Sparse Polynomial Interpolation With Error Correction: Higher Error Capacity by Randomization

Erich L. Kaltofen
NCSU and Duke University
Raleigh, Durham, North Carolina, USA
kaltofen@ncsu.edu

Zhi-Hong Yang
School of Math. and Statistics, Central South Univ.
Changsha, Hunan, China
yangzhihong@csu.edu.cn

ABSTRACT

In [IEEE Trans. Information Theory, vol. 67, nr. 1 (2021)] we have presented error-correcting algorithms that interpolate sparse univariate polynomials from values at arguments which the algorithms compute. We have assumed that the input polynomials are sparse in terms that are powers of the variable (standard basis) or sparse in Chebyshev basis polynomials. We recover all polynomials of sparsity $\le B$ that from our N input points interpolate at least $N - E$ of the points, that is, correct $\le E$ errors in the values at the error capacity E/N. Our IEEE Transactions algorithms have, roughly, an error capacity of $0.75/B$ for power basis and $0.66/B$ for Chebyshev basis.

We present algorithms which randomly select values from sufficiently large finite sets before evaluation, and then return the sparse interpolant in a list of valid interpolants with high probability. The error capacity of our algorithms for both power and Chebyshev bases is, roughly, $1/B$. More precisely, we recover the interpolant from $N = \lfloor E/2 + 1 \rfloor (2B + 1)$ values with probability $\ge 1 - \epsilon$ when sampling from sets that have $\ge 16 \lfloor E/2 + 1 \rfloor DB^2/\epsilon$ elements, where D is an upper bound on the degree of the polynomial. Our algorithms are based on Prony's interpolation algorithm and perform exact arithmetic in the field of scalars, which for Chebyshev basis is required to have characteristic $\neq 2$. The running time is polynomial in the bounds B, E and D or $\log(D)$, depending on the representation of the scalar field elements.

In the special case of evaluations at positive real numbers, as a consequence of Descartes's Rule of Signs, our algorithms recover a unique real interpolant for $B, E \ge 2$, and for sparsity in both standard and Chebyshev bases can be de-randomized to deterministic versions.

CCS CONCEPTS

• **Mathematics of computing → Interpolation**.

KEYWORDS

sparse model fitting; outlier error correction; orthogonal polynomial basis; Prony interpolation algorithm;

ACM Reference Format:
Erich L. Kaltofen and Zhi-Hong Yang. 2024. Sparse Polynomial Interpolation With Error Correction: Higher Error Capacity by Randomization . In *International Symposium on Symbolic and Algebraic Computation (ISSAC '24), July 16–19, 2024, Raleigh, NC, USA.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3666000.3669698

1. INTRODUCTION

When interpolating a univariate polynomial or Laurent polynomial

$$f(x) = \sum_{j=1}^{t} c_j \mathcal{P}_{\delta_j}(x), \delta_1 < \cdots < \delta_t = \deg(f),\ \forall j\colon c_j \neq 0. \quad (1)$$

represented in a polynomial basis $(\mathcal{P}_n(x))_{n\in\mathbb{Z}}$, the sparsity $t \ll \deg(f)$ has been exploited—since de Prony and BCH decoding—for reconstructing f from fewer than $\deg(f)+1$ values. Here we use two bases: the standard power basis $\mathcal{P}_n(x) = x^n$ for $n \in \mathbb{Z}$ and Chebyshev polynomials of the First Kind $\mathcal{P}_n(x) = T_n(x)$ for $n \in \mathbb{Z}_{\ge 0}$. Interpolation algorithms that correct errors in the values by oversampling constitute algebraic error correcting codes, starting with the Reed-Solomon code. Here we consider both problems: reducing the number of interpolation points for sparse polynomials while correcting errors in the points.

Table 1 summarizes the progress on the accepted error capacities of known sparse univariate interpolation algorithms: if the rate $= R$, one can interpolate with N points while correcting $\le RN$ errors. The larger the rate, the more errors can be tolerated. Unlike Reed-Solomon decoding, where a maximum error rate of $1/2 - \epsilon$ is acceptable for any $\epsilon > 0$, in sparse interpolation the best maximum error rate is $\approx 1/(4t)$. In [15] we give two t-sparse polynomials in power basis that fit $N = (2E + 1)2t - 1$ complex points with E errors, which makes the algorithm in Table 1, Entry 1 optimal. Note that the maximum rate is far worse than Reed-Solomon's decoder, but in sparse interpolation the number of points N is independent of the degree (see Table 1) and therefore one may interpolate from far fewer points. The actual running time of the sparse interpolation algorithms can be reduced to be polynomial in $\log(\deg f)$. As the Reed-Solomon error rate was pushed beyond 1/2 by list-decoding by Guruswami and Sudan, so was the error rate increased for sparse list-interpolation: a list of valid interpolants that fit $\ge N - E$ points is computed, if existent, but the list can have multiple entries (Table 1, Entries 2.–5.).

List-interpolation algorithms are required to run in polynomial-time. In exponential time it may be possible to try all $\binom{N}{E}$ error locations and fit the remaining $N - E$ points.

ISSAC '24, July 16–19, 2024, Raleigh, NC, USA

ACM ISBN 979-8-4007-0696-7/24/07.
https://doi.org/10.1145/3666000.3669698

		Standard Power Basis	Chebyshev Basis
1.	Comer, Kaltofen and Pernet [4]	$N = (2E+1)2B, R \approx 0.25/B$ (unique interpolant; see text about optimality)	—
2.	Kaltofen and Pernet [15]	$N = (E+1)2B - 1, R \approx 0.5/B$ $N = 74, R{\approx}0.67/B$ for $B{=}5, E{=}10$	—
3.	Arnold and Kaltofen [1]	—	$N = 74\lfloor \frac{E}{13} + 1 \rfloor, R \approx 0.52/B$ for $B = 3, E \geq 222$
4.	Kaltofen and Yang, Z.-H. [16]	$N = \lfloor \frac{4}{3}E + 2 \rfloor B, R \approx 0.75/B$	$N = \lfloor \frac{3}{2}E + 2 \rfloor B, R \approx 0.66/B$
5.	*This paper* [2024]	$N{=}\lfloor E/2+1 \rfloor(2B+1), R{\approx}1/B$ (randomized algorithm; deterministic in certain settings: see text)	

Table 1: Interpolation Algo's: $\leq B$ terms, $\leq E$ errors, N evaluations, max. error rate $R{=}\frac{E}{N}$

Our algorithms have polynomial running time under the assumptions of Prony interpolation, which computes polynomial roots which are the values of the terms of the sparse interpolant, and then computes from the term values the degrees of the terms. As a consequence, our randomized algorithms produce $O(EB^3)$ candidate sparse interpolants. The upper bound B for the number of terms is an input to our algorithms.[1] The model of randomization is Monte Carlo: a sparse interpolant that fits the points except at $\leq E$ values is in the list with controllably high probability. However, we no longer can guarantee that for the randomly chosen arguments the number of interpolants with $\leq E$ errors is $(EB)^{O(1)}$. The reason is that if an interpolant is placed in the list, others may be omitted at the same arguments with probability 1.

A special case is when the field of coefficients $\mathsf{K} \subseteq \mathbb{R}$ and the arguments to the interpolant are real numbers > 0. By [15, Theorem 4] and [1, Corollary 2.4] if $N \geq 2B + 2E$ there exists at most one valid interpolant, which our algorithms can compute deterministically for both power basis and Chebyshev basis in polynomial time from $N = \lfloor E/2 + 1 \rfloor(2B + 1) \geq 2B + 2E$ points for all $B \geq 2$ and $E \geq 2$. We note that for $E = 1$ we list-interpolate sparse candidate polynomials from $2B+1 < 2B+2$ values. Uniqueness is no longer guaranteed: for example, for $B = 2$ terms the two interpolants $f_1(x) = x^3 + 56x$ and $f_2(x) = 14x^2 + 64$ with $f_1(x) - f_2(x) = (x-2)(x-4)(x-8)$ both fit the first three values for the arguments $x = 2, 4, 8$ and can each have 1 error in the two values for $x = 16, 32$.

Our algorithms can correct errors when the scalar field is a finite field. In certain settings the Prony algorithms can then be implemented to run in polynomial time in $\log(D)$ for a degree upper bound D [12].[2] Our algorithms also can use complex roots of unity as arguments, which keeps the values small in absolute value and is used for purpose of numerical stability [6].

Our method follows that in [16]: we first show how to correct 1 error with one extra value, namely, $N = 2B + 1$. Therefore, in $\lfloor E/2 + 1 \rfloor$ blocks of $2B + 1$ values, in the presence of $\leq E$ errors not all blocks can have ≥ 2 errors and the list-interpolation algorithm will compute the interpolant from the block with ≤ 1 error with high probability. Additional solutions can be verified for all values. Note that if E is even, the last block can be shortened to $2B$ values. As in [16] we place a variable for the value at all the possible $2B + 1$ erroneous locations in a block. By Prony's property, the term locator polynomial produces a column relation in the corresponding $(2B + 1) \times (2B + 1)$ Hankel matrix. If the determinant is $\neq 0$ for the symbolic error, one can solve the polynomial equation for the correct value. We can prove, in the standard basis case, that for random arguments all determinants are non-zero with high probability by the early termination technique in [14].

Sparse interpolation in Chebyshev basis begins with [17]. Chebyshev polynomials via the property $T_n(\cos(\xi)) = \cos(n\xi)$ yield periodic sinusoid functions and sparse sums are important in signal processing. The functions are essentially Laurent polynomials in the reciprocal terms $y^\delta + \frac{1}{y^\delta}$ [1, Section 4] (see also (24) below). The symmetry can cause restrictions in the transfer of power basis techniques, for example in the early termination theorems [14, Theorem 11], [1, Theorem 4.3] and the maximum rates in interpolation with error correction [Table 1, Entries 3 and 4]. Here we deploy a technique that gives us matching computational complexities for standard and Chebyshev bases: we add a symbolic error to the correct value (Theorem 3.1) and prove the resulting determinant to be $\neq 0$ by proving that the coefficient of the linear term is $\neq 0$, with high probability. The technique also yields the derandomization result when evaluating a polynomial with real number coefficients at real arguments > 0, which is specific to error correction and does not apply to early termination. See also Remark 5.2.

By the techniques in [11], our results transfer to Chebyshev polynomials of the second–fourth kind and related recursively defined polynomial bases. In [13, Section 5.3] we give algorithms for sparse polynomial Hermite interpolation including error correction, to which our improvements here can be applied.

Notation. We shall write $\tau \times \tau$ Hankel matrices as follows: $\mathrm{Hankel}_\tau(a_{i_0+is} : i{=}0, \ldots, 2\tau{-}2) =$

$$\begin{bmatrix} a_{i_0} & a_{i_0+s} & \cdots & a_{i_0+(\tau-1)s} \\ a_{i_0+s} & a_{i_0+2s} & \iddots & a_{i_0+\tau s} \\ \vdots & \iddots & \iddots & \vdots \\ a_{i_0+(\tau-1)s} & a_{i_0+\tau s} & \cdots & a_{i_0+(2\tau-2)s} \end{bmatrix}. \tag{2}$$

2. STANDARD POWER BASIS

Let K be a field and $f(x) \in \mathsf{K}[x, \frac{1}{x}]$ be a sparse univariate Laurent polynomial:

[1] In the literature the letter $T \geq t$ is sometimes used for the bound. Here T_n denote the Chebyshev polynomials.

[2] Note that there are more $(\log D)^{O(1)}$-time algorithms but they use $O(B)$ evaluations. See [7] and the literature cited there.

$$f(x) = \sum\nolimits_{j=1}^{t} c_j x^{\delta_j},\ \delta_1 < \delta_2 < \cdots < \delta_t = \deg(f),$$
$$\forall j, 1 \le j \le t : c_j \ne 0. \quad (3)$$

We assume that f can be sampled at arguments $\in \mathsf{K}$, e.g., with a black box for f; the values can be erroneous. This section is to show how to Prony-list-interpolate f from $2t{+}1$ evaluations when no more than one of the evaluations is erroneous. Let $\hat{a}_i$ be the output of the black box at the input argument ω^i for $\omega \in \mathsf{K}$ and $1 \le i \le 2t+1$. We assume that there is at most one index $\mu \in \{1, 2, \ldots, 2t+1\}$ such that $\hat{a}_\mu \ne f(\omega^\mu)$.

