}^n\},$$

where $\mathbf{q}$ is defined to be $\mathbf{q} := \{0, \ldots, q-1\}$.

The overall outline of our note is as follows: In the first section we will assume A to be a cyclic group. In this almost trivial case minimal zero-test sets and optimal interpolation procedures can be constructed quite easily in a rather natural and a straightforward manner. Once this is established we will show in the second section that for surprisingly many other choices of A and X our problem can be reduced to the cyclic case.

In various cases this can be done simply by exhibiting a cyclic submonoid, (i.e. a submonoid wich is a cyclic group) A' of A which distinguishes the charachters in the given set X (i.e. with $\chi|_{A'} \neq \psi|_{A'}$ for any two different characters χ and ψ in X).

In other cases where this simple procedure cannot be applied a more subtle approach can be used instead which consists in the construction of a whole family of cyclic submonoids such that for any k characters from X there exists at least one member in this family which distinguishes these k characters. It is remarkable that all but one of the cases studied in [BT88], [CDGK88] and [GKS88] fall in either one of these two categories.

In section 3 we will discuss methods which apply to 'properly' non-cyclic cases. A method based on a simple idea, developed in [CDGK88], by which zero-test sets for a product of monoids can be constructed from zero-test sets of the factors, is presented. In addition a quite general and efficient interpolation algorithm is given, of course needing more evaluations than in the cyclic case, but not needing to find roots of a polynomial as it is necessary in the case of cyclic groups. Instead, it presupposes the knowledge of a finite super set Y of $supp(f)$, say of cardinality q, in which case it needs one inversion of a $q \times q$-matrix and many inversions of $k \times k$-matrices.

Finally, in the last section, we will use all these results to discuss in some detail how for a given submonoid U of the multiplicative monoid $(K, *)$ and for variable $n, q, k \in \mathbb{N}$ the minimal cardinality of zero-test sets in U^n for k-sums of characters from the set $X = X(q, n)$ varies with n, q and k. As it will turn out there seems to exist some kind of 'phase transition' depending on the size first of all of q, but also of n and k, relative to the cardinality of U. This will help to clarify in particular the relation between the results presented in [BT88], [CDGK88] and [GKS88].

1 Character Sums of Cyclic Groups

In this section we assume A to be a cyclic group, generated by some $a \in A$, and we assume X to consist of all K-valued characters of A:

$$X = Hom(A, (K, *)).$$

Without loss of generality we may assume A to be infinite in which case evaluation at a defines a bijection

$$X \to K, \quad \chi \mapsto \chi(a)$$

whose inverse is given by

$$K \to X, \quad c \mapsto (\chi_c : A \to K, a^i \mapsto c^i).$$

The basis observation on which everything in the next two sections is based, is the following Vandermonde Lemma:

Lemma 1.1 *Let A be a cyclic group generated by an element $a \in A$. Then for $X = Hom(A, (K, *))$ and each natural number $k \leq \#A$ the set*

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

is a minimal zero-test set for X_k.

Proof. Let $f = \sum_{\kappa=1}^{k} f_\kappa \chi_\kappa \in X_k$ be a k-sum of characters. We have

$$f(a^i) = \sum_{\kappa=1}^{k} f_\kappa \chi_\kappa(a^i) = \sum_{\kappa=1}^{k} f_\kappa \chi_\kappa(a)^i$$

for all $i \in \mathbb{N}_0$. Thus we obtain the following matrix equation

$$(\chi_\kappa(a)^i)_{0 \leq i < k, 1 \leq \kappa \leq k} \cdot (f_\kappa)_{1 \leq \kappa \leq k} = (f(a^i))_{0 \leq i < k}.$$

The k-square matrix $(\chi_\kappa(a)^i)_{0 \leq i < k, 1 \leq \kappa \leq k}$ is a non-singular Vandermonde matrix since the $\chi_\kappa(a)$ are pairwise different. □

Note that our proof shows as well how to compute the coefficients of any $f \in X_k$ from the values $f(1), f(a), f(a^2), \ldots, f(a^{k-1})$ once its support is known.

