Numerical Sparsity Determination and Early Termination*

Zhiwei Hao
Key Laboratory of Mathematics Mechanization, AMSS
Beijing 100190, China
haozhiwei@mmrc.iss.ac.cn

Erich L. Kaltofen
Dept. of Mathematics, NCSU
Raleigh, North Carolina
27695-8205, USA
kaltofen@math.ncsu.edu
http://www.kaltofen.us

Lihong Zhi
Key Laboratory of Mathematics Mechanization, AMSS
Beijing 100190, China
lzhi@mmrc.iss.ac.cn
http://www.mmrc.iss.ac.cn/~lzhi/

ABSTRACT

Ankur Moitra in his paper at STOC 2015 has given an in-depth analysis of how oversampling improves the conditioning of the arising Prony systems for sparse interpolation and signal recovery from numeric data. Moitra assumes that oversampling is done for a number of samples beyond the actual sparsity of the polynomial/signal. We give an algorithm that can be used to compute the sparsity and estimate the minimal number of samples needed in numerical sparse interpolation. The early termination strategy of polynomial interpolation has been incorporated in the algorithm: by oversampling at a small number of extra sample points we can diagnose that the sparsity has not been reached.

Our algorithm still has to make a guess, the number ζ of oversamples, and we show by example that if ζ is guessed too small, premature termination can occur, but our criterion is numerically more accurate than that by Kaltofen, Lee and Yang (Proc. SNC 2011, ACM [12]), but not as efficiently computable. For heuristic justification one has available the multivariate early termination theorem by Kaltofen and Lee (JSC vol. 36(3–4) 2003 [11]) for exact arithmetic, and the numeric Schwartz-Zippel Lemma by Kaltofen, Yang and Zhi (Proc. SNC 2007, ACM [13]). A main contribution here is a modified proof of the Theorem by Kaltofen and Lee that permits starting the sequence at the point $(1, \ldots, 1)$, for scalar fields of characteristic $\neq 2$ (in characteristic 2 counter-examples are given).

Categories and Subject Descriptors

F.2.1 [**Numerical Algorithms and Problems**]: Computations on matrices, Computations on polynomials; G.1.1 [**Interpolation**]; I.1.2 [**Algorithms**]: Algebraic algorithms, Analysis of algorithms

*This research was supported in part by the National Science Foundation under Grant CCF-1421128 (Kaltofen) and by the National Natural Science Foundation of China under Grants 11571350 (Zhi).

ISSAC '16, July 19 - 22, 2016, Waterloo, ON, Canada

 ISBN 978-1-4503-4380-0/16/07…$15.00

DOI: http://dx.doi.org/10.1145/2930889.2930924

Keywords

Hankel matrix, Vandermonde matrix, condition number, sparse polynomial interpolation, early termination, sparse signal processing

1. INTRODUCTION

The sparse interpolation problem has been studied and widely used in many different areas of science and engineering since the work of Prony (1795). The classical Prony's method aims to solve the exponential interpolation problem

$$f(x) = \sum_{j=1}^{t} c_j \exp(d_j 2\pi \mathrm{i} x),$$

where the frequencies $d_i \in [0, 1)$. By sampling f at $f(0), \ldots, f(2t-1)$ and solving a Hankel linear system to compute the term locator polynomial whose roots are $= \exp(d_j 2\pi \mathrm{i}), 1 \leq j \leq t$. The amplitude coefficients c_j can be computed by solving a Vandermonde linear system. With highly accurate big floating point precision, Prony's method is straightforward to implement.

When there is inaccuracy (noise) in the measurements, both the Hankel matrix and Vandermonde matrix appearing in Prony's method can have exponentially large condition numbers [2, 9]. Moreover, as shown by Moitra in [17, Theorems 2.3, 3.1] there is a sharp phase transition for the condition number of the Vandermonde matrix and the minimum number of samples needed, the place of which essentially depending on the minimum separation in the presence of noise. In Moitra's algorithm [17, Algorithm 1], both the sparsity and the minimal number of samples are input as known values. However, without knowing the structure of sparsity, it is unclear how to estimate the condition number of the Vandermonde matrix and determine the minimal measurements needed. The arising Hankel matrix H_m can only be used to bound the conditioning of the Vandermonde matrix after m reaches the sparsity t (see (26), i.e., V_m has full column rank). As shown by Example 4.1, an arising Hankel matrix can be nearly-singular before m reaches t for unluckily chosen samples. Therefore, a well-conditioned Vandermonde matrix may correspond to a nearly-singular Hankel matrix when $m \leq t$. That phenomenon motivates us to investigate how to reliably determine the number of terms t of f and how many number of measurements are minimally needed in the entire process of numerical sparse interpolation with unknown sparsity.

In exact arithmetic, the early termination strategy [11] has been introduced as a means to determine the number

of terms t: one terminates the interpolation algorithm after consecutively encountering singular Hankel matrices ζ times for a pre-chosen threshold $\zeta \geq 1$. It has been shown in [11] that with a high probability that grows with ζ, one does not stop before the sparsity is reached. However, in numerical cases, as we have explained above, the Hankel matrices could be extremely ill-conditioned, and one may not be able to detect the number of terms by observing the first several nearly-singular Hankel matrices. Based on the precise quantitative bounds given in [17], we present a lower bound on the t-th singular value $\sigma_t(H_m)$ of the m-th arising Hankel matrix H_m and an upper bound on the ratio of $\sigma_1(H_m)/\sigma_t(H_m)$, which give us the criterion (24), which computes the sparsity t of f by checking whether the first t singular values of all Hankel matrices $H_m, H_{m+1}, \ldots, H_{m+\zeta-1}$ are larger than $1-\epsilon$ and the remaining singular values are less than ϵ and none lie in between. We show by experiments that the criterion is quite tolerant to noise in the samples. In particular, in Example 4.1 from [2] we can avoid premature termination by a moderately large number ζ (≥ 6) of oversamples.

Finally, in Section 4.1 we prove the Early Termination Theorem [11, Theorem 4] for the (unshifted)-sequence starting at the point $(1, \ldots, 1)$ for coefficient fields of characteristic $\neq 2$ (see Theorem 4.1) and give counterexamples for characteristic $= 2$, which resolves an open question in [11].

2. PRELIMINARIES

We consider the polynomial version of Prony's method with coefficients from an arbitrary field K. Let $f \in \mathsf{K}[x]$, where

$$f = \sum_{i=1}^{t} c_i x^{e_i}, \ c_i \neq 0,$$

and K is an arbitrary field. p is a prime number larger than $\deg(f)$. Let $a_i = f(\omega^i)$ where ω is selected as a random p-th root of unity. Let H_m be the Hankel matrix defined by the sequence of $a_0, \ldots, a_{2m-2}$:

$$H_m = \begin{bmatrix} a_0 & \cdots & a_{m-1} \\ a_1 & \cdots & a_m \\ \vdots & \vdots & \vdots \\ a_{m-1} & \cdots & a_{2m-2} \end{bmatrix}. \tag{1}$$

We have the following well-known decomposition of H_m:

$$H_m = V_m \cdot D \cdot V_m^{\mathrm{T}}, \tag{2}$$

where V_m is the $m \times t$ Vandermonde matrix:

$$V_m = \begin{bmatrix} 1 & \cdots & 1 \\ \omega^{e_1} & \cdots & \omega^{e_t} \\ \vdots & \vdots & \vdots \\ \omega^{e_1(m-1)} & \cdots & \omega^{e_t(m-1)} \end{bmatrix} \tag{3}$$

and D is a $t \times t$ diagonal matrix:

$$D = \begin{bmatrix} c_1 & & \\ & \ddots & \\ & & c_t \end{bmatrix}. \tag{4}$$

By V_m^{T} we denote the transpose of the Vandermonde matrix V_m.