Let $a_i = f(\omega^i)$ for $i \ge 1$, and H_τ be the Hankel matrix with entries $(a_1, \ldots, a_{2\tau-1})$:

$$H_\tau{=}\mathrm{Hankel}_\tau(a_{1+i}\colon i{=}0,...,2\tau{-}2) \in \mathsf{K}^{\tau\times\tau}, \tau{\ge}1 \text{ (see (2))}. \quad (4)$$

The sequence $(a_1, a_2, \ldots, a_{2t}, \ldots)$ is linearly generated by the term locator polynomial

$$\Lambda(z) = \prod\nolimits_{j=1}^{t} (z - \omega^{\delta_j}). \quad (5)$$

If $\omega^{\delta_i} \ne \omega^{\delta_j}$ for any $i \ne j$, then $\Lambda(z)$ is squarefree and H_t is non-singular and H_{t+1} is singular. We proposed in [16] to correct one error from $3t$ evaluations by replacing the error with a symbol and then solve for the symbol. Here we use the same idea and give a randomized algorithm for correcting one error from $2t+1$ evaluations.

The difficulty is to prove that for all $\mu = 1, \ldots, 2t+1$ the determinants of the new matrices

$$\hat{H}_{t+1,\mu} = \mathrm{Hankel}_{t+1}(a_1, \ldots, a_{\mu-1}, \hat{\alpha}, a_{\mu+1}, \ldots, a_{2t+1}) \quad (6)$$

are non-zero with high probability. Then the correct value can be computed from the equation $\det(\hat{H}_{t+1,\mu}) = 0$.[3] The determinant of $\hat{H}_{t+1,\mu}$ depends on the choice of the argument ω.

Example 2.1. Let $\mathsf{K} = \mathbb{Z}_{17}$, the integer residues modulo 17, $t = 3$, and $f = 1 + 6x + x^6$. Let $a_i = f(\omega^i), i = 1, \ldots, 2t+1$, be the sequence of evaluations of f at the powers of ω.

Case $\omega = 5$: Replacing a_2 by $\hat{\alpha}$ in H_4, we get

$$H_4 = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_6 \\ a_4 & a_5 & a_6 & a_7 \end{bmatrix} = \begin{bmatrix} 16 & 2 & 11 & 10 \\ 2 & 11 & 10 & 15 \\ 11 & 10 & 15 & 9 \\ 10 & 15 & 9 & 2 \end{bmatrix}, \hat{H}_{4,2} = \begin{bmatrix} 16 & \hat{\alpha} & 11 & 10 \\ \hat{\alpha} & 11 & 10 & 15 \\ 11 & 10 & 15 & 9 \\ 10 & 15 & 9 & 2 \end{bmatrix}$$

and $\det(\hat{H}_{4,2}) = 0 \in \mathbb{Z}_{17}$. Therefore, if the value for $f(\omega^2)$ is an error, then we cannot correct this error by solving the equation $\det(\hat{H}_{4,2}) = 0$.

Case $\omega = 3$: Replacing a_2 by $\hat{\alpha}$ in H_4, we get

$$H_4 = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_6 \\ a_4 & a_5 & a_6 & a_7 \end{bmatrix} = \begin{bmatrix} 0 & 8 & 2 & 10 \\ 8 & 2 & 10 & 16 \\ 2 & 10 & 16 & 2 \\ 10 & 16 & 2 & 7 \end{bmatrix}, \hat{H}_{4,2} = \begin{bmatrix} 0 & \hat{\alpha} & 2 & 10 \\ \hat{\alpha} & 2 & 10 & 16 \\ 2 & 10 & 16 & 2 \\ 10 & 16 & 2 & 7 \end{bmatrix}$$

and $\det(\hat{H}_{4,2}) = 11(\hat{\alpha}+9)(\hat{\alpha}+12) \in \mathbb{Z}_{17}[\hat{\alpha}]$. In the case $\omega = 3$, if the error location is $\mu = 2$, then we can compute two candidates for the correct value $a_2 \equiv -9 \equiv 8 = f(\omega^2)$ by solving the equation $\det(\hat{H}_{4,2}) = 0$ in $\mathbb{Z}_{17}$. The Prony algorithm computes f for $a_2 = 8$. □

We prove that there exists a polynomial $\Gamma_f(x) \in \mathsf{K}[x]$, which depends on the coefficients and term degrees of f in (3), such that the following implication holds:

$$\Gamma_f(\omega) \ne 0 \text{ and } \omega^{\delta_1}, \ldots, \omega^{\delta_t} \text{ are pairwise distinct}$$
$$\Longrightarrow \forall\mu, 1 \le \mu \le 2t+1 : \det(\hat{H}_{t+1,\mu}) \ne 0, \quad (7)$$

and we provide a degree bound for Γ_f. The condition in (7) is sufficient for recovering a t-sparse black box polynomial f from $2t{+}1$ evaluations containing at most one error. Therefore, our algorithm would succeed if the argument ω is not a root of Γ_f and ω has order $> \delta_t$ (or $> 2\max\{|\delta_1|, \delta_t\}$ if $\delta_1 < 0$).

The idea is to show that for evaluations at symbolic powers $\omega^i = x^i$, the determinant of the matrix containing $\hat{\alpha}$ is non-zero. Let $\alpha_i = f(x^i)$ be the symbolic evaluations of f at powers x^i and $\mathcal{H}_{t+1}$ be the $(t+1)\times(t+1)$ Hankel matrix:

$$\mathcal{H}_{t+1} = \mathrm{Hankel}_{t+1}(\alpha_{1+i}\colon i{=}0, ..., 2t)$$
$$\in \mathsf{K}[x, 1/x]^{(t+1)\times(t+1)} \text{ (see (2))}. \quad (8)$$

Let $\hat{\mathcal{H}}_{t+1,\mu}$ be the matrix obtained by substituting α_μ with $\alpha_\mu + \hat{\alpha}$ in $\mathcal{H}_{t+1}$, as depicted in (9) for $\hat{\mathcal{H}}_{4,2}$:[4]

$$\hat{\mathcal{H}}_{4,2} = \begin{bmatrix} \alpha_1 & \alpha_2{+}\hat{\alpha} & \alpha_3 & \alpha_4 \\ \alpha_2{+}\hat{\alpha} & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 \\ \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 \end{bmatrix}. \quad (9)$$

Let B be an upper bound on the sparsity of the black box polynomial f (see (3)), and $D \ge |\delta_j|$ for all $1 \le j \le t$. First, if K is any scalar field, we can use the Kaltofen-Lee early termination theorem [14, Theorem 4] to show that the leading coefficient of $\det(\hat{\mathcal{H}}_{t+1,\mu})$ in $\hat{\alpha}$ is non-zero. By taking the product of all leading coefficients of $\det(\hat{\mathcal{H}}_{t+1,\mu}), \mu = 2, \ldots, 2t$ in $\hat{\alpha}$ and clearing all possible denominators, we obtain a polynomial Γ_f of degree bounded by $2B^3D$ such that the implication (7) holds. Consequently, we can correct one error from $2t{+}1$ evaluations by solving the equations $\det(\hat{H}_{t+1,\mu}) = 0$ for all $\mu = 2, \ldots, 2t$. Note that if the error is $\hat{a}_1$ or $\hat{a}_{2t+1}$, we can simply remove the error and recover f from the remaining $2t$ evaluations using Prony's algorithm.

Lemma 2.2. *Assume that all term degrees of $f(x)$ in (3) are non-negative, namely, $0 \le \delta_1$. Let γ_μ^* be the leading coefficient of $\det(\hat{\mathcal{H}}_{t+1,\mu})$ in the variable $\hat{\alpha}$, and let $\Gamma_f^*(x) = \prod_{\mu=2}^{2t} \gamma_\mu^*(x)$. For sparsity and degree upper bounds: $B \ge t \ge 1$ and $D \ge \delta_j$ with $1 \le j \le t$, we have*

$$\deg(\Gamma_f^*) < t^3 D \le B^3 D. \quad (10)$$

Proof see Appendix C.

Theorem 2.3. *Let K be any scalar field, $\omega \in \mathsf{K}$, and $\hat{H}_{t+1,\mu}$ be as in (6) for $1 \le \mu \le 2t+1$. Then there exists a polynomial $\Gamma_f(x) \in \mathsf{K}[x]$, which depends on the coefficients and term degrees of f in (3), such that the implication (7) holds and*

$$\deg_x(\Gamma_f) < 2t^3 D \le 2B^3 D. \quad (11)$$

Proof see Appendix C.

Second, if the characteristic of the field K is $\ne 2$, we prove that the linear term of $\det(\hat{\mathcal{H}}_{t+1,\mu})$ in $\hat{\alpha}$ is non-zero. Taking the product of all coefficients of the linear term of $\det(\hat{\mathcal{H}}_{t+1,\mu}), \mu = 2, \ldots, 2t$ in $\hat{\alpha}$ and clearing all possible denominators, we obtain a polynomial Γ_f of degree bounded by $4B^2D$ such that the implication (7) holds. Note that $4B^2D \le 2B^3D$ for all $B \ge 2$,

[3] We have used the letter α in the early termination theorems for evaluations when ω was a variable [1, 14]. In [16] α was used as the variable for the erroneous value. Here we use $\hat{\alpha}$ for the variable in the place of the error.

[4] By hatting the matrices $\hat{H}_{t+1,\mu}$, $\hat{\mathcal{H}}_{t+1,\mu}$ we indicate that the entries contain the variable $\hat{\alpha}$. By using the calligraphic $\mathcal{H}$ we indicate the arguments ω^i are terms x^i. The matrix $\hat{H}_{t+1,\mu}$ has $\hat{\alpha}$ on the anti-diagonal where a_μ sits, and $\mathcal{H}_{t+1,\mu}$ has $\alpha_\mu + \hat{\alpha}$ on the anti-diagonal where α_μ sits. Similar notation will be used in Section 3.

which means that if characteristic $(\mathsf{K}) \neq 2$, we can choose the argument ω from smaller subsets of K while maintaining the same probability of success, similarly to early termination [8]. In the remainder of the paper, we assume that the characteristic of the base field K is $\neq 2$.

Theorem 2.4. *Let $\mu = 1, 2, \ldots, 2t+1$ and $\hat{\mathcal{H}}_{t+1,\mu}$ be the matrix obtained by substituting α_μ with $\alpha_\mu + \hat{\alpha}$ in $\mathcal{H}_{t+1}$ (see (8) for $\mathcal{H}_{t+1}$). Let $\gamma_{t+1,\mu}$ be the coefficient of the linear term of $\det(\hat{\mathcal{H}}_{t+1,\mu})$ with respect to the variable $\hat{\alpha}$. Let $Q' = \sum_{j=1}^{t}(2j+1)\delta_j$. Then $\gamma_{t+1,\mu}$ has the leading monomial $\sigma(\prod_{j=1}^{t} c_j)x^Q$:*
If μ is an even integer: $\sigma = -2$, $Q = Q' - Q''$,

$$Q'' = \Big(\sum_{j=1}^{(\mu/2)-1} \delta_j\Big) + \Big(\sum_{j=1}^{\mu/2} \delta_j\Big).$$

If μ is an odd integer: $\sigma{=}1$, $Q{=}Q'{-}Q''$, $Q''{=}2\Big(\sum_{j=1}^{(\mu-1)/2} \delta_j\Big)$.