To find the support of f from its values on the zero-test set $\{1, a, a^2, \ldots, a^{2k-1}\}$ for X_{2k} we can use the following result, rather special cases of which occur in [BT88] and [CDGK88] and decoding of BCH-codes, see [LN83].

Theorem 1 *Let A be a cyclic group 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 $M_k := (f(a^{i+j}))_{0\le i,j<k}$ *coincides with the cardinality of* $supp(f)$*.*

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

$$\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_{\tilde{k}} \end{pmatrix} := M_{\tilde{k}}^{-1} \cdot \begin{pmatrix} -f(a^{\tilde{k}}) \\ -f(a^{\tilde{k}+1}) \\ \vdots \\ -f(a^{2\tilde{k}-1}) \end{pmatrix}$$

then the equation

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

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

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

Proof. Let $f = \sum_{\kappa\in I} f_\kappa \chi_\kappa$, where I is any finite superset of the indices of the support of f. We denote by $e_i(I)$ the i-th elementary symmetric polynomial in $\#I$ indeterminates, evaluated at $(\chi_\alpha(a))_{\alpha\in I}$. Now substituting $\chi_\alpha(a)$, $\alpha \in I$, for X in the polynomial

$$p := \prod_{\beta\in I}(X - \chi_\beta(a)) = \sum_{j=0}^{\#I} (-1)^{\#I-j} e_{\#I-j}(I) \cdot X^j \in K[X] \tag{2}$$

yields the generalized Newton identities [MS72], p. 244

$$0 = \sum_{j=0}^{\#I} (-1)^{\#I-j} e_{\#I-j}(I) \chi_\alpha(a)^j, \quad \alpha \in I.$$

Fixing an $i \in \mathbb{N}_0$, multiplying the equation corresponding to α by $f_\alpha \chi_\alpha(a)^i$ and summing over all $\alpha \in I$ results in the following system of equations

$$0 = \sum_{j=0}^{\#I} (-1)^{\#I-j} e_{\#I-j}(I) f(a^{i+j}), \quad i \in \mathbb{N}.$$

As $e_0(I) = 1$ the equations for $0 \le i < \#I$ are equivalent to the matrix equation

$$(f(a^{i+j})_{0\le i,j<\#I} \cdot \Big((-1)^{\#I-j}\, e_{\#I-j}\,(I)\Big)_{0\le j<\#I} = -(f(a^{i+\#I}))_{0\le i<\#I}. \quad (3)$$

The matrix $(f(a^{i+j}))_{0\le i,j<\#I}$ equals $(\chi_\alpha(a^i))D_I(\chi_\alpha(a^i))^t$, where the $\#I$-square matrix D_I is the diagonal matrix $\mathrm{diag}((f_\alpha)_{\alpha\in I})$, see [LN83], 9.48, 9.49. As $\#\{\chi_\alpha(a) \mid \alpha \in supp(f)\} = \tilde{k}$, the cardinality of supp(f) equals the rank of the k-square matrix $f(a^{i+j}))_{0\le i,j<k}$ and this proves *i)*. Furthermore $M_{\tilde{k}} = (f(a^{i+j}))_{0\le i,j<\tilde{k}}$ is non-singular and from equation (3) we see that $e_{\tilde{k}-j} = (-1)^{\#I-j}\, e_{\#I-j}\,(I)$ holds for all $1 \le j \le \tilde{k}$ and for $I = supp(f)$. Therefore the polynomial in equation (1) coincides with p and *ii)* is proved. ▫

If an efficient algorithm for finding the roots of a polynomial over K which is known to have all its roots in K, then it is easy to derive an efficient algorithm to interpolate any $f \in X_k$ from its values on $\{1, a, \dots, a^{2k-1}\}$ from Theorem 1

2 Character Sets which Allow Reduction to Cyclic Groups

Given an abelian monoid A and a set $X \subseteq Hom(A,(K,*))$ of K-valued characters of A, we say that X *allows reduction to one cyclic group* if there exists an element $a \in A$ which distinguishes all characters in X, i.e. $\chi(a) \ne \xi(a)$ for $\chi \ne \xi$. It follows immediately from the Artin-Dedekind Lemma that in this case a k-sum f of characters from X is trivial if and only if the restriction of f to the cyclic group generated by a is trivial. Hence the results of section 1 can be applied. In particular $\{1, a, \dots, a^{k-1}\}$ is a zero-test for X_k and the sums f of characters in X_k can be identified from the values of f on $\{1, a, \dots, a^{2k-1}\}$.