In exact arithmetic, the early termination strategy can determine the number of terms with high probability, i.e., with high probability, all $j \times j$ leading principle minors of H_t are non-singular for $2 \leq j \leq t$. Moreover, H_j must be singular for all $j > t$. Hence the number of terms is detected as follows: for $j = 2, 3, \ldots$, the first time H_j becomes singular is when $j = t+1$. Strictly speaking, one needs that the characteristic of the field is $\neq 2$ and our new Theorem 4.1 (see Section 4.1 for more detail). It is known that the Hankel matrices can become extremely ill-conditioned: [12] investigates how to estimate the spectral norm of the inverse of a Hankel matrix H_t and how to employ several randomization ideas of [9] for heuristically achieving a relatively well-conditioned Hankel matrix H_t. Then one can detect the number of terms by observing a sharp increase in the condition number of H_{t+1}.

Oversampling is another popular method to improve the conditioning of the Hankel matrix [6]. There are many exciting new results on sparse signal recovering from noisy data, see [4, 5, 15, 17] and the references there. Especially, in [17], Ankur Moitra provides an explicit formula to estimate the condition number of the Vandermonde matrix provided that $m > (1/\Delta) + 1$, where Δ is the minimum separation of the evaluated terms in f. Moreover, a lower bound of the condition number of V_m was also given to show that in the noisy case, if $m = (1-\epsilon)/\Delta$ there is a pair of t point sources x and x', each with separation Δ, which allow only exponentially small noise to tell them apart. Such extreme ill-posedness has also been illustrated in [5] based on the work of David Slepian [18].

In the following, we will show how to apply quantitative bounds for singular values of Hankel matrices and the early termination strategy for the unshifted case in order to determine the sparsity of the polynomial f in the presence of noise.

3. NUMERIC SPARSITY DETERMINATION

We extend Theorem 2.3 in [17] to give a lower bound on the t-th singular value of H_m for $m > \frac{1}{\Delta} + 1$, which provides us a new criterion to estimate the number of terms of f by checking whether the singular values of oversampled Hankel matrices are separated into those $> 1-\epsilon$ and those $< \epsilon$ and none lie in between. In this section K is specialized as the complex field.

Definition 3.1 (see [5]). *Let $\mathcal{B}$ be the unit circle obtained by identifying the endpoints on $[0, 1]$. For a family of points $B \subset \mathcal{B}$, the minimal separation is defined as the closest distance between any two elements from B:*

$$\Delta(B) = \inf_{(b,b') \in B : b \neq b'} |b - b'|, \tag{5}$$

where $|b-b'|$ is the wrap-around distance. That is the length of the minor arc between b and b' divided by 2π.

Let

$$\omega = e^{2\pi \mathrm{i} j/p}, \ 0 \leq j < p, \tag{6}$$

where the integer j can be chosen randomly or fixed. Let

$$\Delta = \Delta(\omega^{e_1}, \ldots, \omega^{e_t}).$$

It is clear that

$$1 + \frac{1}{\Delta} > t.$$

The following theorem has been proved in [17].

Theorem 3.1. *Let $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_t$ be singular values of V_m, provided $m > 1 + \frac{1}{\Delta}$, we have*

$$m - 1 + \frac{1}{\Delta} \geq \sigma_1^2 \geq \sigma_2^2 \geq \cdots \geq \sigma_t^2 \geq m - 1 - \frac{1}{\Delta}. \quad (7)$$

The condition number κ of V_m satisfies

$$\kappa^2 \leq \frac{m + 1/\Delta - 1}{m - 1/\Delta - 1}. \quad (8)$$

The upper and lower bounds given in (7) and (8) can be used to bound $\sigma_t(H_m)$ and $\sigma_1(H_m)$ for $m > 1 + \frac{1}{\Delta}$. First, let us see how to bound $\sigma_t(H_m)$ by the t-th singular value $\sigma_t(V_m)$ of V_m.

Lemma 3.2. *For $m \geqslant t$, we have*

$$\sigma_t(H_m) \geq \sigma_t^2(V_m) \cdot \min_{1 \leq i \leq t} |c_i|. \quad (9)$$

Proof. Rewrite $H_m = V_m \cdot D^{\frac{1}{2}} \cdot D^{\frac{1}{2}} \cdot V_m^{\mathrm{T}}$ and set

$$W_m = V_m \cdot D^{\frac{1}{2}} \in \mathbb{C}^{m \times t}.$$

If $\omega^{e_i} \neq \omega^{e_j}$ for $i \neq j$, and $m \geq t$, then $V_m \in \mathbb{C}^{m \times t}$ has full column rank t. Moreover, since $c_i \neq 0$, the diagonal matrix $D \in \mathbb{C}^{t \times t}$ is invertible. Hence we have

$$\mathrm{rank}(H_m) = \mathrm{rank}(D) = \mathrm{rank}(W_m) = \mathrm{rank}(V_m) = t.$$

Claim 3.3. $\sigma_t(H_m) \geqslant \sigma_t^2(W_m)$.

Indeed, let $W_m = U \cdot \Sigma \cdot V$ be the singular value decomposition of W_m, where $U \in \mathbb{C}^{m \times m}$, $\Sigma \in \mathbb{C}^{m \times t}$, $V \in \mathbb{C}^{t \times t}$. Denote by $W_m^\dagger$ the Moore-Penrose pseudoinverse of W_m, which has been proved to be unique [10], and $W_m^\dagger = V^H \cdot \Sigma^\dagger \cdot U^H$, where V^H and U^H represent the Hermitian transpose of the matrix V and U respectively and $\Sigma^\dagger$ is constructed by substituting the non-zero items in Σ by their inverse. It is clear that

$$H_m^\dagger = (W_m \cdot W_m^{\mathrm{T}})^\dagger = (W_m^{\mathrm{T}})^\dagger \cdot W_m^\dagger, \quad (10)$$

see [19]. This indicates that:

$$\sigma_1(H_m^\dagger) \leqslant \sigma_1((W_m^{\mathrm{T}})^\dagger) \cdot \sigma_1(W_m^\dagger) = \sigma_1^2(W_m^\dagger). \quad (11)$$

By noticing that:

$$\sigma_1(H_m^\dagger) = \frac{1}{\sigma_t(H_m)}, \sigma_1(W_m^\dagger) = \frac{1}{\sigma_t(W_m)}, \quad (12)$$

we obtain Claim 3.3.

Now we consider the t-th singular value of W_m. According to the property of singular values, we have

$$\sigma_t(W_m) = \min_{\mathrm{rank}(A) < t} \|W_m - A\|_2. \quad (13)$$

Let A_0 be a minimizer in (13), then $A_0 \cdot D^{-\frac{1}{2}}$ is of rank smaller than t. Therefore, we have:

$$\begin{aligned} \sigma_t(V_m) &= \min_{\mathrm{rank}(B) < t} \|V_m - B\|_2, \\ &\leq \|V_m - A_0 \cdot D^{-\frac{1}{2}}\|_2 \\ &= \|(V_m \cdot D^{\frac{1}{2}} - A_0) \cdot D^{-\frac{1}{2}}\|_2 \\ &\leq \|W_m - A_0\|_2 \cdot \|D^{-\frac{1}{2}}\|_2 \\ &= \sigma_t(W_m) \cdot \|D^{-\frac{1}{2}}\|_2. \end{aligned}$$

By noticing that $\frac{1}{\|D^{-1/2}\|_2^2} = \min_{1 \leq i \leq t} |c_i|$, we have

$$\sigma_t^2(W_m) \geq \sigma_t^2(V_m) \cdot \min_{1 \leq i \leq t} |c_i|. \quad (14)$$