Proof. Let $(\mathcal{H}_{t+1})\downarrow_{u,v}$ be the submatrix of $\mathcal{H}_{t+1}$ by removing the u-th row and v-th column from $\mathcal{H}_{t+1}$. By the minor expansion formula, we have

$$(-1)^{\mu+1}\gamma_{t+1,\mu} = \sum_{\substack{1\le u,v\le t+1\\ u+v=\mu+1}} \det((\mathcal{H}_{t+1})\downarrow_{u,v}), \tag{12}$$

Let

$$\beta_1 = x^{\delta_1}, \beta_2 = x^{\delta_2}, \ldots, \beta_t = x^{\delta_t} \tag{13}$$

be the terms in $f(x)$ (3). Consider the matrices

$$\begin{aligned} \mathcal{B}_{t+1} &= \Big[\beta_j^{i-1}\Big]_{1\le i\le t+1, 1\le j\le t} \in \mathsf{K}[x, \frac{1}{x}]^{(t+1)\times t},\\ C &= \operatorname{diag}(c_1, \ldots, c_t) \in \mathsf{K}^{t\times t},\\ \bar{\mathcal{B}}_{t+1} &= \Big[\beta_j^{i}\Big]^T_{1\le i\le t+1, 1\le j\le t} \in \mathsf{K}[x, \frac{1}{x}]^{t\times(t+1)} \end{aligned} \tag{14}$$

Let $(\mathcal{B}_{t+1})\downarrow_{u,*}$ be the submatrix of $\mathcal{B}_{t+1}$ with the u-th row removed and $(\bar{\mathcal{B}}_{t+1})\downarrow_{*,v}$ be the submatrix of $\bar{\mathcal{B}}_{t+1}$ with the v-th column removed. Then

$$(\mathcal{H}_{t+1})\downarrow_{u,v} = (\mathcal{B}_{t+1})\downarrow_{u,*} C\, (\bar{\mathcal{B}}_{t+1})\downarrow_{*,v}. \tag{15}$$

By Lemma A.1, the largest degree term in $\det((\mathcal{B}_{t+1})\downarrow_{u,*})$ is the product of the diagonal terms:

$$\beta_0^{-1}\beta_1^{0}\beta_2^{1}\cdots\beta_{u-1}^{u-2}\beta_u^{u}\cdots\beta_t^{t} \text{ for } 1\le u\le t \text{ with } \beta_0 = 1. \tag{16}$$

and the largest degree term in $\det((\bar{\mathcal{B}}_{t+1})\downarrow_{*,v})$ is

$$\beta_0^{0}\beta_1^{1}\beta_2^{2}\cdots\beta_{v-1}^{v-1}\beta_v^{v+1}\cdots\beta_t^{t+1}\beta_{t+1}^{t+2} \text{ for } 1\le v\le t+1 \text{ with } \beta_0 = \beta_{t+1} = 1. \tag{17}$$

Therefore the leading term of $\det((\mathcal{H}_{t+1})\downarrow_{u,v})$ is

$$\begin{aligned} \rho_{u,v} &= \text{ leading term of } \det((\mathcal{H}_{t+1})\downarrow_{u,v})\\ &= \Big(\prod_{j=1}^{u-1}\beta_j^{-1}\Big)\Big(\prod_{j=1}^{v-1}\beta_j^{-1}\Big)\Big(\prod_{j=1}^{t}\beta_j^{2j+1}\Big). \end{aligned} \tag{18}$$

Then $\rho_{u,v} = \beta_u\beta_{v-1}^{-1}\,\rho_{u+1,v-1}$ (moving up the anti-diagonal) and $\deg(\rho_{u,v}) - \deg(\rho_{u+1,v-1}) = \delta_u - \delta_{v-1}$. Since $\delta_u - \delta_{v-1} < 0 \iff u < v-1 = \mu - u - 2$, we have $\deg(\rho_{u,v}) < \deg(\rho_{u+1,v-1})$ for $u+1 < \mu/2$. Let

$$u_{\max} = \lfloor(\mu-1)/2\rfloor,\ v_{\max} = \mu - 1 - u_{\max}, \tag{19}$$

then $\deg(\rho_{u,v}) < \deg(\rho_{u_{\max},v_{\max}})$ for all $u \neq u_{\max}$. Therefore, the leading term of (12) is

$$\left.\begin{aligned} \rho_{\frac{\mu}{2}-1,\frac{\mu}{2}} &{=}\Big(\prod_{j=1}^{\mu/2-1}\beta_j^{-1}\Big)\Big(\prod_{j=1}^{\mu/2}\beta_j^{-1}\Big)\Big(\prod_{j=1}^{t}\beta_j^{2j+1}\Big) \ (\mu \text{ even}),\\ \rho_{\frac{\mu-1}{2},\frac{\mu-1}{2}} &{=}\Big(\prod_{j=1}^{\frac{\mu-1}{2}}\beta_j^{-1}\Big)\Big(\prod_{j=1}^{\frac{\mu-1}{2}}\beta_j^{-1}\Big)\Big(\prod_{j=1}^{t}\beta_j^{2j+1}\Big) \ (\mu \text{ odd}). \end{aligned}\right\} \tag{20}$$

The theorem follows from the equations (12), (15), and (20). □

Lemma 2.5. *Let $\gamma_{t+1,\mu}$ be the coefficient of the linear term of $\det(\hat{\mathcal{H}}_{t+1,\mu})$ (see Theorem 2.4), and let*

$$\Psi_t(x) = \prod_{1\le j_1<j_2\le t}(\beta_{j_1} - \beta_{j_2}) \textit{ (See (13) for } \beta_j\textit{).} \tag{21}$$

If all the term degrees of $f(x)$ in (3) are non-negative, namely, $\delta_j \geq 0$ for all $1 \leq j \leq t$, then $\bar{\gamma}_{t+1,\mu} = \gamma_{t+1,\mu}/(\Psi_t(x)^2\prod_{j=1}^{t}\beta_j)$ is a polynomial in $\mathsf{K}[x]$ of degree $(\sum_{j=1}^{t} 2\delta_j) - Q''$ where Q'' is as in Theorem 2.4.

Proof. By the factorization of $(\mathcal{H}_{t+1})\downarrow_{u,v}$ (see (15)) and Lemma A.2, the determinant of each $(\mathcal{H}_{t+1})\downarrow_{u,v}$ has factor $\Psi_t(x)^2\prod_{j=1}^{t}\beta_j$. The degree of $\bar{\gamma}_{t+1,\mu}$ is $\deg(\gamma_{t+1,\mu}) - \sum_{j=1}^{t}(2(j-1)+1)\delta_j = Q - \sum_{j=1}^{t}(2j-1)\delta_j = \Big(\sum_{j=1}^{t} 2\delta_j\Big) - Q''$, where Q and Q'' are as in Theorem 2.4. □

Lemma 2.6. *Let $\gamma_{t+1,\mu}$ be the coefficient of the linear term of $\det(\hat{\mathcal{H}}_{t+1,\mu})$ (see Theorem 2.4), and let $\Psi_t(x)$ as (21) in Lemma 2.5. If $f(x)$ in (3) has negative degree terms, namely, $\delta_1 < 0$, then $\bar{\gamma}_{t+1,\mu} = x^{(2t-\mu+1)|\delta_1|}\gamma_{t+1,\mu}/(\Psi_t(x)^2\prod_{j=1}^{t}\beta_j)$ is a polynomial in $\mathsf{K}[x]$ of degree $(\sum_{j=1}^{t} 2\delta_j) - Q'' + (2t-\mu+1)|\delta_1|$ where Q'' is as in Theorem 2.4. Proof see Appendix C.*

Theorem 2.7. *Assume that the field K has characteristic $\neq 2$. Let $\omega \in \mathsf{K}$ and let $\hat{H}_{t+1,\mu}$ be as in (6) for $1 \leq \mu \leq 2t+1$. Then there exists a polynomial $\Gamma_f(x) \in \mathsf{K}[x]$, which depends on the coefficients and term degrees of f in (3), such that the implication (7) holds. Moreover, for all $B \geq t$ and $D \geq |\delta_j|$ with $1 \leq j \leq t$, we have*

$$\deg_x(\Gamma_f) \leq 2(t^2 - t)(\delta_t + |\delta_1|) < 4B^2D. \tag{22}$$

Proof see Appendix C.

3. CHEBYSHEV BASIS

Let $f(x)$ be a t-sparse polynomial in Chebyshev-1 basis $T_n(x)$,

$$f(x){=}\sum_{j=1}^{t} c_j T_{\delta_j}(x){\in}\mathsf{K}[x], 0{\le}\delta_1{<}\delta_2{<}\cdots{<}\delta_t{=}\deg_x(f), \quad c_j \neq 0 \text{ for all } 1\le j\le t, \tag{23}$$

where K is a field of characteristic $\neq 2$. We first show how to Prony-list-interpolate f from values $\hat{a}_i$ for $1 \leq i \leq 2t+1$, when no more than one value $\hat{a}_\ell$ is incorrect, that is $\hat{a}_i = f(\omega^{2i-1})$ for all $1 \leq i \leq 2t+1$ and $i \neq \ell$. If ω is selected randomly and uniformly from a finite set $S \subseteq \mathsf{K}$ of cardinality $|S| \geq \frac{(t\deg(f))^{O(1)}}{\epsilon}$ (see Theorem 4.1 for the precise analysis), then the polynomial f is in the list of computed interpolants with probability $\geq 1 - \epsilon$.

Let

$$g(y) = f\Big(\frac{y+\frac{1}{y}}{2}\Big) = \textstyle\sum_{j=1}^{t} \frac{c_j}{2}\big(y^{\delta_j} + \frac{1}{y^{\delta_j}}\big) \in \mathsf{K}[y, \frac{1}{y}],$$

$$t_g = \begin{Bmatrix} 2t-1 & \text{if } \delta_1 = 0, \\ 2t & \text{if } \delta_1 > 0. \end{Bmatrix} \qquad (24)$$

The polynomial g is a t_g-sparse Laurent polynomial in the power basis $(y^n)_{n\in\mathbb{Z}}$ with coefficients in K. The Prony/BCH-decoding algorithm can recover g by evaluating at $a_{2i-1} = a_{-(2i-1)} = g(\omega^{2i-1})$ for $i = 1, \ldots, t_g$. Note that the subscript is the exponent or negated exponent; odd powers are used to avoid the use of $g(1)$, which could be erroneous in each block [16, Section III]. The $2t_g$-element sequence

$$a_{-(2t_g-1)}, a_{-(2t_g-3)}, \ldots, a_{-3}, a_{-1}, a_1, a_3, a_5, \ldots, a_{2t_g-1} \qquad (25)$$

is linearly generated by

$$\Lambda(z) = \begin{Bmatrix} \prod_{j=1}^{t_g} (z-\omega^{2\delta_j})(z-\omega^{-2\delta_j}) & \text{if } \delta_1 \neq 0 \\ (z-1)\prod_{j=2}^{t_g} (z-\omega^{2\delta_j})(z-\omega^{-2\delta_j}) & \text{if } \delta_1 = 0 \end{Bmatrix}, \qquad (26)$$

$\deg(\Lambda) = t_g$. Note that the sequence of values for each monomial $c(\omega^{\delta})^{2i-1}$ for $i = -i_0, -i_0+1, \ldots, 0, 1, \ldots$ is linearly generated by $z - \omega^{2\delta}$. One selects ω so that all roots of $\Lambda(z)$ are distinct, computes Λ and its roots, computes c_j, and recovers the δ_j from the roots.

If $\Lambda(z)$ is squarefree, $\Lambda(z)$ is the minimal linear generator for (25). Then the Hankel matrices

$$H_\tau = \mathrm{Hankel}_\tau(a_{-(2\tau-3)+2i} \colon i{=}0, \ldots, 2\tau{-}2) \in \mathsf{K}^{\tau\times\tau}, \tau \geq 1, \qquad (27)$$

have the property that H_{t_g} is non-singular because Λ is minimal and H_{t_g+1} is singular because of the column relation given by the linear generator Λ.

If a value $\hat{a}_{2\ell-1}$ is incorrect, we again place a variable $\hat{\alpha}$ for $a_{2\ell-1}$ and $a_{-(2\ell-1)}$ in H_{t_g+1}. We shall prove that if ω is randomly and uniformly selected from a sufficiently large finite set $S \subseteq \mathsf{K}$, then all matrices

$$m{=}t_g+1, \hat{H}_{m,\mu} {=} \begin{Bmatrix} \text{replace in } H_m \text{ the anti-diagonals} \\ \text{containing } a_{2\mu-1} \text{ and } a_{-(2\mu-1)}, \\ \text{which are equal, by the single} \\ \text{variable } \hat{\alpha} \end{Bmatrix} \qquad (28)$$

are non-singular matrices in $\mathsf{K}[\hat{\alpha}]^{m\times m}$, with high probability. Therefore, the correct value $a_{2\ell-1}$ is among the roots of the determinants of all $\hat{H}_{m,\mu}$, and f is in the list of all valid interpolants computed from those roots, with high probability.