Important examples of character sets which allow cyclic reduction are the following ones:

1. If the submonoid U of $(K,*)$ contains a submonoid which is a free abelian submonoid of rank n, generated, say, by $\{u_1, u_2, \dots, u_n\}$, (in particular, this is the case if U contains $\mathbb{Q}$), then the set of all monomial charcters $\{\chi^\alpha \mid \alpha \in \mathbb{Z}^n\}$ of U^n allows reduction to a cyclic group:

indeed, any two different monomial characters of U^n differ necessarily on $a := (u_1, \dots, u_n)$. This implies in particular many of the results presented in [GK87] and [BT88], where u_i is chosen to be the i-th prime.

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

In particular, since any infinite submonoid of $(K, *)$ either contains an element of infinite order or cyclic submonoids of arbitary large order (cf. Artin) we get the following essentialy trivial, though surprisingly general theorem.

Theorem 2 *If U is an infinite submonoid of the multiplicative monoid $(K, *)$ of a field K and if for natural numbers n and q*

$$X := X(q, n) = \{\chi^\alpha \mid \alpha \in \mathbf{q}^n\}$$

denotes the set of all monomial characters of U^n local degree between 0 and $q - 1$, then for any $k \in \mathbb{N}$ there exists a zero-test set of the form $\{1, a, \dots, a^{k-1}\}$ for X^k in U^n and, in addition, one can identify the support of any map $f \in X_k$ from its values on a corresponding zero-test set for X_{2k}.

To apply the results from section 1 even in cases which do not simply allow reduction to a cyclic group we use the following definition: for givien A and $X \subseteq Hom(X, (K, *))$, as above we define a subset $D \subseteq A$ to be a *k-cover* for X if for any subset $Y \subseteq X$ of cardinality at most k there exists some $a \in D$ with $\chi(a) \neq \psi(a)$ for all $\chi, \xi \in Y$ with $\chi \neq \xi$. Obviously, Lemma 1.1 implies :

Lemma 2.1 *If D is a k-cover of an abelian monoid A and for a character set $X \subseteq Hom(X, (K, *)))$, then $D^{[k]} := \{a^i \mid a \in D,\ 1 \leq i < k\}$ is a zero-test set for X_k.*

In particular, we have the following

Corollary 2.2 *If $X = Hom(A, (K, *))$ and if $D \subseteq A$ generates A, then $D^{[2]} = D \cup \{1_A\}$ is a zero-test set for X_2.*

To construct k-covers in more general situations we may adopt an idea from [GKS88]: for $X \subseteq Hom(A,(K,*))$ and a natural number k we define the collection of *h-distinction sets:*

$$\mathcal{D}(X,h) := \{D \subseteq A|\ \forall \chi,\xi \in X,\ \chi \neq \xi,\ \#\{d \in D \mid \chi(d) = \xi(d)\} < h\}.$$

Hence a member D of $\mathcal{D}(X,h)$ has the property that for every pair of distinct characters there are at most $h-1$ elements in D where the two characters are equal. Of course we are not interested in sets D of cardinality smaller than h, which are trivially in $\mathcal{D}(X,h)$, but in those which are large enough to have subsets being in $\mathcal{D}(X,1)$ as well.