Combining with Claim 3.3, we complete the proof. □

Remark 3.1. It should be noted that $\sigma_t(H_t) = \sigma_t^2(W_t)$ when W_t is a real matrix. Otherwise, we may have $\sigma_t(H_t) > \sigma_t^2(W_t)$. For instance, suppose:

$$V_2 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, D = \begin{bmatrix} -1 & 0 \\ 0 & 2 \end{bmatrix}, \quad (15)$$

then

$$H_2 = \begin{bmatrix} 1 & 3 \\ 3 & 7 \end{bmatrix}, W_2 = \begin{bmatrix} \mathrm{i} & \sqrt{2} \\ \mathrm{i} & 2\sqrt{2} \end{bmatrix}, \quad (16)$$

therefore

$$\sigma_2(H_2) = 0.243 > \sigma_2^2(W_2) = 0.169. \square \quad (17)$$

Remark 3.2. Lemma 3.2 is only correct for $m \geq t$. For $m < t$, there exists a well-conditioned Vandermonde matrix V_m which corresponds to a singular Hankel matrix $H_m = V_m \cdot D \cdot V_m^{\mathrm{T}}$, see Example 4.1. □

Theorem 3.4. *For given f and ω, when $m > 1 + \frac{1}{\Delta}$, we have*

$$\sigma_t(H_m) \geq \left(m - 1 - \frac{1}{\Delta}\right) \cdot \min_{1 \leq i \leq t} |c_i|, \quad (18)$$

and

$$\frac{\sigma_1(H_m)}{\sigma_t(H_m)} \leq \frac{m - 1 + \frac{1}{\Delta}}{m - 1 - \frac{1}{\Delta}} \cdot \frac{\max_{1 \leq i \leq t} |c_i|}{\min_{1 \leq i \leq t} |c_i|}. \quad (19)$$

Proof. When $m > 1 + \frac{1}{\Delta}$, according to Theorem 3.1,

$$m - 1 + \frac{1}{\Delta} \geq \sigma_1^2(V_m) \geq \sigma_t^2(V_m) \geq m - 1 - \frac{1}{\Delta}. \quad (20)$$

When $m > 1 + \frac{1}{\Delta} \geq t$, by (9), we have

$$\sigma_t(H_m) \geq \sigma_t^2(V_m) \cdot \min_{1 \leq i \leq t} |c_i| \geq \left(m - 1 - \frac{1}{\Delta}\right) \cdot \min_{1 \leq i \leq t} |c_i|.$$

On the other hand, $\sigma_1(H_m)$ is the 2-norm of H_m, we have

$$\begin{aligned} \sigma_1(H_m) &\leq \sigma_1(V_m) \cdot \sigma_1(D) \cdot \sigma_1(V_m^{\mathrm{T}}) \\ &= \sigma_1^2(V_m) \cdot \max_{1 \leq i \leq t} |c_i| \\ &\leq \left(m - 1 + \frac{1}{\Delta}\right) \cdot \max_{1 \leq i \leq t} |c_i|. \end{aligned}$$

Therefore we can derive (19). □

Theorem 3.4 gives us an estimation on how many evaluations we need to get a Hankel matrix with the t-th singular value larger than or equal to 1.

Theorem 3.5. *When m satisfies*

$$m \geq 1 + \frac{1}{\Delta} + \max_{1 \leq i \leq t} \frac{1}{|c_i|}, \quad (21)$$

we have $\sigma_t(H_m) \geq 1$.

Proof. According to Theorem 3.4, when $m \geq 1 + \frac{1}{\Delta}$, we have

$$\sigma_t(H_m) \geq \left(m - 1 - \frac{1}{\Delta}\right) \cdot \min_{1 \leq i \leq t} |c_i|.$$

Therefore, if m satisfies (21), then

$$\sigma_t(H_m) \geq \max_{1 \leq i \leq t} \frac{1}{|c_i|} \cdot \min_{1 \leq i \leq t} |c_i| = 1. \quad \square$$

The following perturbation theorem about the singular values can be found in [20, 16].

Theorem 3.6. *Let $\sigma_j(A)$ be the j-th singular value of A. Let E be a small perturbation matrix. For $1 \le i \le \dim(A)$, we have*

$$|\sigma_i(A+E) - \sigma_i(A)| \le \|E\|_2. \tag{22}$$

Remark 3.3. In the noise-free case, for $m \ge t+1$, we have

$$\sigma_j(H_m) = 0, \ t+1 \le j \le m.$$

Therefore, according to Theorem 3.6, we have

$$|\sigma_j(H_m + E)| \le \|E\|_2 \overset{\text{def}}{=} \epsilon. \tag{23}$$

The constant 1 in Theorem 3.5 can be an arbitrary number $\tau > 2\epsilon$, and we can always separate the singular values of $H_m + E$ into two groups; $\sigma_j(H_m+E) \ge \tau - \|E\|_2 > \epsilon$ for $j \le t$ and $\sigma_j(H_m+E) \le \epsilon$ for $j > t$. However, choosing $\tau = 1$ means the Hankel matrix H_m is far from being of rank $t-1$. □

Theorem 3.5 and inequality (23) provide us a robust criterion to detect the sparsity t in the numeric case when no premature termination occurs.

Before we state the main algorithm for detecting the sparsity t, we introduce some quantities first.

- m: size of the current Hankel matrix;
- ϵ: error bound for Hankel matrices;
- $n_{\sigma \ge 1-\epsilon}$: the number of the singular values of H_{m-1} that are larger than or equal to $1-\epsilon$;
- $n_{\sigma \le \epsilon}$: the number of the singular values of H_{m-1} that are smaller than or equal to ϵ;
- ζ: the algorithm will be terminated if the condition

$$\begin{cases} n_{\sigma \ge 1-\epsilon}(H_{m+i}) = n_{\sigma \ge 1-\epsilon}(H_{m-1}), \\ n_{\sigma \le \epsilon}(H_{m+i}) = m + i - n_{\sigma \ge 1-\epsilon}(H_{m-1}), \end{cases} \tag{24}$$

is satisfied for any i with $0 \le i \le \zeta - 1$.

Algorithm 1 Sparsity determination

Input:
$f(x)$: a univariate black box polynomial;
ζ: a positive integer, the threshold for early termination;
ϵ: an error bound for Hankel matrices;

Output:
t: the sparsity of $f(x)$.

1: Estimate a prime upper bound p of $\deg(f)$.
2: For a randomly chosen integer $j \in [1, p-1]$, set $\omega \leftarrow e^{2\pi i j/p}$, $n_{\sigma \ge 1-\epsilon} \leftarrow 0$, $n_{\sigma \le \epsilon} \leftarrow 0$, $k \leftarrow 0$, $m \leftarrow 1$, $H_1 \leftarrow f(1)$.
3: **while** $k < \zeta$ **do**
4: Compute the singular values of H_m;
$l_1 \leftarrow$ the number of singular values larger than $1-\epsilon$;
$l_2 \leftarrow$ the number of singular values smaller than ϵ.
5: **if** $l_1 + l_2 = m$ and $l_1 = n_{\sigma \ge 1-\epsilon}$ **then**
6: $k \leftarrow k+1$.
7: **else**
8: $k \leftarrow 0$.
9: **end if**
10: $n_{\sigma \ge 1-\epsilon} \leftarrow l_1$, $n_{\sigma \le \epsilon} \leftarrow l_2$, $m \leftarrow m+1$.
11: Update H_m by evaluating $f(x)$ at ω^{2m-3} and ω^{2m-2}.
12: **end while**
13: $t \leftarrow n_{\sigma \ge 1-\epsilon}$.