We prove that $\hat{H}_{m,\mu}$ is non-singular for symbolic evaluation, that is values $\alpha_{2i-1} = g(y^{2i-1})$. The corresponding Hankel matrix $\in \mathsf{K}[y, 1/y]^{m\times m}$ is denoted as

$$\mathcal{H}_m = \mathrm{Hankel}_m(\alpha_{-(2m-3)+2i} \colon i{=}0, \ldots, 2m{-}2). \qquad (29)$$

We wish to prove that when the anti-diagonal containing $\alpha_{2\mu-1}$ is substituted by $\hat{\alpha} + \alpha_{2\mu-1}$ and the anti-diagonal containing $\alpha_{-(2\mu-1)}$ is substituted by $\hat{\alpha} + \alpha_{-(2\mu-1)}$, for $\mu = 2, 3, \ldots, t_g = m{-}1$, the resulting matrix $\hat{\mathcal{H}}_{m,\mu} \in \mathsf{K}[y, \frac{1}{y}, \hat{\alpha}]^{m\times m}$ will become non-singular ((30) displays $\hat{\mathcal{H}}_{5,2}$).

$$\hat{\mathcal{H}}_{5,2} = \begin{bmatrix} \alpha_{-7} & \alpha_{-5} & \alpha_{-3}{+}\hat{\alpha} & \alpha_{-1} & \alpha_1 \\ \alpha_{-5} & \alpha_{-3}{+}\hat{\alpha} & \alpha_{-1} & \alpha_1 & \alpha_3{+}\hat{\alpha} \\ \alpha_{-3}{+}\hat{\alpha} & \alpha_{-1} & \alpha_1 & \alpha_3{+}\hat{\alpha} & \alpha_5 \\ \alpha_{-1} & \alpha_1 & \alpha_3{+}\hat{\alpha} & \alpha_5 & \alpha_7 \\ \alpha_1 & \alpha_3{+}\hat{\alpha} & \alpha_5 & \alpha_7 & \alpha_9 \end{bmatrix}. \qquad (30)$$

Note that for $\mu = 1$ one has the term $\hat{\alpha}^m$ in $\det(\hat{\mathcal{H}}_{m,\mu})$, and for $\mu = t_g + 1$ the top $(m-1)\times(m-1)$ matrix is non-singular by Prony's argument: the first $t_g = m-1$ equations determine the generator, provided $\Lambda(z)$ (26) is squarefree.

Theorem 3.1. *Let $\mu = 1, 2, \ldots, t_g + 1$ and let $\hat{\mathcal{H}}_{m,\mu}$ be the matrix $\mathcal{H}_m$ (29) that has the variable $\hat{\alpha}$ added to all elements in row u and column v with $u + v = t_g + 2 - \mu$ and $u + v = t_g + 1 + \mu$ (see Appendix 3). Let*

$$\eta_1 = -\delta_t, \eta_2 = -\delta_{t-1}, \ldots, \eta_{t_g} = \delta_t \qquad (31)$$

be the degrees of the terms in $g(y)$ in (24) and let $P = c_t^2/4\ c_{t-1}^2/4 \ldots$ be the product of all coefficients in (24); note that $\sum_{j=1}^{t_g} \eta_j = 0$ and if $\delta_1 = 0$, then P has the factor c_1, else the factor $c_1^2/4$. Let $Q' = 4\sum_{j=2}^{t_g}(j-1)\eta_j$. Then the coefficient of the linear term $\hat{\alpha}$ in $\det(\hat{\mathcal{H}}_{m,\mu})$ has the leading monomial $\sigma P y^Q$:
If $t_g + \mu$ is an even integer: $\sigma = -2$, $Q = Q' - Q''$,

$$Q'' = 2\Big(\sum_{j=1}^{(t_g+\mu)/2} \eta_j\Big) + 2\Big(\sum_{j=1}^{(t_g-\mu)/2+1} \eta_j\Big).$$

If $t_g + \mu$ is an odd integer: $\sigma = 1$, $Q = Q' - Q''$,

$$Q'' = 2\Big(\sum_{j=1}^{(t_g+\mu-1)/2} \eta_j\Big) + 2\Big(\sum_{j=1}^{(t_g-\mu+1)/2} \eta_j\Big).$$

Proof. Let $(\mathcal{H}_m)\downarrow_{u,v}$ define the $m \times m$ submatrix of $\mathcal{H}_m$ which has row u and column v removed from $\mathcal{H}_m$. By the minor expansion formula, for each (u, v) location in $\hat{\mathcal{H}}_{m,\mu}$ which contains the entry $\hat{\alpha} + \alpha_{2\mu-1}$ or $\hat{\alpha} + \alpha_{-(2\mu-1)}$, $(-1)^{u+v}\det($ $(\mathcal{H}_m)\downarrow_{u,v})$ adds to the coefficient of $\hat{\alpha}$ in the determinant $\det($ $\hat{\mathcal{H}}_{m,\mu})$. Let $\gamma_{m,\mu}$ be the coefficient of the linear term of $\det($ $\hat{\mathcal{H}}_{m,\mu})$ with respect to the variable $\hat{\alpha}$, then $\gamma_{m,\mu} = \gamma_{m,\mu}^{\text{bot}} + \gamma_{m,\mu}^{\text{top}}$ where

$$\gamma_{m,\mu}^{\text{bot}} = (-1)^{t_g+1+\mu} \sum_{u+v=t_g+1+\mu} \det((\mathcal{H}_m)\downarrow_{u,v})$$

is the coefficient of $\hat{\alpha}$ collected from the bottom anti-diagonal of $\hat{\mathcal{H}}_{m,\mu}$ and

$$\gamma_{m,\mu}^{\text{top}} = (-1)^{t_g+2-\mu} \sum_{u+v=t_g+2-\mu} \det((\mathcal{H}_m)\downarrow_{u,v})$$

is the coefficient of $\hat{\alpha}$ collected from the top anti-diagonal of $\hat{\mathcal{H}}_{m,\mu}$.

We determine the largest degree term in y in $\det((\mathcal{H}_m)\downarrow_{u,v})$. We have the following factorization for the matrix $(\mathcal{H}_m)\downarrow_{u,v}$: Let

$$\beta_1 = y^{-\delta_t}, \beta_2 = y^{-\delta_{t-1}}, \ldots, \beta_{t_g-1} = y^{\delta_{t-1}}, \beta_{t_g} = y^{\delta_t}, \qquad (32)$$

$\deg(\beta_j) = -\deg(\beta_{t_g-(j-1)})$, be the terms in $g(y)$ (24) in degree order. Note that a term β_j with $j \leq t_g/2$ has a negative degree. Consider the matrices

$$\mathcal{B}_m = \Big[\beta_j^{1+2(i-1)}\Big]_{1\leq i\leq t_g+1, 1\leq j\leq t_g} \in \mathsf{K}[y, \frac{1}{y}]^{(t_g+1)\times t_g},$$

$$C_m = \mathrm{diag}(c_t/2, c_{t-1}/2, \ldots, c_{t-1}/2, c_t/2) \in \mathsf{K}^{t_g\times t_g},$$

$$(C_m)_{(t_g+1)/2,(t_g+1)/2} = c_1 \text{ if } \delta_1 = 0,$$

$$\bar{\mathcal{B}}_m = \Big[\beta_{t_g+1-j}^{2t_g+2-2i}\Big]^T_{1\leq i\leq t_g+1, 1\leq j\leq t_g} \in \mathsf{K}[y, \frac{1}{y}]^{t_g\times(t_g+1)} \qquad (33)$$

Note that C_m has the monomial coefficients of $g(y)$ (24) on its diagonal. Let $(\mathcal{B}_m)\downarrow_{u,*}$ be the submatrix of $\mathcal{B}_m$ with row u removed, and let Let $(\bar{\mathcal{B}}_m)\downarrow_{*,v}$ be the submatrix of $\bar{\mathcal{B}}_m$ with the column v removed. We have

$$(\mathcal{H}_m)\downarrow_{u,v} = (\mathcal{B}_m)\downarrow_{u,*}\, C_m\, (\bar{\mathcal{B}}_m)\downarrow_{*,v}. \qquad (34)$$

Similarly to the proof of (18) in Theorem 2.4, we have

$$\text{leading term of } (\mathcal{H}_m)\downarrow_{u,v} = \Big(\prod_{j=1}^{u-1} \beta_j^{-2}\Big)\Big(\prod_{j=1}^{t_g-(v-1)} \beta_j^{-2}\Big)\Big(\prod_{j=1}^{t_g} \beta_j^{4j+1}\Big). \quad (35)$$

Let $(u_{\max}^{\text{bot}}, v_{\max}^{\text{bot}})$ be one of the indices where $\det((\mathcal{H}_m)\downarrow_{u,v})$ reaches the largest degree among all summand determinants in $\gamma_{m,\mu}^{\text{bot}}$ and $(u_{\max}^{\text{top}}, v_{\max}^{\text{top}})$ be that of $\gamma_{m,\mu}^{\text{top}}$ (see Appendix C for details).

We now compare the factor

$$\Big(\prod_{j=1}^{u-1} \beta_j^{-2}\Big)\Big(\prod_{j=1}^{t_g-(v-1)} \beta_j^{-2}\Big) \quad (36)$$

in the minor degree (35) for the maxima on both diagonals. Again, similar to the analysis for (19), there are 2 cases:

Case $t_g+1+\mu$ odd: Then $u_{\max}^{\text{bot}} = t_g/2+\mu/2+1$, $v_{\max}^{\text{bot}} = t_g/2+\mu/2$, and $u_{\max}^{\text{top}} = v_{\max}^{\text{top}} = t_g/2+1-\mu/2$. We have:

$$\begin{array}{r|cc} & u_{\max}-1 & t_g-(v_{\max}-1) \\ \hline \text{bot} & t_g/2+\mu/2 & t_g/2-\mu/2+1 \\ \text{top} & t_g/2-\mu/2 & t_g/2+\mu/2 \end{array} \quad (37)$$

Therefore, the factor (36) has for the maximum on the bottom anti-diagonal the extra factor $\beta_{t_g/2-\mu/2+1}^{-2}$ whose degree is positive by (32) because $t_g/2-\mu/2+1 \le t_g/2$ for $\mu \ge 2$.

Case $t_g+1+\mu$ even: Then $u_{\max}^{\text{bot}} = v_{\max}^{\text{bot}} = t_g/2+\mu/2+1/2$, $u_{\max}^{\text{top}} = t_g/2-\mu/2+1/2$ and $v_{\max}^{\text{top}} = t_g/2-\mu/2+3/2$. We have:

$$\begin{array}{r|cc} & u_{\max}-1 & t_g-(v_{\max}-1) \\ \hline \text{bot} & t_g/2+\mu/2-1/2 & t_g/2-\mu/2+1/2 \\ \text{top} & t_g/2-\mu/2-1/2 & t_g/2+\mu/2-1/2 \end{array} \quad (38)$$

Therefore, the factor (36) has for the maximum on the bottom anti-diagonal the extra factor $\beta_{t_g/2-\mu/2+1/2}^{-2}$ whose degree is positive by (32) because $t_g/2-\mu/2+1/2 < t_g/2$ for $\mu \ge 2$.

In summary, the maximum degree of the minors is larger on the bottom anti-diagonal. □

For later probability analysis, we refine Theorem 3.1.

Lemma 3.2. *Let $\gamma_{m,\mu}(y)$ be the coefficient of $\hat{\alpha}$ of $\det(\hat{\mathcal{H}}_{m,\mu})$ (see Theorem 3.1), and let*

$$\Psi_{t_g}(y) = \prod_{1\le j_1<j_2\le t_g} (\beta_{j_1}^2 - \beta_{j_2}^2) \quad (39)$$

(see (32) for a definition of β_j). Then $\bar{\gamma}_{m,\mu}(y) = y^{Q-Q'}\gamma_{m,\mu}(y)/\Psi_{t_g}(y)^2$ is a polynomial in $\mathsf{K}[y]$ with $\bar{\gamma}_{m,\mu}(y) \ne 0$ of degree $2(Q-Q')$. Proof see Appendix C.