Lemma 2.3 *Every h-distinction set D having more than $(h-1)\cdot\binom{k}{2}$ elements is a k-cover of X.*

Proof. Let Y be a subset of X, having at most k elements. The set $\cup_{\chi,\xi\in Y,\chi\neq\xi}\{d \in D \mid \chi(d) = \xi(d)\}$ has atmost $(h-1)\cdot\binom{\#Y}{2} \leq (h-1)\cdot\binom{k}{2}$ elements, therefore there exists an element a in D such that $\chi(a) \neq \xi(a)$ for all distinct $\chi,\xi \in Y$. □

In [GKS88] D. Grigoriev, M. Karpinski and M. Singer have shown that the following observation — tranformed here into our more general context — has striking consequences.

Lemma 2.4 (cf. [GKS88]) . *Let A denote an abelian monoid and assume K to be field, containing a primitive root of unity ω of order e. Assume that for some positive integer n we have characters $\chi_1,\ldots,\chi_n : A \to K$, elements $a_1,\ldots,a_n \in A$, and integers $\epsilon_{\mu,\nu} \in \mathbb{Z}$ for all $1 \leq \mu,\nu \leq n$ such that*

$$\chi_\mu(a_\nu) = \omega^{\epsilon_{\mu,\nu}}.$$

Assume furthermore that $det(\epsilon_{\mu,\nu}) \neq 0$ and that $c := (c_{\nu,\rho})_{1\leq\nu\leq n,1\leq\rho\leq r}$ is an $n \times r$-matrix for some $r \geq n$ such that every $n \times n$-submatrix of c has a non-vanishing determinant. Then if

$$q := \left\lceil \frac{e}{n \cdot max_{\mu,\rho}(|\sum_{1\leq\nu\leq n}\epsilon_{\mu,\nu}c_{\nu,\rho})|)} \right\rceil$$

and

$$X := \{\chi^\alpha : A \to R \mid \alpha \in \mathbf{q^n}\},$$

where χ^α *denotes* $\prod_{1\le\nu\le n}\chi_\nu^{\alpha_\nu}$, *is a set of* q^n *different characters, then the set*

$$D := \{d_\rho := \prod_{1\le\nu\le n} a_\nu^{c_{\nu,\rho}} \mid 1\le\rho\le r\}$$

is in $\mathcal{D}(X,n)$.

Proof. For every pair of different characters χ^α and χ^β from X and for all $1\le\rho\le r$ we have

$$\chi^\alpha(d_\rho) = \omega^{\sum_{\mu=1}^n(\sum_{\nu=1}^n \epsilon_{\mu,\nu}c_{\nu,\rho})\alpha_\mu}$$

which equals $\chi^\beta(d_\rho)$ if and only if

$$\sum_{\mu=1}^n(\sum_{\nu=1}^n \epsilon_{\mu,\nu}c_{\nu,\rho})(\alpha_\mu-\beta_\mu)\equiv 0 \ \text{ modulo } e.$$

Furthermore we have

$$|\sum_{\mu=1}^n(\sum_{\nu=1}^n \epsilon_{\mu,\nu}c_{\nu,\rho})(\alpha_\mu-\beta_\mu)| \le n\cdot max_{\mu,\rho}(|\sum_{1\le\nu\le n}\epsilon_{\mu,\nu}c_{\nu,\rho}|)(q-1) < e.$$

Altogether two different characters $\chi^\alpha,\chi^\beta\in X$ coincide at an element $d_\rho\in D$ if and only if

$$\sum_{\mu=1}^n(\sum_{\nu=1}^n \epsilon_{\mu,\nu}c_{\nu,\rho})(\alpha_\mu-\beta_\mu) = 0.$$

If there were more than $n-1$ elements from D where χ^α and χ^β coincide then the non-singularity of the corresponding $n\times n$-submatrix of c together with that of $det(\epsilon_{\mu,\nu})$ would imply $\alpha-\beta=(0,\dots,0)$. □

In order to apply this lemma we first of all have to construct an integral matrix c satisfying the requirements from the lemma and having not too large entries. To do this we present the following lemma from [GKS88], which uses Cauchy's determinants in a rather elegant way:

Lemma 2.5 *For every two positive integers* r *and* n *there exists an integral* $n\times r$*-matrix* $c=(c_{\nu,\rho})_{1\le\nu\le n,1\le\rho\le r}$, *the absolute value of each entry bounded by* $n+r-1$, *such that no subdeterminant of* c *vanishes. Furthermore, all entries in the first row are pairwise different.*