Theorem 3.7. *Suppose the errors in Hankel matrices are bounded by ϵ. The algorithm terminates when m satisfies*

$$m \ge 1 + \frac{1}{\Delta} + \max_{1 \le i \le t} \frac{1}{|c_i|} + (\zeta - 1). \tag{25}$$

With high probability, Algorithm 1 returns the number of terms t in f.

Proof. According to Theorem 3.5, when m satisfies

$$m \ge 1 + \frac{1}{\Delta} + \max_{1 \le i \le t} \frac{1}{|c_i|},$$

$\sigma_t(H_m)$ will be at least 1. Moreover, according to Theorem 3.6, we have

$$|\sigma_t(H_m + E)| \ge |\sigma_t(H_m)| - \|E\|_2 \ge 1 - \epsilon.$$

For $m \ge t+1$, we have

$$\sigma_j(H_m) = 0, \ t+1 \le j \le m.$$

According to Theorem 3.6 and inequality (23), for $j = t+1, \ldots, m$, we have

$$|\sigma_j(H_m + E)| \le \|E\|_2 \le \epsilon.$$

Hence the condition (24) will be satisfied ζ times.

A heuristic probabilistic analysis for Algorithm 1 returning the number of terms t in f will be given in Section 4.1. □

Remark 3.4. Since the minimum number of measurements given in (25) depends on $\min_{1 \le i \le t} |c_i|$, if the minimum value is much smaller than 1, then we need a large number of evaluations to bound the singular value $\sigma_t(H_m)$ from 1. In this case, the inequality (19) may give us a better criterion to stop the algorithm. □

The following theorem shows that the t-th singular value of the Vandermonde matrix V_m is bounded below by the t-th singular value of H_m too.

Theorem 3.8. *For $m \geqslant t$, we have*

$$\sigma_t(V_m) \ge \frac{\sigma_t(H_m)}{2m \max_{1 \le i \le t} |c_i|}. \tag{26}$$

Proof. Suppose $V_m = U \cdot \Sigma \cdot V$ is the singular value decomposition of V_m, where $\Sigma \in \mathbb{C}^{m \times t}$, $U \in \mathbb{C}^{m \times m}$, $V \in \mathbb{C}^{t \times t}$. We have

$$\begin{aligned} \sigma_t(V_m) &= \min_{\text{rank}(B) < t} \|V_m - B\|_2, \\ &= \|V_m - \bar{V}_m\|_2, \end{aligned}$$

where

$$\bar{V}_m = U \cdot \text{diag}(\sigma_1(V_m), \ldots, \sigma_{t-1}(V_m), 0) \cdot V.$$

Hence, we have:

$$\begin{aligned} \sigma_t(H_m) &= \min_{\text{rank}(A) < t} \|V_m D V_m^{\mathrm{T}} - A\|_2 \\ &\le \|V_m D V_m^{\mathrm{T}} - \bar{V}_m D \bar{V}_m^{\mathrm{T}}\|_2 \\ &= \|V_m D V_m^{\mathrm{T}} - V_m D \bar{V}_m^{\mathrm{T}} + V_m D \bar{V}_m^{\mathrm{T}} - \bar{V}_m D \bar{V}_m^{\mathrm{T}}\| \\ &\le \|V_m D (V_m^{\mathrm{T}} - \bar{V}_m^{\mathrm{T}})\|_2 + \|(V_m - \bar{V}_m) D \bar{V}_m^{\mathrm{T}}\|_2 \\ &\le \sigma_t(V_m) \|V_m\|_2 \|D\|_2 + \sigma_t(V_m) \|\bar{V}_m\|_2 \|D\|_2 \\ &\le 2\sigma_t(V_m) \|V_m\|_2 \|D\|_2 \\ &\le 2m \max_{1 \le i \le t} |c_i| \sigma_t(V_m). \quad \square \end{aligned}$$

The minimum number of measurements given in (25) depends also on the minimum separation Δ. In [9], several randomization strategies are proposed to enlarge the minimum separation. The following theorem extends results in [9, Theorem 4.3].

Theorem 3.9. *Suppose p is a prime number and $p > \deg(f)$. For a uniformly and randomly chosen integer j with $0 < j < p$ in (6), with probability at least $1 - \frac{1}{2k}$, we have*

$$\Delta > \frac{1}{2kt^2}, \ \forall k \in \mathbb{Z}_{>0}. \tag{27}$$

Proof. We extend the proof in [9, Theorem 4.3]. Assume $e_u > e_v$ for $u < v$, by Definition 3.1, we have

$$\Delta = \frac{1}{p} \cdot \min_{1 \le u < v \le t} \min\{\delta_{u,v}, p - \delta_{u,v}\}, \tag{28}$$

where

$$\delta_{u,v} = e_u \cdot j - e_v \cdot j \mod p.$$

There are at most $\binom{t}{2} \le \frac{t^2}{2}$ distinct values of $(e_u - e_v) \mod p$. For any $k \in \mathbb{Z}_{>0}$, let

$$l = \frac{p}{2kt^2}, \tag{29}$$

then for all

$$c \in \{1, \ldots, \lfloor l \rfloor\} \cup \{p - \lfloor l \rfloor + 1, \ldots, p\},$$

where the floor function $\lfloor l \rfloor$ denotes the largest integer $\le l$, there is only one $j \in \mathbb{Z}_p$ such that

$$\delta_{u,v} = c.$$

Indeed, as p is a prime number larger than $\deg(f)$, $[e_u - e_v]$ is invertible in $\mathbb{Z}_p$, which indicates

$$j = (e_u - e_v)^{-1} \cdot c \mod p,$$

Therefore for any given e_u and e_v, there are $2 \cdot \lfloor l \rfloor$ values of j such that

$$\min\{\delta_{u,v}, p - \delta_{u,v}\} \le l. \tag{30}$$

There are totally at most $(t^2/2) \cdot 2 \cdot \lfloor l \rfloor$ values of j, such that (30) is satisfied by some $\delta_{u,v}$. Therefore with probability

$$\le \frac{t^2}{2} \cdot 2 \cdot \lfloor l \rfloor \cdot \frac{1}{p} \le \frac{t^2}{2} \cdot 2l \cdot \frac{1}{p} = \frac{1}{2k},$$

we can have $\Delta \le \frac{\lfloor l \rfloor}{p} \le \frac{l}{p} \le \frac{1}{2kt^2}$, by (28) and (29). □

Example 3.1. Let $f = 2x^{109} - 5x^{59} + x^{58} + 2x^{47} + 3x^{35}$ and set $\zeta = 5$.

1. Set $\omega = e^{2\pi i/119}$, and assume the evaluation error in H_m is bounded by $\epsilon = 0.05$. The wrap-around distance is

   $$\Delta(\omega^{109}, \ldots, \omega^{35}) = \frac{1}{119}.$$

   When m becomes larger than 16, there are always 5 singular values of H_m that are larger than 1 and all other singular values of H_m are less than 0.05. Therefore the algorithm will stop after $21 = 16 + 5$ steps and return $t = 5$.

   We have $\frac{\sigma_1(H_4)}{\sigma_4(H_4)} \approx 48.7$, $\frac{\sigma_1(H_5)}{\sigma_5(H_5)} \approx 4387$. Therefore, if we use the sharp increase in the condition number of H_m to detect the sparsity, we may mistakenly take $t = 4$.

   We also notice that our algorithm can terminate much earlier than the worst case bound $\frac{1}{\Delta} + 1 = 120$ to detect the sparsity and get a well-conditioned Vandermonde matrix (the condition number of V_{16} is 8.6).