Theorem 3.3. *Let $\omega \in \mathsf{K}$ and let $\hat{H}_{m,\mu}$ for $1 \le \mu \le t_g+1$ be as in (28) and let $\Delta_{m,\mu}(\hat{\alpha}) = \det(\hat{H}_{m,\mu}) \in \mathsf{K}[\hat{\alpha}]$. Note that $\Delta_{m,\mu}(\omega^{2\mu-1}) = 0$ for all μ. Then there exists a polynomial $\Gamma_f(y) \in \mathsf{K}[y]$, which depends on the coefficients and term degrees of f in (23), such that:*

$$\omega \ne 0 \text{ and } \Gamma_f(\omega) \ne 0 \text{ and } \Psi_{t_g}(\omega) \ne 0 \implies \Lambda(z) \text{ in (26) is squarefree and } \forall\mu, 1 \le \mu \le t_g+1\colon \Delta_{m,\mu}(\hat{\alpha}) \ne 0. \quad (40)$$

See (39) for a definition of Ψ_{t_g}. Moreover, we have for all $B \ge t$ and $D \ge \delta_t$ the degree upper bounds

$$\deg_y(\Gamma_f) \le 8t^2(2\delta_t - t + 1) \le 16B^2D. \quad (41)$$

Proof see Appendix C.

4. RANDOMIZED ALGORITHMS

We present randomized algorithms for error-correcting sparse interpolation in power basis or Chebyshev polynomial basis where the arguments for the values of f incorporate randomness.

Definition 4.1. Let $B \in \mathbb{Z}_{>0}$, $D, E \in \mathbb{Z}_{\ge 0}$, $\theta = \lfloor E/2 \rfloor + 1$ and let $\omega_\nu \in \mathsf{K}$ for $1 \le \nu \le \theta$, where K is a field. Furthermore, let $\hat{a}_{\nu,i} \in \mathsf{K}$ and $\hat{a}_{\nu,2i-1} \in \mathsf{K}$ for $1 \le i \le 2B+1$. We call $f(x) \in \mathsf{K}[x, \frac{1}{x}]$ (3) or $f(x) \in \mathsf{K}[x]$ (23) a (B, D, E)-*sparse interpolant* if the following are satisfied:

A. $t \le B$, where t is the sparsity of f;
B. $\deg(f) = \delta_t \le D$ and $|\delta_1| \le D$ in (3);
C. $k = |I| \le E$ where $I = \{(\nu, i) \mid f(\omega_\nu^i) \ne \hat{a}_{\nu,i}, 1 \le \nu \le \theta, 1 \le i \le 2B+1\}$ for power basis, $I = \{(\nu, i) \mid f(\frac{\omega_\nu^{2i-1}}{2} + \frac{1}{2\omega_\nu^{2i-1}}) \ne \hat{a}_{\nu,2i-1}, 1 \le \nu \le \theta, 1 \le i \le 2B+1\}$ for Chebyshev basis;
D. for all $1 \le i \le 2B+1$ and $1 \le \nu \le \theta$ and $(\nu, i) \notin I$: $f(\omega_\nu^i) = \hat{a}_{\nu,i}$ for power basis, $f(\frac{\omega_\nu^{2i-1}}{2} + \frac{1}{2\omega_\nu^{2i-1}}) = \hat{a}_{\nu,2i-1}$ for Chebyshev basis.

Definition 4.2. We call a family of sample sets $S_\nu \subseteq \mathsf{K}$ for $1 \le \nu \le \theta$ *usable* for failure probability $\epsilon > 0$ if the following is satisfied, where $|S_\nu|$ denotes the number of elements in S_ν.

A. $\forall\nu\colon$ $|S_\nu| \ge (2B^3D)/\epsilon$ for power basis and $\text{char}(\mathsf{K}) = 2$, $|S_\nu| \ge (4B^2D)/\epsilon$ for power basis and $\text{char}(\mathsf{K}) \ne 2$, $|S_\nu| \ge (16B^2D)/\epsilon$ for Chebyshev basis (requires $\text{char}(\mathsf{K}) \ne 2$).
B. $\forall\nu, \forall\omega \in S_\nu, \forall J_1, J_2$ with $-D \le J_1 < J_2 \le D\colon$ $\omega^{J_1} \ne \omega^{J_2}$ for power basis, and $\omega^{2J_1} \ne \omega^{2J_2}$ for Chebyshev basis ($\Longrightarrow 0, 1, -1 \notin S_\nu$).
C. $\forall\nu_1, \nu_2$ with $\nu_1 \ne \nu_2, \forall\omega_{\nu_1} \in S_{\nu_1}, \forall\omega_{\nu_2} \in S_{\nu_2}, \forall i_1, i_2$ with $1 \le i_1, i_2 \le 2B+1\colon$ $\omega_{\nu_1}^{i_1} \ne \omega_{\nu_2}^{i_2}$ for power basis, $\omega_{\nu_1}^{2i_1-1} \ne \omega_{\nu_2}^{2i_2-1}$ and $\omega_{\nu_1}^{2i_1-1} \ne \omega_{\nu_2}^{-(2i_2-1)}$ for Chebyshev basis.

The condition in Definition 4.2.B guarantees that the term locator polynomial $\Lambda(z)$ (see (5) for power basis and (26) for Chebyshev basis) is squarefree. Squarefreeness can also be achieved by randomization, in which case the cardinality bound in Definition 4.2.A needs to be increased. See Remark 4.2 below. The condition in Definition 4.2.C guarantees that for all random samples, the arguments ω_ν^i of power basis interpolant values $f(\omega_\nu^i)$ are distinct, and the arguments $\frac{\omega_\nu^{2i-1}}{2}+\frac{1}{2\omega_\nu^{2i-1}}$ of the Chebyshev basis interpolant values $f(\frac{\omega_\nu^{2i-1}}{2}+\frac{1}{2\omega_\nu^{2i-1}})$ are distinct, the latter by Lemma A.3.[5] For $\mathsf{K} \supseteq \mathbb{Q}$ one can deterministically construct a usable family of sample sets, for example, by using distinct prime numbers.

We note that the error locations and erroneous values of Definition 4.1.C above depend on how the polynomials are evaluated. For instance, the interpolant f may be given by a black box that at a randomly selected ω_ν returns an error at some ω_ν^i. The $\le E$ errors depend on the arguments and are not at random locations. See also Theorem 4.1 and the remark following its proof below.

4.1. Randomized Error-correcting Sparse Interpolation

Input: ▸ Bounds $D, E \in \mathbb{Z}_{\ge 0}$, $B \in \mathbb{Z}_{>0}$ for the absolute values

[5] The condition in Definition 4.2.C is also required in [16, Section III].

of the term degrees, number of errors, and number of terms;
‣ An algorithmic error probability bound $\epsilon \in \mathbb{R}$ with $0<\epsilon<1$;
‣ An arguments list $\omega_\nu \in S_\nu$ for $1 \le \nu \le \theta = \lfloor E/2 \rfloor + 1$, where each ω_ν is sampled uniformly, independently, and randomly from a usable finite set S_ν (see Definition 4.2);
‣ For $1 \le \nu \le \theta$ and $1 \le i \le 2B+1$ an array of values: $\hat{a}_{\nu,i} \in \mathsf{K}$ for power basis and $\hat{a}_{\nu,2i-1} \in \mathsf{K}$ for Chebyshev basis.

Output: ‣ A list of (B, D, E)-sparse interpolants for the arguments/values inputs (see Definition 4.1).

```
1: For $\nu = 1, \ldots, \theta$ Do Step 2;
   After completion, return the list of interpolants;
2: For $t = 1, \ldots, B$ [ $t_g = 1, \ldots, 2B$ for Chebyshev basis ] Do Step 3;
   We try to interpolate, while correcting a single possible error, a polynomial which is sparse with $t$ terms from the values $\hat{a}_{\nu,i}$ for $1 \le i \le 2t+1$ [ for Chebyshev basis: $t_g$ terms in $g(y)$ (24) from the values $\hat{a}_{\nu,2i-1}$ for $1 \le i \le t_g+1$ ].
3: For $\mu = 1, \ldots, 2t+1$ [ $\mu = 1, \ldots, t_g+1$ for Chebyshev basis ] Do Step 4;
4: We guess that the error is in $\hat{a}_{\nu,\mu}$ [ the error is in $\hat{a}_{\nu,2\mu-1}$ for Chebyshev basis ].
    4(a): Compute $\Delta_{m,\mu}(\hat{\alpha})$ for $m = t+1$ and $\hat{a}_i = \hat{a}_{\nu,i}$ for $1 \le i \le m$ [ for Chebyshev basis: $m = t_g+1$ and $\hat{a}_{\pm(2i-1)} = \hat{a}_{\nu,2i-1}$ for $1 \le i \le m$ ];
          See Theorems 2.7, 3.3 for the definition of $\Delta_{m,\mu}$.
    4(b): If $\Delta_{m,\mu}(\hat{\alpha}) \in \mathsf{K}$ (a constant polynomial) continue with next $\mu$;
    4(c): Compute all roots $\xi_1, \ldots, \xi_b \in \mathsf{K}$ for $\Delta_{m,\mu}(\hat{\alpha}) = 0$;
    4(d): For all $\xi \in \{\xi_1, \ldots, \xi_b\}$ try Prony's Algorithm on the sequence $a_i = \hat{a}_i$ for $i \neq \mu$, $a_\mu = \xi$ [ for Chebyshev basis: $a_{\pm(2i-1)} = \hat{a}_{2i-1}$ for $i \neq \mu$, $a_{\pm(2\mu-1)} = \xi$ ]; see [16, Algorithm 1 Try Prony's algorithm] for a complete description of the algorithm.
          If a valid interpolant $f(x)$ is returned, perform Step 5.
5: For all other rows $\kappa$ with $1 \le \kappa \le \theta, \kappa \neq \nu$ and all $1 \le i \le 2B+1$ count for the computed interpolant $f(x)$ at row $\nu$ how many more values $\hat{a}_{\kappa,i}$ are $\neq f(\omega_\kappa^i)$ [ for Chebyshev basis: count the number of $\hat{a}_{\kappa,2i-1} \neq f(\frac{\omega_\kappa^{2i-1}}{2}+\frac{1}{2\omega_\kappa^{2i-1}})$ ];
   If the total count of errors in all rows is $\le E$, add $f(x)$ to the list of interpolants.
```

Theorem 4.1. *Let $f(x) = \sum_{j=1}^{t} c_j x^{\delta_j}$ with $t \le B$ and $-D \le \delta_1 < \delta_2 < \cdots < \delta_t \le D$ (or let $f(x)$ be a polynomial of degree $\delta_t \le D$ with $t \le B$ Chebyshev terms (23)). Suppose the arguments to f are ω_ν^i for randomly sampled ω_ν from the sets S_ν, and the array $\hat{a}_{\nu,i}$ contains $f(\omega_\nu^i)$ except in $k \le E$ places (or if f has Chebyshev terms, the arguments to f are $\frac{\omega_\nu^{2i-1}}{2}+\frac{1}{2\omega_\nu^{2i-1}}$ for randomly sampled ω_ν from the sets S_ν, and the array $\hat{a}_{\nu,2i-1}$ contains $f(\frac{\omega_\nu^{2i-1}}{2}+\frac{1}{2\omega_\nu^{2i-1}})$ except in $k \le E$ places). Then f is in the list of returned interpolants of Algorithm 4.1 with probability $\ge (1-\epsilon)^\theta \ge 1-\theta\epsilon$ with $\theta = \lfloor E/2 \rfloor + 1$.*

Proof. We prove the theorem for the power basis case with $\mathrm{char}(\mathsf{K}) \neq 2$, while the other cases can be proven similarly.

By the assumption in Definition 4.2.A we have $\omega_\nu \neq 0$ and by the assumption in Definition 4.2.B we have $\Psi_t(\omega_\nu) \neq 0$ (21). None of the randomly sampled ω_ν are roots of $\Gamma_f(x)$ with probability $\ge \prod_\nu (1-\deg(\Gamma_f)/|S_\nu|)$, which by (22) is $\ge \prod_\nu (1-4B^2D/|S_\nu|) \ge (1-\epsilon)^\theta$.