Proof. Choose a prime number p with $n+r \le p < 2(n+r)$. Then for $1 \le \nu \le n$ and $1 \le \rho \le r$ none of the numbers $\nu+\rho-1$ considered in $GF(p)$ equals 0. Therefore we can consider the matrix

$$\Big(\frac{1}{\nu+\rho-1}\Big)_{1\le \nu,\rho<r} \in GF(p)^{n\times r}.$$

By Lemma 2.6 below no subdeterminant of this matrix vanishes. Choose integers $c_{\nu,\rho}$ with $-\frac{p-1}{2} \le c_{\nu,\rho} \le \frac{p-1}{2}$ such that $\frac{1}{\nu+\rho-1} = c_{\nu,\rho}$ in $GF(p)$, then the same is true for the matrix $c = (c_{\nu,\rho})$. ▫

Lemma 2.6 (Cauchy) . *For every natural number n the following identity in rational functions in commuting indeterminates* $(x_1,\dots,x_n),(y_1,\dots,y_n)$ *holds:*

$$\det\Big(\frac{1}{x_i+y_j}\Big)_{1\le i\le n, 1\le j\le n} = \frac{\prod_{1\le i<j\le n}(x_j-x_i)\prod_{1\le i<j\le n}(y_j-y_i)}{n\prod_{1\le i,j\le n}(x_i+y_j)}.$$

Proof. The polynomial

$$\prod_{1\le i,j\le n}(x_i+y_j)\det\Big(\frac{1}{x_i+y_j}\Big)_{1\le i\le n,1\le j\le n}$$

is not the zero-polynomial, because the coefficient of

$$x_1^{n-1}x_2^{n-2}\dots x_{n-1}y_1^{n-1}y_2^{n-2}\dots y_{n-1}$$

is 1. Considered as polynomial in the y's it is alternating. Each coefficient of the monomials in the y's is itself an alternating polynomial in the x's. As the Vandermonde is the alternating non-zero polynomial having smallest degree, namely $\binom{n}{2}$, it is a scalar multiple of the Vandermonde determinant involving the indeterminates $(y_1,\dots,y_n)$ and the coefficient has to be a Vandermonde determinant involving $(x_1,\dots,x_n)$. ▫

The last lemmata together imply the next result.

Theorem 3 *If U is a finite (and therefore cyclic!) subgroup 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 integer 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 $k \cdot ((n-1) \cdot \binom{k}{2} + 1)$ *for the sums of characters from* $X(q,n)_k = \{\chi^\alpha \mid \alpha \in \mathbf{q^n}\}_k$.

Proof. W.l.o.g. assume $n \geq 2$. Put $r := (n-1) \cdot \binom{k}{2} + 1$ and choose $c = (c_{\nu,\rho})_{1 \leq \nu \leq n, 1 \leq \rho \leq r}$ according to Lemma 2.5. Choose a generator ω for U. Note that $\chi_\mu(a_\nu) = \omega^{\delta_{\mu,\nu}}$ for

$$a_\nu := (1, \ldots, 1, \omega, 1, \ldots, 1),$$

ω at the position ν, and the projections $\chi_\mu = \chi^{(\delta_{\mu,0}, \ldots, \delta_{\mu,n-1})}$ to the μ-th component holds for all $1 \leq \mu, \nu \leq n$. An application of Lemma 2.4 guarantees the set

$$D := \{d_\rho := \prod_{1 \leq \nu \leq n} a_\nu^{c_{\nu,\rho}} \mid 1 \leq \rho \leq r\}$$

to be in $\mathcal{D}(X(\tilde{q}, n), n)$ for $\tilde{q} := \lceil \frac{e}{n \cdot max_{\mu,\rho}(|\sum_{1 \leq \nu \leq n} \epsilon_{\mu,\nu} c_{\nu,\rho})|)} \rceil$ and therefore in $\mathcal{D}(X(q,n), n)$ in view of