2. We take a random rotation of ω, for instance, set $\omega = e^{2\pi i \cdot 9/119}$. The minimal separation increases and the wrap-around distance is

   $$\Delta(\omega^{109}, \ldots, \omega^{35}) \approx 1/13.$$

   The termination of the algorithm is made 8 steps earlier, i.e., the condition (24) will be satisfied at $m = 8$. □

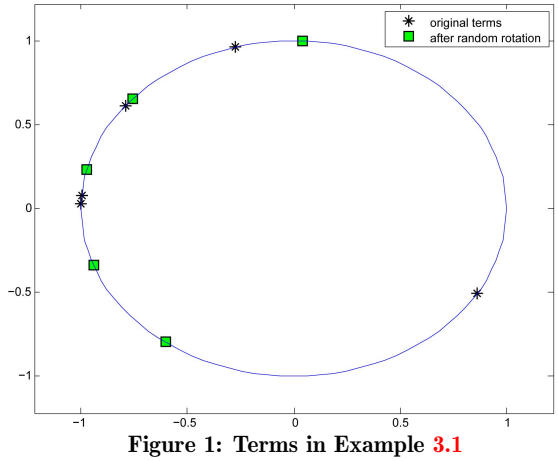

Figure 1: Terms in Example 3.1

4. EARLY TERMINATION STRATEGIES

It should be noted that Algorithm 1 may terminate before m reaches the number of terms t in f.

Example 4.1. [2] Let $f = \sum_{j=1}^{t} c_j x^{e_j}$, where $t = 61$, $c_j = 1$ for $j = 1, \ldots, t$,

$$e_j = \begin{cases} 2(j-1) & j = 1, \ldots, 41, \\ 63 + 2(j-42) & j = 42, \ldots, 51, \\ 1 + 2(j-52) & j = 52, \ldots, 61. \end{cases}$$

Figure 2 shows all terms in f evaluating at $\omega = e^{2\pi i/82}$.

1. The smallest singular value of the Hankel matrix H_m is less than 10^{-11} for any m larger than 23. It is an example used in [2] to show that the Hankel matrices can have exponentially large condition numbers.

2. For m from 37 to 41, the first 22 singular values of H_m are larger than 1, and the rest singular values of H_m are smaller than 10^{-10}. Therefore if we set $\zeta \le 5$, $\epsilon = 10^{-10}$, according to the criterion (24), the algorithm will terminate wrongly and return $t = 22$. However, if we continue to $m = 42$, the Hankel matrix H_{42} has 23 singular values larger than 1, which does not satisfy the criterion (24).

3. For this example, we have

   $$\Delta(\omega^{e_1}, \ldots, \omega^{e_t}) = \frac{1}{82}.$$

   For any $m \ge 76$, the first 61 singular values of H_m are larger than 1 while the remaining singular values are smaller than 10^{-13}. Therefore, Algorithm 1 will return $t = 61$ successfully if we set $\zeta > 5$ or $\epsilon = 10^{-13}$.

4. It is noted that the Vandermonde matrices V_m are well-conditioned for $1 \le m \le 41$, with condition numbers being about 1.41. The condition number of V_m increases to $1.9 \cdot 10^9$ when m reaches 61, and then decreases to 1.976 for m going from 62 to 81.

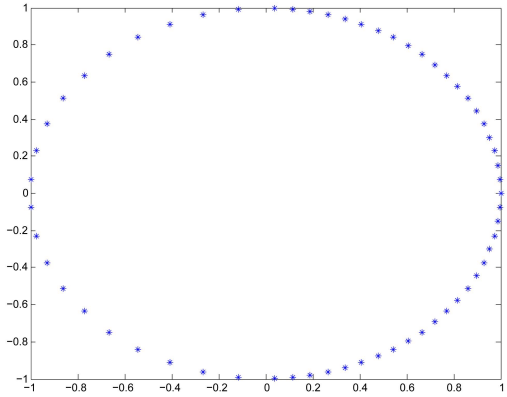

Figure 2: Terms in Example 4.1.

In the following, we will show that with high probability, the algorithm will not terminate before it reaches the sparsity t.

4.1 Kaltofen-Lee Early Termination Revisited

For exact coefficient fields, the probabilistic analysis that checking termination conditions with high probability prevents a sparsity computation where t is smaller than the actual sparsity is due to [11]. The randomized algorithm in [11] is said to terminate early because the number of evaluations is $2t+1$ with high probability, which is the minimum number of evaluations necessary without knowing the sparsity t on input. The setting by Kaltofen and Lee is the multivariate polynomial version by Ben-Or and Tiwari [3] of Prony's algorithm with coefficients from an arbitrary field K. Let

$$f(x_1,\ldots,x_n) = \sum_{j=1}^{t} c_j\, x_1^{e_{j,1}} \cdots x_n^{e_{j,n}}, c_j \in \mathsf{K}, c_j \neq 0 \qquad (31)$$

be a t-sparse polynomial in $\mathsf{K}[x_1,\ldots,x_n]$, let

$$\left.\begin{array}{l} \alpha_i = f(x_1^i,\ldots,x_n^i) \in \mathsf{K}[x_1,\ldots,x_n], i = 1,2,3,\ldots \\ \alpha_0 = c_1 + \cdots + c_t \end{array}\right\} \qquad (32)$$

be the evaluations of f at the i-th powers of a generic point with the j-th component being the variable x_j, and let

$$H_m(h_1,\ldots,h_{2m-1}) = \begin{bmatrix} h_1 & h_2 & \ldots & h_m \\ h_2 & h_3 & \iddots & h_{m+1} \\ h_3 & h_4 & \iddots & h_{m+2} \\ \vdots & \vdots & \iddots & \vdots \\ h_m & h_{m+1} & \ldots & h_{2m-1} \end{bmatrix} \qquad (33)$$

be an $m \times m$ Hankel matrix formed by the entries h_1, ..., h_{2m-1}. Theorem 4 in [11] states that

$$\forall m, 1 \leq m \leq t\colon \det(H_m(\alpha_1,\ldots,\alpha_{2m-1})) \neq 0.$$

One always has $\det(H_{m'}(\alpha_1,\ldots,\alpha_{2m'-1})) = 0$ for all $m' \geq t+1$. Thus, by the DeMillo-Lipton/Schwartz/Zippel Lemma, by substituting field elements $\omega_j \in S \subseteq \mathsf{K}$ that are uniformly and randomly chosen from the finite set S one has with probability

$$\geq 1 - \left(t^3 + \frac{3}{2}\,t^2 + \frac{1}{2}\,t\right) \deg(f)\, \frac{1}{3\,|S|} \qquad (34)$$

($|S|$ denoting the number of elements in S) that the determinants of $H_m(a_1,\ldots,a_{2m-1}) \neq 0$ for $a_i = \alpha_i(\omega_1,\ldots,\omega_n)$ and all m with $1 \leq m \leq t$ [11, Theorem 5]. Therefore, the first singular Hankel matrix that appears has with high probability dimension $(t+1)\times(t+1)$, yielding the sparsity t. The entire sequence of determinants $(\det(H_m(a_1,...,a_{2m-1}))_{1\leq m\leq t+1}$ can be computed one after another from the sequence a_1,a_2, a_3, ... by the fraction-free Berlekamp/Massey Algorithm [7, 14] in a total of $O(t^2)$ arithmetic operations. We recall that in our numerical Algorithm 1 above the termination criterion is that singular values are separated into those $> 1-\epsilon$ and those $< \epsilon$ and none in between in a matrix $H_{m+\zeta}$ that has 2ζ additional evaluations for each m.