There is at least one row $[\hat{a}_{\nu,i}]_{1\le i\le 2B+1}$ that has ≤ 1 error, because otherwise there would be at least $2(\lfloor E/2 \rfloor + 1) > E$ errors in total. Suppose row ν_1 has ≤ 1 error, and if there is an error it is in $\hat{a}_{\nu_1,\ell}$. Note that by the assumption in Definition 4.2.C the possible error cannot be duplicated in another row because all arguments in the other rows are different. If $\Gamma_f(\omega_{\nu_1}) \neq 0$ then $\Delta_{t+1,\ell}(\hat{\alpha}) \neq 0$ and the correct value $a_{\nu_1,\ell}$ will be among its roots. Therefore Step 4d will add f to the list of interpolants. □

The number of interpolants that Algorithm 4.1 adds to its returned list is $\le 4(\lfloor E/2 \rfloor + 1)B(2B+1)^2$. However, unlike previous deterministic algorithms, Theorem 4.1 does not state that there are at most a polynomial number of (B, D, E)-interpolants for the input data: a selection of the ω_ν's that is lucky for one (B, D, E)-interpolant may exclude another, and vice-versa.

Remark 4.2. We can execute Algorithm 4.1 without the assumptions in Definition 4.2.B–C. We detail the Chebyshev basis case. One can choose all ω_ν randomly from a single large set $S \subseteq \mathsf{K}$ such that

$$\Xi_{t_g}(\omega_1, \ldots, \omega_\theta) \prod_{\nu=1}^{\theta} \Gamma_f(\omega_\nu)\Psi_{t_g}(\omega_\nu) \neq 0 \tag{42}$$

with probability $\ge 1-\epsilon$, where

$$\Xi_{t_g}(y_1, \ldots, y_\theta) = \prod_{1\le\nu_1<\nu_2\le\theta} \prod_{i_1=1}^{2B+1} \prod_{i_2=1}^{2B+1} (y_{\nu_1}^{2i_1-1} - y_{\nu_2}^{2i_2-1}) \times (y_{\nu_1}^{2i_1-1} y_{\nu_2}^{2i_2-1} - 1) \tag{43}$$

and Γ_f, Ψ_{t_g} as in (40). Note that $\deg(\Psi_{t_g}) \le 2B^2D$ and $\deg(\Xi_{t_g}) = O(E^2B^3)$, so that the binary lengths of the elements in S are $O(\log(BDE\epsilon^{-1}))$.

However, it is possible to enforce the input requirements in Definition 4.2.B–C a-priori without randomization. For $\mathsf{K} \supseteq \mathbb{Q}$, we can choose distinct prime numbers in all sets, similarly to [2]. Moreover, if $\mathsf{K} \subseteq \mathbb{R}$ and all $\omega_\nu > 0$ and if $N - 2E \ge 2B$ for $N = \theta(2B+1)$, there cannot be two (B, D, E)-interpolants $f_1(x), f_2(x)$: the proof considers the corresponding Laurent polynomials $g_1(y), g_2(y)$ (24). The power basis case follows directly from Descartes's Rule of Signs. We describe the proof for the Chebyshev basis case. Then $g_1(y) - g_2(y)$ is a Laurent polynomial with $\le 4B$ terms which is $= 0$ at $\ge 4B$ distinct positive real values ω_ν^{2i-1} and $\omega_\nu^{-(2i-1)}$ for $(\nu, i) \notin I_{f_1}, I_{f_2}$, where I_{f_1} is the set of error locations for f_1 and I_{f_2} is the set of error locations for f_2. By Descartes's Rule of Signs $g_1 - g_2 = 0$. See also [3], [15], [1]. We have $\theta(2B+1) - 2E \ge 2B$ for $B \ge 2$ and $E \ge 2$. Note that for $E = 1$ one cannot guarantee recovery of a single interpolant from $2B+1$ values at a positive real ω (a counter-example is given in Section 1).

For $\mathsf{K} = \mathbb{C}$ one may choose roots $\neq 1$ of $x^{n_\nu} - 1$ such that each n_ν is a distinct sufficiently large prime number, that is, $n_\nu \neq n_\kappa$ for all $\kappa \neq \nu$. The condition in Definition 4.2.B can be enforced similarly. Roots of unity as arguments give numerical stability [6].

For very large degree bounds D (supersparse polynomials) and $\mathsf{K} \supseteq \mathbb{Q}$ one may be able to evaluate f modulo a prime number p, for instance if f is given by a straight-line program. One can then select the modulus p such that $p - 1 = n_1 \cdots n_\theta n^*$, where n_ν are small distinct prime numbers $> 2B + 1$ and the prime factors of n^* are larger than all n_ν. Then the sets S_ν can be chosen as the primitive roots of $x^{(p-1)/n_\nu} - 1 \pmod{p}$. The term degrees may be recovered from the derivative of f, for example; see [10]. □

5. DETERMINISTIC ALGORITHMS

Let the field of scalars be the real numbers, $\mathsf{K} = \mathbb{R}$. We wish to prove that if $\omega \in \mathbb{R}$, $\omega > 0$ and $\omega \neq 1$ ($\Longrightarrow \Psi_t(\omega) \neq 0$) for power basis and if $\omega \in \mathbb{R}$, $\omega \neq 0$, $\omega \neq -1$ and $\omega \neq 1$ ($\Longrightarrow \Psi_{t_g}(\omega) \neq 0$) for Chebyshev basis, then we always have $\Gamma_f(\omega) \neq 0$. For power basis we have by Oscar Mitchell's Theorem on the co-factor of generalized Vandermonde matrices (see Lemma A.2) and the proof of Lemma 2.5 that all coefficients of all co-factors of all $\det((\mathcal{H}_m)\downarrow_{u,v})$ have the same sign: all are real numbers ≥ 0 or all are real numbers ≤ 0. Therefore at values $\omega > 0$ all evaluated determinants are $\neq 0$. We now shall prove that for Chebyshev basis and $\mathsf{K} = \mathbb{R}$, $\omega \in \mathbb{R}$, we have for the coefficient of $\hat{\alpha} \times (-1)^{t_g+1+\mu}$ in $\hat{\mathcal{H}}_{m,\mu}$:

$$\begin{aligned}&\forall \mu, 1 \leq \mu \leq t_g + 1, \forall \omega \in \mathbb{R}, \omega \neq 0, 1, -1\colon\\ &\Big(\sum\nolimits_{u+v=t_g+1+\mu} \det((\mathcal{H}_m)\downarrow_{u,v})(\omega)\Big)\\ &\qquad - \Big(\sum\nolimits_{u+v=t_g+2-\mu} \det((\mathcal{H}_m)\downarrow_{u,v})(\omega)\Big) \neq 0. \qquad (44)\end{aligned}$$

Lemma 5.1. *Let $0 \leq \delta_1 < \delta_2 < \cdots < \delta_t$ be the term degree, $\omega \in \mathbb{R}$, $\omega \neq 0$ and let*

$$\Lambda(z) = \prod\nolimits_{j=1}^{t_g} (z - \omega^{2\eta_j}) = \sum\nolimits_{j=0}^{t_g} (-1)^{t_g - j} \lambda_j z^j \in \mathbb{R}[z], \quad (45)$$

where $\eta_1 = -\delta_t$, $\eta_{t_g} = \delta_t$, $\eta_2 = -\delta_{t-1}$, $\eta_{t_g-1} = \delta_{t-1}, \ldots$ (31). Note that $t_g = 2t - 1 \iff \delta_1 = 0 = \eta_t$, otherwise $-\eta_t = \eta_{t+1} = \delta_1$. Then for all j with $0 \leq j \leq \tau = \lfloor t_g/2 \rfloor$ we have $\lambda_j = (-1)^{t_g} \lambda_{t_g - j}$, $\lambda_j > 0$ and for all $0 \leq j \leq \tau - 1$: $\lambda_j < \lambda_{j+1}$. Note that for $t_g = 2t - 1$ we have $\lambda_t = \lambda_{t-1}$.

Proof. The proof is by induction on t_g. Suppose t_g is even, that is, $\delta_1 > 0$. We have for

$$\sum_{j=0}^{t_g} (-1)^j \lambda_j z^j = \Big(\sum_{j=0}^{t_g-2} (-1)^j \chi_j z^j\Big)\Big(z^2 - \big(\underbrace{\omega^{2\delta_t} + \frac{1}{\omega^{2\delta_t}}}_{\bar{\omega}>1}\big)z + 1\Big) \quad (46)$$

the new coefficient difference $\lambda_{j+1} - \lambda_j = \chi_{j+1} - \chi_{j-2} + (\bar{\omega} - 1)(\chi_j - \chi_{j-1})$ with $\chi_{-j'} = 0$ and $\chi_{t_g-2+j'} = 0$ for all $j' \geq 1$. Then by hypothesis for the coefficients χ_j we have $\lambda_{j+1} - \lambda_j > 0$ for $j \leq \tau - 1$. Note that for $j + 1 = \tau$ we have by hypothesis $\chi_\tau - \chi_{\tau-3} = \chi_{\tau-2} - \chi_{\tau-3} > 0$. If $t_g = 2t - 1$, in (46) we can additionally multiply with $z - 1$ instead of $z^2 - \bar{\omega}z + 1$. □

Remark 5.2. In Lemma 5.1 above, $\omega < 0$ is valid because the term degrees are squared in the term locator polynomial due to the choice of arguments, ω^{2i-1}. By that, we prevent the common argument value $1 = \omega^0$ in all blocks. As a consequence, the condition $\omega > 0$ is avoidable in our deterministic Chebyshev algorithms. However, uniqueness of the interpolant requires $\omega_\nu > 0$ for all ν (see Remark 4.2). □

Lemma 5.3. *Let $\bar{\mathcal{B}}_m$ be the matrix as in (33), and let $(\bar{\mathcal{B}}_m)\downarrow_{*,v}$ be the submatrix of $\bar{\mathcal{B}}_m$ by removing the v-th column. The determinant of the matrix $(\bar{\mathcal{B}}_m)\downarrow_{*,v}$ is*

$$\det((\bar{\mathcal{B}}_m)\downarrow_{*,v}) = \phi_{v-1} \det((\bar{\mathcal{B}}_m)\downarrow_{*,m}), \quad (47)$$

where $\phi_{t_g} = 1$ and $\phi_0, \phi_1, \ldots, \phi_{t_g-1}$ satisfy

$$\sum\nolimits_{j=0}^{t_g} (-1)^{t_g - j} \phi_j z^j = \prod\nolimits_{j=1}^{t_g} (z - \beta_j^2) \quad (\textit{see } (32)). \quad (48)$$

Proof. The coefficients $\phi_0, \phi_1, \ldots, \phi_{t-1}$ in (48) yield a linear generator and therefore satisfy the following Hankel system: $\mathcal{H}_{t_g} = \mathrm{Hankel}_{t_g}(\alpha_{-(2t_g-3)+2i}\colon i{=}0, \ldots, 2t_g - 2)$:

$$\mathcal{H}_{t_g} \begin{bmatrix} (-1)^{t_g-0}\phi_0 \\ (-1)^{t_g-1}\phi_1 \\ \vdots \\ (-1)^1 \phi_{t_g-1} \end{bmatrix} = (-1) \times \begin{bmatrix} \alpha_3 \\ \alpha_5 \\ \vdots \\ \alpha_{2t_g+1} \end{bmatrix}. \quad (49)$$

Let $\bar{\mathcal{H}}_{t_g}^{(v)}$ be the matrix obtained by substituting the v-th column of $\mathcal{H}_{t_g}$ by the right side vector in (49). By Cramer's rule, we have

$$\begin{aligned}&(-1)^{t_g-(v-1)} \phi_{v-1}\\ &= \det(\bar{\mathcal{H}}_{t_g}^{(v)})/\det(\mathcal{H}_{t_g}) = (-1)^{t_g+1-v} \det((\mathcal{H}_m)\downarrow_{m,v})/\det(\mathcal{H}_{t_g})\\ &= (-1)^{t_g+1-v} \frac{\det((\mathcal{B}_m)\downarrow_{m,*}) \det(C_m) \det((\bar{\mathcal{B}}_m)\downarrow_{*,v})}{\det((\mathcal{B}_m)\downarrow_{m,*}) \det(C_m) \det((\bar{\mathcal{B}}_m)\downarrow_{*,m})},\end{aligned}$$

where the last equality is due to (34). This concludes (47). □

Lemma 5.4. *The determinant of $(\mathcal{H}_m)\downarrow_{u,v}$ is*

$$\det((\mathcal{H}_m)\downarrow_{u,v}) = \phi_{u-1}\phi_{v-1} P\, \Psi_{t_g}^2 \quad (50)$$

where $\Psi_{t_g}(y) = \prod_{1 \leq j_1 < j_2 \leq t_g} (\beta_{j_1}^2 - \beta_{j_2}^2)$ (see (32) for β_j) and $P = \det(C_m)$ (see (33) for the matrix C_m).