$$\begin{aligned} q &< \frac{e}{n \cdot (n + (n-1) \cdot \binom{k}{2})} + 1 = \frac{e}{n \cdot (n + r - 1)} + 1 \leq \\ &\leq \frac{e}{n \cdot max_{\mu,\rho}(|c_{\mu,\rho}|)} + 1 \leq \tilde{q} + 1, \end{aligned}$$

that is $q \leq \tilde{q}$. In view of $0 \neq |c_{0,\rho} - c_{0,\rho'}| \leq 2 \cdot (n+r-1) = 2 \cdot (n + (n-1) \cdot \binom{k}{2}) < e$ and therefore $d_\rho \neq d_{\rho'}$ for $1 \leq \rho < \rho' \leq r$ the set D has r elements. Hence $(n-1) \cdot \binom{k}{2} \leq r = \#D$ and we may apply the Lemmata 2.3 and 2.1 to conclude that

$$\{(\omega^{\kappa \cdot c_{0,\rho}}, \omega^{\kappa \cdot c_{1,\rho}}, \ldots, \omega^{\kappa \cdot c_{n-1,\rho}}) \mid 1 \leq \rho \leq r, 1 \leq \kappa < k\}$$

is a zero-test set for $X(q,n)_k$ of size at most $k \cdot r = k \cdot ((n-1) \cdot \binom{k}{2} + 1)$ ▫

The main result of the paper [GKS88] is the case where K is the finite field $GF(s)$ for a some s with $s \geq qk^2n^2$ and $U := GF(s) \setminus \{0\}$ in Theorem 3.

3 General Case

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

Lemma 3.1 (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 $(X \times Y)_k$.

Proof. Note that any $f \in (X \times Y)_k$ can be written uniquely in the form

$$f = \sum_{\eta \in Y} f_\eta \cdot \eta$$

for some $f_\eta \in X_{i(\eta)}$ $(\eta \in Y)$ and $\sum_{\eta \in Y} i(\eta) \leq k$. Obviously the cardinality j of the Y-*support* $supp_Y(f) := \{\eta \in Y \mid f_\eta \neq 0\}$ of f is bounded by k and in case $f \neq 0$ there must exist some $\eta_0 \in supp_Y(f)$ with $i(\eta_0) \leq \frac{k}{j}$. Choose $a \in A_{i(\eta_0)}$ with $f_{\eta_0}(a) \neq 0$. Consequently, $f(a,-)$ is a non-zero j-sum of characters from Y for which we can find an element $b \in B_j$ with $f(a,b) \neq 0$.
□

This lemma generalizes immediately to the situation of more than two factors.

Lemma 3.2 *If $A^{(1)}, \ldots, A^{(n)}$ are abelian monoids, if for given $X^{(\nu)} \subseteq Hom(A^{(\nu)}, R)$ we have zero-test sets $A_1^{(\nu)} = \{1_{A^{(\nu)}}\}, A_2^{(\nu)}, \ldots, A_k^{(\nu)} \subseteq A^{(\nu)}$ for $X_1^{(\nu)}, X_2^{(\nu)}, \ldots, X_k^{(\nu)}$, respectively for $\nu = 1, \ldots, n$, then the set*

$$\bigcup_{i_1 \cdot \ldots \cdot i_n \leq k} A_{i_1}^{(1)} \times \ldots \times A_{i_n}^{(n)} \subseteq A^{(1)} \times \ldots \times A^{(n)}$$

is a zero-test set for k-sums from $X^{(1)} \times \ldots \times X^{(n)} \subseteq Hom(A^{(1)}, R) \times \ldots \times Hom(A^{(n)}, R) = Hom(A^{(1)} \times \ldots \times A^{(n)}, R)$.