Our univariate algorithm with floating point arithmetic above and the multivariate Ben-Or and Tiwari Algorithm with exact scalar arithmetic start the sequence at $(\omega_1^0, \ldots, \omega_n^0) = (1,1,\ldots,1)$, in which case $H_1(\alpha_0) = c_1 + \cdots + c_t$ can be $= 0$. If the coefficient field K has characteristic $= 2$, then for $c_1 = \cdots = c_t = 1$ one has for all m with $0 \leq m \leq t-1$ and $t-m$ an odd integer that $\det(H_m(\alpha_0,\ldots,\alpha_{2m-2})) = 0$ (see Appendix Section 6). That fact shows that the shift in [11] starting at α_1 is necessary to have all H_m with $m \geq 2$ non-singular, for coefficient fields of characteristic $= 2$.

It also follows from the Proof of Theorem 4 in [11] (see (46) below) that for coefficient fields K of any characteristic we have

$$\forall m, 1\leq m\leq t-1\colon \left\{\begin{array}{l} \det(H_m(\alpha_0,...,\alpha_{2m-2}))\neq 0 \\ \text{and/or} \\ \det(H_{m+1}(\alpha_0,...,\alpha_{2m}))\neq 0. \end{array}\right\} \qquad (35)$$

Therefore, if one stops when one has encountered $\zeta = 2$ consecutive singular Hankel matrices, the upper bound on the probability of premature failure can be reduced at the cost of 2 additional evaluations.

For coefficient fields K of characteristic $\neq 2$ we can improve Theorem 4 in [11] unconditionally, giving a positive answer to the question raised in Footnote 2 in [11, Proof of Theorem 4].

Theorem 4.1. *Let K be a field of characteristic $\neq 2$, let α_i be as in (32) and let H_m be as in (33). Then*

$$\left.\begin{array}{l} \det(H_1(\alpha_0)) = c_1 + \cdots + c_t, \\ \det(H_m(\alpha_0,\ldots,\alpha_{2m-2})) \neq 0 \text{ for all } 2 \leq m \leq t. \end{array}\right\} \qquad (36)$$

Proof. Our proof gives a finer analysis of the term structure in the expansion of the formula for $\det(H_m(\alpha_0,\ldots,\alpha_{2m-2}))$ given in [11, cf. Equ. (9)] (see also (2) above). Let $J = \{1,2,\ldots,t\}$, let

$$F(y_1,\ldots,y_t) = \sum_{\{j_1,\ldots,j_m\}\subseteq J} c_{j_1}\cdots c_{j_m} \prod_{1\leq v<u\leq m} (y_{j_u} - y_{j_v})^2 \in \mathsf{K}[y_1,\ldots,y_t], \qquad (37)$$

and let $\beta_j = x_1^{e_{j,1}} \cdots x_n^{e_{j,n}}$ be the j-th term in (31). Then we have

$$\det(H_m(\alpha_0,\ldots,\alpha_{2m-2})) = F(\beta_1,\ldots,\beta_t). \qquad (38)$$

There are $\binom{t}{m}$ summands in (37) and each product in (37) has $\binom{m}{2}$ squared factors.

We will use admissible total term orders on both $\mathsf{K}[x_1,\ldots,x_n]$ for the terms in $F(\beta_1,\ldots,\beta_t)$ and on $\mathsf{K}[y_1,\ldots,y_t]$ for the terms in $F(y_1,\ldots,y_t)$ and denote them by $\succeq x$ and $\succeq y$, respectively. We write $\succ x$ and $\succ y$ when the terms are strictly in order, that is, in order and not equal. The term orders can be pure lexicographical term orders. Note that all terms

in F in (37), if $F \neq 0$, have total degree $2\binom{m}{2} = m(m-1)$ in $y_1, \ldots, y_t$. We order the terms β_j in f in (31) as

$$\beta_1 \succ_x \beta_2 \succ_x \ldots \succ_x \beta_t \tag{39}$$

and the variables y_j as

$$y_1 \succ_y y_2 \succ_y \cdots \succ_y y_t. \tag{40}$$

The leading term with respect to the term order $\succeq y$ among all terms in all products $\prod_{1\le v<u\le m}(y_{j_u} - y_{j_v})^2$ in (37) is

$$M_1 = y_1^{2m-2} y_2^{2m-4} \cdots y_{m-2}^4 y_{m-1}^2 \in \mathsf{K}[y_1, \ldots, y_t], \tag{41}$$

which we will prove below. We shall consider a third, partial order $\sqsupseteq y$ on the terms $\in \mathsf{K}[y_1, \ldots, y_t]$ of F:

Definition 4.1. *Let $M \in \mathsf{K}[y_1, \ldots, y_t]$ be a term of degree $D = m(m-1)$. By* vlist(M) *we denote the list of factors that are variables in order sorted with respect to (40):*

$$\text{vlist}(M) \stackrel{\text{def}}{=} [\underbrace{y_{j_1}, \ldots, y_{j_1}}_{e_1 \text{ times}}, \ldots, \underbrace{y_{j_k}, \ldots, y_{j_k}}_{e_k \text{ times}}]$$
$$\text{for } M = y_{j_1}^{e_1} \cdots y_{j_k}^{e_k}, e_1 \ge 1, \ldots, e_k \ge 1, j_1 < j_2 < \cdots < j_k.$$

By vlist$(M)[\ell]$ *we denote the ℓ-th component in the list, which is a variable y_η, $j_1 \le \eta \le j_k$. Now let M' be another term in $\mathsf{K}[y_1, \ldots, y_t]$ of degree D. We define*

$$\begin{aligned} &M \sqsupseteq y\ M' \\ &\stackrel{\text{def}}{\Longleftrightarrow} \forall \ell, 1 \le \ell \le D\colon \eta \le \eta' \text{ for } \left\{ \begin{array}{l} y_\eta = \text{vlist}(M)[\ell], \\ y_{\eta'} = \text{vlist}(M')[\ell] \end{array} \right\} \\ &\Longleftrightarrow \forall \ell, 1 \le \ell \le D\colon \text{vlist}(M)[\ell] \succeq y\ \text{vlist}(M')[\ell]. \end{aligned} \tag{42}$$

We write $M \sqsupset y\ M' \stackrel{\text{def}}{\Longleftrightarrow} M \sqsupseteq y\ M'$ and $M \neq M'$, which means that in (42) vlist$(M)[\ell] \succ y$ vlist$(M')[\ell]$ *for at least one index ℓ. We have*

$$\begin{aligned} &M \not\sqsupseteq y\ M' \\ &\Longleftrightarrow \exists \ell, 1 \le \ell \le D : \text{vlist}(M')[\ell] \succ y\ \text{vlist}(M)[\ell]. \end{aligned} \tag{43}$$

Note that $\sqsupset y$ is a (strict) partial order: for $M = y_1^4 y_3^2$ and $M' = y_1^2 y_2^4 \neq M$ we have both $M \not\sqsupset y\ M'$ and $M' \not\sqsupset y\ M$. We first claim that

$$M \sqsupset y\ M' \Longrightarrow M(\beta_1, \ldots, \beta_t) \succ_x M'(\beta_1, \ldots \beta_t). \tag{44}$$

The strict order (44) of the evaluated terms is a consequence of the (39), (40), definition (42) and the admissibility property of $\succeq x$: for terms β, β', γ, γ' in $\mathsf{K}[x_1, \ldots, x_n]$ we have $\beta \succeq x\ \beta'$ and $\gamma \succeq x\ \gamma' \Longrightarrow \beta\gamma \succeq x\ \beta'\gamma'$ with $\beta\gamma \succ x\ \beta'\gamma'$ if $\beta \succ x\ \beta'$ and/or $\gamma \succ x\ \gamma'$.