Proof. The formula (50) follows from the factorization (34) of $(\mathcal{H}_m)\downarrow_{u,v}$ and applying Lemma 5.3 to the matrices $(\mathcal{B}_m)\downarrow_{u,*}$ and $(\bar{\mathcal{B}}_m)\downarrow_{*,v}$. □

Lemma 5.5. *Let $t_g \geq 1$ and let $0 < \lambda_0 < \lambda_1 < \cdots < \lambda_\tau$ for $\tau = \lfloor t_g/2 \rfloor$ and let $\lambda_{t_g - j} = \lambda_j$ for $0 \leq j \leq \tau$. Furthermore, let μ be an index with $1 \leq \mu \leq t_g + 1$. Then*

$$W_\mu = \Big(\sum_{\substack{1 \leq u,v \leq t_g+1,\\ u+v=t_g+1+\mu}} \lambda_{u-1}\lambda_{v-1}\Big) - \Big(\sum_{\substack{1 \leq u,v \leq t_g+1,\\ u+v=t_g+2-\mu}} \lambda_{u-1}\lambda_{v-1}\Big) > 0. \quad (51)$$

Proof. We define $\lambda_{t_g+j'} = 0$ and $\lambda_{-j'} = 0$ for all $j' \geq 1$. Then we have for all μ in (51):

$$W_\mu = \sum\nolimits_{j=1}^{\tau+1} (\lambda_{j+\mu-2} - \lambda_{j-\mu-1})(\lambda_{j-1} - \lambda_{j-2}). \quad (52)$$

For the second factor in the summands in (52) we have by assumption $\lambda_{j-1} - \lambda_{j-2} > 0$. The first factor $\lambda_{j+\mu-2} - \lambda_{j-\mu-1}$ is > 0 when the larger index is $j + \mu - 2 \leq \tau$. Suppose now that $j + \mu - 2 > \tau$ and $\lambda_{j+\mu-2} = \lambda_{t_g-(j+\mu-2)} < \lambda_{j-\mu-1}$ where we always have $j - \mu - 1 < \tau$. Then $t_g - (j + \mu - 2) < j - \mu - 1 \Longrightarrow t_g + 3 < 2j$ which implies $j > t_g/2 + 3/2 \geq \lfloor t_g/2 \rfloor + 3/2 > \tau + 1$, which is outside the range of j in (52). □

Combining the Lemmas 5.1, 5.4 and 5.5, we have (44), and therefore, all evaluated determinants are non-zero. A full description of the deterministic algorithms is in Section B.1.

ACKNOWLEDGMENTS

We thank the reviewers for their comments.

Zhi-Hong Yang is supported by the National Natural Science Foundation of China (12201425). Our investigations began when Zhi-Hong Yang was attending the trimester program *Recent Trends in Computer Algebra* (Sep. 18 to Dec. 11, 2023) supported by the Institut Henri Poincaré (UAR 839 CNRS-Sorbonne Université) and LabEx CARMIN (ANR-10-LABX-59-01).

REFERENCES

[1] Andrew Arnold and Erich L. Kaltofen. 2015. Error-Correcting Sparse Interpolation in the Chebyshev Basis. In *ISSAC'15 Proc. 2015 ACM Internat. Symp. Symbolic Algebraic Comput.* Association for Computing Machinery, New York, N. Y., 21–28. URL: http://users.cs.duke.edu/~elk27/bibliography/15/ArKa15.pdf.

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

[3] Allan Borodin and Prasoon Tiwari. 1991. On the decidability of sparse univariate polynomial interpolation. *Computational Complexity* 1 (1991), 67–90. URL: https://link.springer.com/article/10.1007/BF01200058.

[4] Matthew T. Comer, Erich L. Kaltofen, and Clément Pernet. 2012. Sparse Polynomial Interpolation and Berlekamp/Massey Algorithms That Correct Outlier Errors in Input Values. In *ISSAC 2012 Proc. 37th Internat. Symp. Symbolic Algebraic Comput.*, Joris van der Hoeven and Mark van Hoeij (Eds.). Association for Computing Machinery, New York, N. Y., 138–145. URL: http://users.cs.duke.edu/~elk27/bibliography/12/CKP12.pdf.

[5] R. J. Evans and I. M. Isaacs. 1976. Generalized Vandermonde determinants and roots of unity of prime order. *Proc. Amer. Math. Soc.* 58 (1976), 1–54.

[6] Mark Giesbrecht, George Labahn, and Wen-shin Lee. 2009. Symbolic-numeric sparse interpolation of multivariate polynomials. *J. Symbolic Comput.* 44 (2009), 943–959.

[7] Pascal Giorgi, Bruno Grenet, Armelle Perret du Cray, and Daniel Roche. 2022. Sparse Polynomial Interpolation and Division in Soft-linear Time, See [9], 459–468.

[8] Zhiwei Hao, Erich L. Kaltofen, and Lihong Zhi. 2016. Numerical Sparsity Determination and Early Termination. In *ISSAC'16 Proc. 2016 ACM Internat. Symp. Symbolic Algebraic Comput.*, Markus Rosenkranz (Ed.). Association for Computing Machinery, New York, N. Y., 247–254. URL: http://users.cs.duke.edu/~elk27/bibliography/16/HKZ16.pdf.

[9] Amir Hashemi (Ed.). 2022. *ISSAC '22 Proc. 2022 ACM Internat. Symp. Symbolic Algebraic Comput.* Association for Computing Machinery, New York, N. Y.

[10] Qiao-Long Huang. 2019. Sparse Polynomial Interpolation over Fields with Large or Zero Characteristic. In *Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation, ISSAC 2019, Beijing, China, July 15-18, 2019*, James H. Davenport, Dongming Wang, Manuel Kauers, and Russell J. Bradford (Eds.). ACM, 219–226. URL: https://doi.org/10.1145/3326229.3326250.

[11] Erdal Imamoglu, Erich L. Kaltofen, and Zhengfeng Yang. 2018. Sparse Polynomial Interpolation With Arbitrary Orthogonal Polynomial Bases. In *ISSAC '18 Proc. 2018 ACM Internat. Symp. Symbolic Algebraic Comput.*, Carlos Arreche (Ed.). Association for Computing Machinery, New York, N. Y., 223–230. In memory of Bobby F. Caviness (3/24/1940–1/11/2018). URL: http://users.cs.duke.edu/~elk27/bibliography/18/IKY18.pdf.

[12] Erich L. Kaltofen. 2010. Fifteen years after DSC and WLSS2 What parallel computations I do today [Invited Lecture at PASCO 2010]. In *PASCO'10 Proc. 2010 Internat. Workshop on Parallel Symbolic Comput.*, M. Moreno Maza and Jean-Louis Roch (Eds.). Association for Computing Machinery, New York, N. Y., 10–17. URL: http://users.cs.duke.edu/~elk27/bibliography/10/Ka10_pasco.pdf.

[13] Erich L. Kaltofen. 2022. Sparse Polynomial Hermite Interpolation, See [9], 469–478. URL: http://users.cs.duke.edu/~elk27/bibliography/22/Ka22herm.pdf, https://doi.org/10.1145/3476446.3535501.

[14] Erich Kaltofen and Wen-shin Lee. 2003. Early Termination in Sparse Interpolation Algorithms. *J. Symbolic Comput.* 36, 3–4 (2003), 365–400. Special issue Internat. Symp. Symbolic Algebraic Comput. (ISSAC 2002). Guest editors: M. Giusti & L. M. Pardo. URL: http://users.cs.duke.edu/~elk27/bibliography/03/KL03.pdf.

[15] Erich L. Kaltofen and Clément Pernet. 2014. Sparse Polynomial Interpolation Codes and Their Decoding Beyond Half the Minimal Distance. In *ISSAC 2014 Proc. 39th Internat. Symp. Symbolic Algebraic Comput.*, Katsusuke Nabeshima (Ed.). Association for Computing Machinery, New York, N. Y., 272–279. URL: http://users.cs.duke.edu/~elk27/bibliography/14/KaPe14.pdf.

[16] Erich L. Kaltofen and Zhi-Hong Yang. 2021. Sparse Interpolation With Errors in Chebyshev Basis Beyond Redundant-Block Decoding. *IEEE Trans. Information Theory* 67, 1 (Jan. 2021), 232–243. URL: http://users.cs.duke.edu/~elk27/bibliography/19/KaYa19.pdf, https://ieeexplore.ieee.org/document/9207761, https://arxiv.org/abs/1912.05719.

[17] Lakshman Y. N. and B. D. Saunders. 1995. Sparse polynomial interpolation in non-standard bases. *SIAM J. Comput.* 24, 2 (1995), 387–397.

A. APPENDIX: AUXILIARY STANDARD LEMMAS

The following Lemma is used in the proof of Theorem 2.4 and Theorem 3.1.

LEMMA A.1. *Let $e_i, d_i \in \mathbb{Z}$ for $1 \le i \le n$ with $d_1 < d_2 < \cdots < d_n$ and $e_1 < e_2 < \cdots < e_n$ and let $V = [y^{d_i e_j}]_{1\le i,j\le n} \in \mathbb{Z}[y, \frac{1}{y}]^{n\times n}$ be a generalized Vandermonde matrix. Then the monomial with largest degree of its determinant $\det(V)$ is y^Q with $Q = d_1e_1 + d_2e_2 + \cdots + d_ne_n$.*

PROOF. The terms in the minor expansion are $\pm y^{Q_\sigma}$ where σ is a permutation on $\{1, \ldots, n\}$ and $Q_\sigma = \sum_i d_i e_{\sigma(i)}$. If we use the entry (n, k) with $k < n$, then by induction hypothesis for dimension $n - 1$ for the minor $\det(V\!\downarrow_{n,k})$, the maximum monomial degree using the $y^{d_n e_k}$ entry is

$$Q_k = d_n e_k + \Big(\sum\nolimits_{i=1}^{k-1} d_i e_i\Big) + \Big(\sum\nolimits_{i=k}^{n-1} d_i e_{i+1}\Big). \qquad (53)$$

We set $d_i = d_k + d'_i$ with $0 < d'_{k+1} < \cdots < d'_n$ and $e_i = e_k + e'_i$ with $0 < e'_{k+1} < \cdots < e'_n$, and have

$$Q - Q_k = d'_{k+1}e'_{k+1} + \sum\nolimits_{i=k+2}^{n} (d'_i - d'_{i-1})e'_i > 0. \quad \square \qquad (54)$$

LEMMA A.2. *Let $d_i \in \mathbb{Z}$ with $d_1 < d_2 < \cdots < d_n$ and let $\mathcal{V} = [Y_j^{d_i}]_{1\le i,j\le n} \in \mathsf{K}[Y_1, \frac{1}{Y_1}, \ldots, Y_n, \frac{1}{Y_n}]^{n\times n}$ be a generalized Vandermonde matrix. Then $\det(\mathcal{V}) = F(Y_1, \ldots, Y_n)\prod_{1\le i<j\le n}(Y_i - Y_j)$, where $F(Y_1, \ldots, Y_n) \in \mathsf{K}[Y_1, \frac{1}{Y_1} \ldots, Y_n, \frac{1}{Y_n}]$ with $F \ne 0$. Moreover, if the scalar field K has characteristic 0, the coefficients of F are positive integers.*

PROOF. See [5]; the positivity of the coefficients of F is Oscar H. Mitchell's 1882 theorem. □

LEMMA A.3. *Let $\omega_1, \omega_2 \in \mathsf{K}$, $\omega_1 \ne 0$, $\omega_2 \ne 0$, $d_1, d_2 \in \mathbb{Z}$. Then*
$\omega_1^{d_1}{+}1/\omega_1^{d_1} \ne \omega_2^{d_2}{+}1/\omega_2^{d_2} \iff \big(\,\omega_1^{d_1}{\ne}\omega_2^{d_2}$ *and* $\omega_1^{d_1}{\ne}\omega_2^{-d_2}\,\big)$.