Corollary 3.3 *Let A be a finitely generated abelian group isomorphic to $\prod_{1 \leq \nu \leq n} C_{q_\nu}$ where C_{q_ν} is a cyclic group of order q_ν, q_ν a prime power or ∞, generated by a_ν. Then*

$$\bigcup_{\substack{k_1 \cdot \ldots \cdot k_n \leq k \\ k_\nu \leq min(k, q_\nu)}} T_{k_1}^{(1)} \times \ldots \times T_{k_n}^{(n)},$$

where $T_{k_\nu}^{(\nu)} := \{1, a_\nu, a_\nu^2, \ldots, a_\nu^{\mathbf{k}_\nu - 1}\}$ *is a zero-test set for all sums of characters from* $X_k = \{\chi^\alpha \mid \alpha \in \prod_{1 \le \nu \le n} \mathbf{q}_\nu\}$ *($\infty := \mathbb{Z}$).*

Theorem 4 (cf. [CDGK88]) . *Let U be a finite submonoid of order q of the multiplicative group of a field K for a natural number q, let X be the set of characters $X(n, q)$ for U^n and T be any zerotest set for X_k. If U contains 0, then for every subset $S \subseteq \{1, ..., n\}$ such that $\#S \le \lfloor log_2 k \rfloor$ the set T contains an element $a^S = (a_1^S, \ldots, a_n^S)$ with $S = \{i : a_i^S = 0\}$. Hence T has at least $\sum_{i=0}^{\lfloor \log_2 k \rfloor} \binom{n}{i}$ elements.*

Proof. For every subset $S \subseteq \{1, ..., n\}$ such that $\#S \le \lfloor log_2 k \rfloor$ define a sum of characters by

$$f_S := \prod_{i \in S} (\chi_i^{q-1} - 1) \cdot \prod_{i \notin S} \chi_i,$$

where χ_i is the projection to the i-th component. These functions have the following properties:

1. p_S is in X_k.
2. $p_S(a) \neq 0$ if and only if $\{i : a_i = 0\} = S$.

The first property follows from $2^{\#S} \le 2^{\lfloor log_2 k \rfloor} \le k$, the second from the fact that the zeros of $\chi_i^{q-1} - 1$ are exactly the elements of $U \setminus \{0\}$. Hence, to distinguish such a polynomial and the zero-polynomial, there has to be an element a^S as claimed in the set A. □

In case $q = 2$ we may combine Corollary 2.2 and the results before to obtain a minimal zero-test set.

Theorem 5 (cf. [CDGK88]) . *Let U be the submonoid $\{0, 1\}$ of a field K, let X be the set of characters $X(n, 2)$ for U^n. Then*

$$\{a^S \in U^n \mid S \subseteq \{1, ..., n\},\ a_i^S = \begin{cases} 1, & \text{if } i \in S; \\ 0, & \text{if } i \neq S. \end{cases}$$

is a minimal zero-test set of X_k of cardinality $\sum_{i=0}^{\lfloor \log_2 k \rfloor} \binom{n}{i}$.

Proof. It suffices to show that this set really is a zero-test set, but this follows from Lemma 3.1 using $A_2^{(\nu)} := \{0, 1\}$ for all $1 \leq \nu \leq n$. $\square$

As we have observed already in the introductions there does not seem to exist a universally applicable algorithm which would allow to interpolate k-sums of characters from some character set X from their restrictions to zero-test sets for X_{2k}. Hence to construct interpolation algorithms one has to consider more specific situations. One such situation is described in the following:

Theorem 6 . *Assume that for some field K, some monoid A, some finite set $X \subseteq Hom(A, (K, *))$ of K-valued characters of A of cardinality q, and some subset $D \subseteq A$ of the same cardinality q with $det(\chi(a))_{\chi \in X, a \in D} \neq 0$, the inverse of the $q \times q$-matrix $(\chi(a))_{\chi \in X, a \in D}$ is given and that in addition for any two natural numbers k and n a zero-test set $T_{n,k} \subseteq A^n$ of cardinality $t(n, k)$ for X^n is specified. Then for any $k, n \in \mathbb{N}$ one can compute $supp(f)$ as well as the coefficients of f for any $f \in (X^n)_k$ from altogether at most $n \cdot (k^2 = q) \cdot t(n-1, k)$ evaluations of f by an algorithm which needs at most $2n$ matrix inversions, each matrix having at most k rows ans colums, and otherwise only matrix multiplications and methods to find for $r \leq k$ and $r \leq l \leq max(k^2, q)$ the first r linearly indepentent columns in an $r \times l$ matrix of rank r. Moreover, the $2n$ matrix inversions can be performed on n parallel processors so that the first n inversions, then the next $\frac{n}{2}, \frac{n}{4}, \ldots$ inversions can be done in parallel, leading to altogether to $\log_2(n)$ basic computational rounds.*