Now let $M \in \mathsf{K}[y_1, \ldots, y_t]$ be any term in any of the products $\prod_{1\le v<u\le m}(y_{j_u} - y_{j_v})^2$ in (37). For the term M_1 in (41) we have

$$M_1 \sqsupseteq y\ M \text{ for all such terms } M. \tag{45}$$

The reason is the following: for $\mu = 1, 2, \ldots, m-1$, the largest position index $\ell_\mu^{[\max]}$ that y_μ can reach in vlist(M) is $\ell_\mu^{[\max]} = 2(m-1) + 2(m-2) + \cdots + 2(m-\mu)$, because the maximum total degree in $y_1, \ldots, y_\mu$ in M is $= \ell_\mu^{[\max]}$: there are least $2\binom{m-\mu}{2} = (m-\mu)(m-\mu-1)$ factors $(y_{j_u} - y_{j_v})$ with $j_u > \mu$ and $j_v > \mu$ whose variables contribute to M a total degree $\ge (m-\mu)(m-\mu-1)$, so the maximum total degree in $y_1, \ldots, y_\mu$ is $\le m(m-1) - (m-\mu)(m-\mu-1) = \ell_\mu^{[\max]}$. Those maxima are achieved for all μ in vlist(M_1). In particular, y_μ appears first at position $\ell_{\mu-1}^{[\max]} + 1$ in vlist(M_1). Suppose now that $M_1 \not\sqsupseteq y\ M \Longleftrightarrow$ there exists an ℓ with $1 \le \ell \le D$ and vlist$(M)[\ell] \succ y$ vlist$(M_1)[\ell]$ (see (42)), meaning $\mu' \le \mu - 1$ for $y_{\mu'} =$ vlist$(M)[\ell]$ and $y_\mu =$ vlist$(M_1)[\ell]$. For y_μ in vlist(M_1) we have $\ell > \ell_{\mu-1}^{[\max]}$. This means that $y_{\mu'}$ is in a position $> \ell_{\mu-1}^{[\max]}$ in vlist(M), for which $\mu' \le \mu - 1$ is too small to be reachable, which proves (45).

From (44) and (45) we conclude that for all $M \neq M_1$ we have $M_1(\beta_1, \ldots, \beta_t) \succ_x M(\beta_1, \ldots, \beta_t)$, which in [11, 1] was argued directly. Our argument here is more detailed and will be used again below. Next we observe that the term M_1 in (41) occurs in (37) precisely in the products $\prod_{1\le v<u\le m}(y_{j_u} - y_{j_v})^2$ for all $\{j_1, \ldots, j_m\} = \{1, \ldots, m-1, \tau\}$ with $\tau = m, m+1, \ldots, t$. Therefore we have the expansion

$$\begin{aligned} F(\beta_1, \ldots, \beta_t) = c_1 \cdots c_{m-1} \Big(\sum_{\tau=m}^{t} c_\tau \Big)\ M_1(\beta_1, \ldots, \beta_t) \\ + \text{lower order terms in } x_1, \ldots, x_n. \end{aligned}$$

Thus we conclude from (38) and $c_j \neq 0$ that

$$\Big(\sum_{\tau=m}^{t} c_\tau \Big) \neq 0 \Longrightarrow \det(H_m(\alpha_0, \ldots, \alpha_{2m-2})) \neq 0 \tag{46}$$

(see [1, Remark 4.2]). Two consecutive sums $\sum_{\tau=m}^{t} c_\tau$ and $\sum_{\tau=m+1}^{t} c_\tau$ cannot both be $= 0$, for then $c_m = 0$, which implies (35) above.

Now suppose that $(\sum_{\tau=m}^{t} c_\tau) = 0$ for $2 \le m \le t$. We then consider the second highest term with respect to the order $\succ y$ in the expansion of (37), namely,

$$M_2 = y_1^{2m-2} y_2^{2m-4} \cdots y_{m-2}^4 y_{m-1} y_m \in \mathsf{K}[y_1, \ldots, y_t]. \tag{47}$$

The term has variables $y_1, \ldots, y_m$ and therefore occurs in only one product, namely, $\prod_{1\le v<u\le m}(y_{j_u} - y_{j_v})^2$ with $\{j_1, \ldots, j_m\} = \{1, \ldots, m\}$, and there with coefficient -2, and thus in (37) has a coefficient $-2c_1 \cdots c_m$. We shall prove that $(\sum_{\tau=m}^{t} c_\tau) = 0$ implies that the term $M_2(\beta_1, \ldots, \beta_t) \in \mathsf{K}[x_1, \ldots, x_n]$ in the expansion of (38) has the same coefficient.

By (44), all terms $M \in \mathsf{K}[y_1, \ldots, y_t]$ in (37) with $M_2 \sqsupset y\ M$ have $M_2(\beta_1, \ldots, \beta_t) \succ_x M(\beta_1, \ldots, \beta_t)$ and therefore cannot additively contribute to the coefficient of $M_2(\beta_1, \ldots, \beta_t)$ in the expansion (38). All remaining terms satisfy $M_2 \not\sqsupseteq y\ M$ (M_1 is such a term). Now let M be a term in (37) with $M_2 \not\sqsupseteq y\ M$. We have for all ℓ with $1 \le \ell \le D-1$ that vlist$(M_2)[\ell] =$ vlist$(M_1)[\ell] \succeq y$ vlist$(M)[\ell]$, the latter being true by (45). Therefore, $M_2 \not\sqsupseteq y\ M$ implies that vlist$(M)[D] = y_{m-1}$, because no y_μ with $\mu \le m-2$ can reach position $D > \ell_{m-2}^{[\max]} \ge \ell_\mu^{[\max]}$ and we must by (43) have vlist$(M)[D] \succ y$ vlist$(M_2)[D] = y_m$.

We finally show that all terms M with $M_2 \not\sqsupseteq y\ M$ have a coefficient $= 0$ in (37). In the previous paragraph we have shown that vlist$(M)[D] = y_{m-1}$. We claim that M can only occur in products $\prod_{1\le v<u\le m}(y_{j_u} - y_{j_v})^2$ with $\{j_1, \ldots, j_m\} = \{1, \ldots, m-1, \tau\}$ and $m \le \tau \le t$. For suppose the set $\{j_1, \ldots, j_m\}$ contains two τ, τ' with $m \le \tau \le t$ and $\tau < \tau' \le t$. Then the product $\prod_{1\le v<u\le m}(y_{j_u} - y_{j_v})^2$ has a factor $(y_\tau - y_{\tau'})^2$, so the total degree in the variables $y_1, \ldots, y_{m-1}$ of each term M in the expansion of that product is $< m(m-$

1), which implies that y_{m-1} cannot reach position D in vlist(M). Now suppose that a term M with $M_2 \not\equiv_y M$ occurs in a product $\prod_{1\le v<u\le m}(y_{j_u}-y_{j_v})^2$ with $\{j_1,\ldots,j_m\} = \{1,\ldots,m-1,\tau\}$ for at least one τ with $m \le \tau \le t$ (otherwise it cannot occur in the full expansion of (37) at all). Then M occurs in those products for all τ with $m \le \tau \le t$, there with the same coefficient a_M (by setting $y_\tau = 0$ in all products) and therefore in the expansion of (37) with coefficient $a_M c_1 \cdots c_{m-1}(\sum_{\tau=m}^t c_\tau) = 0$, the "$= 0$" by our assumption that $(\sum_{\tau=m}^t c_\tau) = 0$.