Proof. We define set partitions $P^l := (P_1^l, \ldots, P_{\lceil \frac{n}{2^l} \rceil}^l)$ of $\mathbf{n}$ for $0 \leq l \leq \lceil \log_2 n \rceil$ by

$$P_\nu^l := \{\nu \cdot 2^l, \nu \cdot 2^l + 1, \ldots, (\nu + 1) \cdot 2^l - 1\},$$

of course stopping at $n - 1$ in the last part. Next the sets $(supp_{P_\nu^l})_{0 \leq \nu < \lceil \frac{n}{2^l} \rceil}$ are determined inductively. In case $l = 0$ we use n-times Lemma **??** for $T := P_\nu^0 = \{\nu\}$ and the supersets $\hat{Y}^{\{\nu\}}$, always setting A^T to be $\prod_{\nu \notin T} A^{(\nu)}$ and making the usual identifications. For the induction step we use at most $\lceil \frac{n}{2^{l+1}} \rceil$-times Lemma **??** for $T := P_\nu^{(l+1)}$ and the supersets $\hat{Y}^{P_\nu^{l+1}} := supp_{P_{2\nu}^l}(f) \times supp_{P_{2\nu+1}^l i}(f)$.
This is justified as more generally suppose that for disjoint subsets T_0 and T_1 of $\mathbf{n}$ the corresponding supports $supp_{Y^{T_0}}(f)$ and $supp_{Y^{T_1}}(f)$ are known,

then it is clear that we can use $Y^{T_0 \cup T_1} \supseteq \hat{Y}^{T_0 \cup T_1} := supp_{Y^{T_0}}(f) \times supp_{Y^{T_1}}(f)$ as a finite superset of $supp_{Y^{T_0 \cup T_1}}(f)$.
Finally we arrive at $supp(f)$. An application of lemma **??** for $T := \mathbf{n}$ gives the coefficients of f. $\square$

Note that we only required elements d^T and zero-test sets Z^T for the at most $2n+1$ sets occuring in the set partitions. The calculations to recover f require at most $2n+1$ applications of Lemma **??**, i.e. in step 0 we have to invert (in parallel) n Vandermonde matrices, having as many rows and columns as the cardinality of the given supersets of $supp_{\{\nu\}}(f)$. In the next $\lceil \log_2 n \rceil$ steps at each stage l at most $\lceil \frac{n}{2^l} \rceil$ Vandermonde matrices of size $k^2 \times k^2$ have to be inverted. A further inversion of a $k \times k$ Vandermonde matrix gives the coefficients. Note further that the number of evaluation points can be reduced if one allows adaptive algorithms.

A similar result holds for the more general case of products $\prod_{1 \le \nu \le n}$ and character sets $X_1, \ldots, X_n$ as long as for every $1 \le \nu \le n$ a zero-test set for a $(\prod_{\mu \ne \nu} X_\mu)_k$ is known.

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

[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.

[KR88] Karp, R.M., Ramachandran, V. L. A Survey of Parallel Algorithms for Shared-Memory Machines, Preprint, 1988, to appear in the Handbook of Theoretical Computer Science, North-Holland

[LN83] Lidl, H., Niederreiter, H. Finite Fields,Encyclopedia of Mathematics and its Applications, Vol.10, Cambridge University Press 1983.

[MS72] MacWilliams, F.J., Sloane, N.J.A. The Theory of Error Correcting Codes,North Holland (1972).

[M86] Mulmuley, K. A Fast Parallel Algorithm to Compute the Rank of a Matrix over an Arbitrary Field, Proc. STOC ACM (1986), 338–339.