Therefore, the only non-zero scalar coefficient for the term $M_2(\beta_1,\ldots,\beta_t)$ in (38) can come from M_2 in (37), which as argued above has a coefficient $-2c_1\cdots c_m$, which is $\neq 0$ because $c_j \neq 0$ and the the field is of characteristic $\neq 2$. We conclude that for all m and t with $2 \le m \le t$ we have $(\sum_{\tau=m}^t c_\tau) = 0 \Longrightarrow \det(H_m(\alpha_0,\ldots,\alpha_{2m-2})) \neq 0$, which together with (46) proves Theorem 4.1. □

Theorem 4.1 yields a slightly better estimate on the early termination success probability than (34) for fields of characteristic $\neq 2$, namely,

$$\ge 1 - (t^3 - t + 3)\deg(f)\frac{1}{3|S|} \tag{48}$$

after $2t+1$ evaluations. The estimate (48) includes testing if $a_1 = f(\omega_1,\ldots,\omega_n)$ is $= 0$ first, in which case f is with high probability the zero polynomial ($t = 0$). If the test fails, our algorithm computes $a_0 = f(1,\ldots,1)$ and $a_2 = f(\omega_1^2,\ldots,\omega_n^2)$ and tests $\det(H_2(a_0,a_1,a_2)) = 0$ next. We do this so that the comparison to (34) is proper, where the zero polynomial is returned after a single evaluation by terminating at $\det(H_1(a_1)) = 0$, as does ours now.

Remark 4.1. Theorem 4.1 remains valid if some $e_{j,\nu}$ in (31) are negative integers. Then $f \in \mathsf{K}[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$, the ring of Laurent polynomials in $x_1,\ldots,x_n$. In our probability estimate (48) with $0 \notin S$ one then can use

$$\deg(f) = \max_{1\le j\le t}(\textstyle\sum_{\nu=1}^n e_{j,\nu}) - \sum_{\nu=1}^n \min_{1\le j\le t}(e_{j,\nu}).$$

Note that for a regular polynomial f that notion of degree is actually smaller than the total degree of f if a variable x_ν divides f. □

Acknowledgement: The ideas of this paper were originally conceived at the Fields Institute in Toronto during our stay during the Major Program in Computer Algebra. We also thank Wen-Shin Lee for her helpful comments.

5. REFERENCES

[1] A. Arnold and E. L. Kaltofen. Error-correcting sparse interpolation in the Chebyshev basis. In *ISSAC'15 Proc. 2015 ACM Internat. Symp. Symbolic Algebraic Comput.*, pages 21–28, New York, N. Y., 2015. ACM. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/15/ArKa15.pdf.

[2] B. Beckermann, G. Golub, and G. Labahn. On the numerical condition of a generalized hankel eigenvalue problem. *Numerische Mathematik*, 106(1):41–68, 2007.

[3] M. Ben-Or and P. Tiwari. A deterministic algorithm for sparse multivariate polynomial interpolation. In *Proc. Twentieth Annual ACM Symp. Theory Comput.*, pages 301–309, New York, N.Y., 1988. ACM Press.

[4] E. J. Candès and C. Fernandez-Granda. Super-resolution from noisy data. *Journal of Fourier Analysis and Applications*, 19(6):1229–1254, 2013.

[5] E. J. Candés and C. Fernandez-Granda. Towards a mathematical theory of super-resolution. *Communications on Pure and Applied Mathematics*, 67(6):906–956, 2014.

[6] A. Cuyt and W.-s. Lee. Sparse interpolation and rational approximation. *Contemporary Mathematics, American Mathematical Society*, 2015.

[7] M. Giesbrecht, E. Kaltofen, and W.-s. Lee. Algorithms for computing the sparsest shifts for polynomials via the Berlekamp/Massey algorithm. In T. Mora, editor, *Proc. 2002 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'02)*, pages 101–108, New York, N. Y., 2002. ACM Press. Journal version in [8]. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/02/GKL02.pdf.

[8] M. Giesbrecht, E. Kaltofen, and W.-s. Lee. Algorithms for computing sparsest shifts of polynomials in power, Chebychev, and Pochhammer bases. *J. Symbolic Comput.*, 36(3–4):401–424, 2003. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/03/GKL03.pdf.

[9] M. Giesbrecht, G. Labahn, and W.-s. Lee. Symbolic-numeric sparse interpolation of multivariate polynomials. *Journal of Symbolic Computation*, 44(8):943 – 959, 2009.

[10] G. H. Golub and C. F. Van Loan. *Matrix Computations*. Johns Hopkins University Press, Baltimore, MD, USA, 1996.

[11] E. Kaltofen and W.-s. Lee. Early termination in sparse interpolation algorithms. *J. Symbolic Comput.*, 36(3–4):365–400, 2003. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/03/KL03.pdf.

[12] E. Kaltofen, W.-s. Lee, and Z. Yang. Fast estimates of Hankel matrix condition numbers and numeric sparse interpolation. In M. Moreno Maza, editor, *SNC'11 Proc. 2011 Internat. Workshop on Symbolic-Numeric Comput.*, pages 130–136, New York, N. Y., June 2011. ACM. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/11/KLY11.pdf.

[13] E. Kaltofen, Z. Yang, and L. Zhi. On probabilistic analysis of randomization in hybrid symbolic-numeric algorithms. In J. Verschelde and S. M. Watt, editors, *SNC'07 Proc. 2007 Internat. Workshop on Symbolic-Numeric Comput.*, pages 11–17, New York, N. Y., 2007. ACM Press. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/07/KYZ07.pdf.

[14] E. Kaltofen and G. Yuhasz. A fraction free matrix Berlekamp/Massey algorithm. *Linear Algebra and Applications*, 439(9):2515–2526, Nov. 2013. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/08/KaYu08.pdf.

[15] W. Liao and A. Fannjiang. MUSIC for single-snapshot spectral estimation: Stability and super-resolution. *Applied and Computational Harmonic Analysis*, 40(1):33 – 67, 2016.

[16] L. Mirsky. Symmetric gauge functions and unitarily invariant norms. *The Quarterly Journal of Mathematics*, 11(1):50–59, 1960.

[17] A. Moitra. Super-resolution, extremal functions and the condition number of vandermonde matrices. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, STOC '15, pages 821–830, New York, NY, USA, 2015. ACM.

[18] D. Slepian. Prolate spheroidal wave functions, Fourier analysis, and uncertainty— V: The discrete case. *Bell System Technical Journal*, 57(5):1371–1430, 1978.

[19] J. Stoer and R. Bulirsch. *Introduction to Numerical Analysis (3rd ed.)*. Springer-Verlag New York, 2002.

[20] H. Weyl. Das asymptotische Verteilungsgesetz der Eigenwerte linearer partieller Differentialgleichungen (mit einer Anwendung auf die Theorie der Hohlraumstrahlung). *Mathematische Annalen*, 71(4):441–479, 1912.

6. APPENDIX: CHARACTERISTIC = 2

If the coefficient field K has characteristic $= 2$, $c_1 = \cdots = c_t = 1$ and $t - m$ is an odd number, then

$$\prod_{1\le v<u\le m}(\beta_{j_v} - \beta_{j_u})^2 = \prod_{1\le v<u\le m}(\beta_{j_v}^2 - \beta_{j_u}^2), \tag{49}$$

which can be viewed as the determinant of the Vandermonde matrix V generated by $\beta_{j_1}^2,\ldots,\beta_{j_m}^2$. Then each term in the expansion of (49) must be a product of elements selected from every column of V. Therefore by (37) and (38), each term in $\det(H_m(\alpha_0,\ldots,\alpha_{2m-2}))$ has the form $M = \beta_{j_1}^{2m-2}\cdot\beta_{j_2}^{2m-4}\cdots\beta_{j_{m-1}}^2$. Let $S = \{1,\ldots,t\}\setminus\{j_1,\ldots,j_{m-1}\}$, then the coefficient of M is $c_{j_1}\cdots c_{j_{m-1}}\cdot\sum_{j_m\in S} c_{j_m} = 0$ for S having an even number of elements. Therefore, we have $\det(H_m(\alpha_0,\ldots,\alpha_{2m-2})) = 0$. □