PROOF. $\omega_1^{d_1}\omega_2^{d_2}(\omega_1^{d_1} + \omega_1^{-d_1} - \omega_2^{d_2} - \omega_2^{-d_2}) = (\omega_1^{d_1}\omega_2^{d_2} - 1)(\omega_1^{d_1} - \omega_2^{d_2})$. (cf. [11, Lemma 2.1]). □

B. APPENDIX

B.1. Deterministic Error-correcting Sparse Interpolation

Input: ▸ Bounds $B \ge 2$, $E \ge 2$ for the numbers of terms and errors; note that the degree bound $D = \infty$.
▸ An arguments list $\omega_\nu \in \mathbb{R}, \omega_\nu > 0, \omega_\nu \ne 1$ for $1 \le \nu \le \theta\lfloor E/2\rfloor + 1$; (we shall require that the interpolation arguments are distinct: $\forall \nu_1, \nu_2$ with $\nu_1 \ne \nu_2, \forall i_1, i_2$ with $1 \le i_1, i_2 \le 2B + 1$: $\omega_{\nu_1}^{i_1} \ne \omega_{\nu_2}^{i_2}$ for power basis, $\omega_{\nu_1}^{2i_1-1} \ne \omega_{\nu_2}^{2i_2-1}$ and $\omega_{\nu_1}^{2i_1-1} \ne \omega_{\nu_2}^{-(2i_2-1)}$ for Chebyshev basis.)
▸ For $1 \le \nu \le \theta = \lfloor E/2\rfloor + 1$ and $1 \le i \le 2B + 1$ an array of real values $\hat{a}_{\nu,i} \in \mathbb{R}$ for power basis and $\hat{a}_{\nu,2i-1} \in \mathbb{R}$ for Chebyshev

basis.

Output: ▸ The unique (B, ∞, E)-sparse interpolant for the arguments/values (see Definition 4.1); or a flag that none exists.

```
1: For $v = 1, \dots, \theta$ Do Step 2;
   After completion, return that no interpolant exists.
2: For $t = 1, \dots, B$ [ $t_g = 1, \dots, 2B$ for Chebyshev basis ] Do Step 3;
   We try to interpolate, while correcting a single possible error, a polynomial which is sparse with $t$ terms from the values $\hat{a}_{v,i}$ for $1 \le i \le 2t + 1$ [ for Chebyshev basis: $t_g$ terms in $g(y)$ (24) from the values $\hat{a}_{v,2i-1}$ for $1 \le i \le t_g + 1$ ].
3: For $\mu = 1, \dots, 2t + 1$ [ $t_g + 1$ for Chebyshev basis ] Do Step 4;
4: We guess that the error is in $\hat{a}_{v,\mu}$ [ $\hat{a}_{v,2\mu-1}$ for Chebyshev basis ].
   4(a): Compute $\Delta_{m,\mu}(\hat{\alpha})$ for $m = t + 1$ and $\hat{a}_i = \hat{a}_{v,i}$ for $1 \le i \le m$ [ for Chebyshev basis: $m = t_g + 1$ and $\hat{a}_{\pm(2i-1)} = \hat{a}_{v,2i-1}$ for $1 \le i \le m$ ];
         See Theorems 2.7, 3.3 for the definition of $\Delta_{m,\mu}$.
   4(b): If $\Delta_{m,\mu}(\hat{\alpha}) \in \mathsf{K}$ (a constant polynomial) continue with next $\mu$;
   4(c): Compute all roots $\xi_1, \dots, \xi_b \in \mathsf{K}$ for $\Delta_{m,\mu}(\hat{\alpha}) = 0$;
   4(d): For all $\xi \in \{\xi_1, \dots, \xi_b\}$ try Prony's Algorithm on the sequence $a_i = \hat{a}_i$ for $i \neq \mu$, $a_\mu = \xi$ [ for Chebyshev basis: $a_{\pm(2i-1)} = \hat{a}_{2i-1}$ for $i \neq \mu$, $a_{\pm(2\mu-1)} = \xi$ ]; see [16, Algorithm 1 Try Prony's algorithm] for a complete description of the algorithm.
         If a valid interpolant $f(x)$ is returned, perform Step 5.
5: For all other rows $\kappa$ with $1 \le \kappa \le \theta, \kappa \neq v$ and all $1 \le i \le 2B + 1$ count for the computed interpolant $f(x)$ at row $v$ how many more values $\hat{a}_{\kappa,i}$ are $\neq f(\omega_\kappa^i)$ [ for Chebyshev basis: $\hat{a}_{\kappa,2i-1}$ are $\neq f(\frac{\omega_\kappa^{2i-1}}{2} + \frac{1}{2\omega_\kappa^{2i-1}})$ ];
   If the total count of errors in all rows is $\le E$, return $f(x)$ as the unique interpolant.
```

C. APPENDIX: DEGREE BOUND PROOFS

Proof of Lemma 2.2. Let

$$\mathcal{A}_{v,i} = \mathrm{Hankel}_i(\alpha_{v+i}\colon i{=}0, \dots, 2i{-}2) \in \mathsf{K}[x]^{i \times i},$$
$$1 \le v \le 2t + 1,\ 1 \le i \le t \text{ (see (2))}. \qquad (55)$$

Then by [14, Theorem 4]

$$\gamma_\mu^*(x) = \begin{cases} \det(\mathcal{A}_{2\mu+1,t-\mu+1}) \neq 0 & \text{if } 1 \le \mu \le t, \\ \det(\mathcal{A}_{1,\mu-t-1}) \neq 0 & \text{if } t + 2 \le \mu \le 2t + 1. \end{cases}$$

By [14, Eq. (9)] we have $\deg(\det(\mathcal{A}_{\mu,i})) \le (\mu - 1 + i^2)D$. Therefore, $\deg(\Gamma_f^*) = \sum_{\mu=2}^{2t} \deg(\gamma_\mu^*) < t^3 D \le B^3 D$ for $D \ge t \ge 1$. □

Proof of Theorem 2.3. If $\delta_1 \ge 0$, let $\Gamma_f = \Gamma_f^*$ of Lemma 2.2, then $\Gamma_f(\omega) \neq 0$ implies that $\det(\hat{H}_{t+1,\mu})$ has positive degree in $\hat{\alpha}$ for all $2 \le \mu \le 2t$. Furthermore, both $\det(\hat{H}_{t+1,1})$ and $\det(\hat{H}_{t+1,2t+1})$ have degree one in $\hat{\alpha}$ if $\omega^{\delta_1}, \dots, \omega^{\delta_t}$ are pairwise distinct. The implication (7) is proved. If $\delta_1 < 0$, then let $f^*(x) = x^{-\delta_1} f(x)$: applying Lemma 2.2 to $f^*(x)$, and $\deg(f^*(x)) \le 2D$ yields (11). □

Proof of Lemma 2.6. Let $f^*(x) = x^{-\delta_1} f(x)$, then $f^*(x)$ has term degrees $\delta'_j = \delta_j + |\delta_1| \ge 0$ for all $1 \le j \le t$. The lemma follows from applying Theorem 2.4 and Lemma 2.5 to $f^*(x)$ and substituting δ_j by δ'_j. □

Proof of Theorem 2.7. Let $\bar{\gamma}_{t+1,\mu}$ be as in Lemma 2.5 if $\delta_1 \ge 0$ or as in Lemma 2.6 if $\delta_1 < 0$, and let

$$\Gamma_f(x) = \prod_{\mu=2,\mu\neq t+1}^{2t} \bar{\gamma}_{t+1,\mu}(x).$$

Then the implication (7) follows by similar arguments as in the proof of Theorem 2.3.

Since $(\sum_{j=1}^{t} 2\delta_j) - Q'' \le (2t - \mu + 1)\delta_t$, the degree of Γ_f is no more than

$$\sum_{\mu=2,\mu\neq t+1}^{2t} (2t - \mu + 1)(\delta_t + |\delta_1|)$$
$$= 2(t^2 - t)(\delta_t + |\delta_1|) < 4B^2 D. \quad \square$$

Detail in Proof of Theorem 3.1. If there is a position $(u, v) = (u, u{-}1)$ on the bottom anti-diagonal which contains $\hat{\alpha} + \alpha_{2\mu-1}$ (see 30)) having $u{+}v = t_g{+}1{+}\mu$, which is odd, then $\deg(\beta_{u-1}) = -\deg(\beta_{t_g-(u-2)}) = -\deg(\beta_{t_g-(v-1)})$, and $\deg(\beta_{u-1}^2 \beta_{t_g-(v-1)}^2)$ $= 0$. There are 2 minors of maximum degree (35), of which one has $u_{\max}^{\text{bot}} = (t_g + 2 + \mu)/2$ and $v_{\max}^{\text{bot}} = u_{\max}^{\text{bot}} - 1$. If there is a position $(u, v) = (u, u)$ on the anti-diagonal having $u + v = t_g + 1 + \mu$, which is even, then $\deg(\beta_{u-1}^2 \beta_{t_g-(v-1)}^2) = \deg(\beta_{u-1}^2 \beta_{t_g-(u-1)}^2) < 0$ and for $(u, v) = (u + 1, u - 1)$ we have $\deg(\beta_{u-1}^2 \beta_{t_g-(v-1)}^2) = \beta_u^2 \beta_{t_g-(u-2)}^2) > 0$. The updates switch from positive to negative degree, and therefore a single minor for $u_{\max}^{\text{bot}} = v_{\max}^{\text{bot}} = (t_g + 1 + \mu)/2$ has maximum degree (35).

The top anti-diagonal (u, v) with $u + v = t_g + 2 - \mu$, whose entries in $\hat{\mathcal{H}}_{m,\mu}$ are $\alpha_{-(2\mu-1)} + \hat{\alpha}$ (see 30)) also contributes minors to the coefficient of the linear term $\hat{\alpha}$. One starts at $u = t_g + 1 - \mu$ and $v = 1$ and ends at $u = 1$ and $v = t_g + 1 - \mu$. At start $\beta_{u-1}^2 \beta_{t_g-(v-1)}^2 = \beta_{t_g-\mu}^2 \beta_{t_g}^2$. Again, the maximum degree of the minors $\det((\mathcal{H}_m)\!\downarrow_{u,v})$ is at $u_{\max}^{\text{top}} = v_{\max}^{\text{top}} = (t_g{+}2{-}\mu)/2$ if $t_g + 2 - \mu$ is even, and at $u = v - 1$ and $u_{\max}^{\text{top}} = v_{\max}^{\text{top}} - 1 = (t_g + 1 - \mu)/2$ if $t_g + 2 - \mu$ is odd.

Proof of Lemma 3.2. By Lemma A.2 above each minor $\det((\mathcal{H}_m)\!\downarrow_{u,v})$ (34) has the factor $\Psi_{t_g}^2$. Because $\gamma_{m,\mu}(y) = \gamma_{m,\mu}(1/y)$, the Laurent polynomial $y^Q \gamma_{m,\mu}(y)$ is a polynomial in $K[y]$ of degree $2Q$. Also, $\Psi_{t_g}(1/y) = \pm\Psi_{t_g}(y)$, and the largest degree term in Ψ is by (39) $\pm y^{Q'/2}$. We conclude that $y^Q \gamma_{m,\mu}(y) / (y^{Q'/2} \Psi_{t_g}(y))^2$ has degree $2(Q - Q')$. □

Proof of Theorem 3.3. Let $\bar{\gamma}_{m,\mu}(y)$ be as in Lemma 3.2 and let $\omega \in \mathsf{K}$ with $\omega \neq 0$ and $\Psi_{t_g}(\omega) \neq 0$ and $\bar{\gamma}_{m,\mu}(\omega) \neq 0$. Let $\mathcal{D}_{m,\mu}(\hat{\alpha}, y) = \det(\hat{\mathcal{H}}_{m,\mu}) \in \mathsf{K}[\hat{\alpha}, y, \frac{1}{y}]$. The Laurent polynomial $\mathcal{D}_{m,\mu}(\hat{\alpha}, \omega) \neq 0$, because $1/\omega^Q \bar{\gamma}_{m,\mu}(\omega) \Psi_{t_g}(\omega)^2 \neq 0$, which is the coefficient of $\hat{\alpha}$. Therefore $\Delta_{m,\mu}(\hat{\alpha}) = \mathcal{D}_{m,\mu}(\hat{\alpha} - a_{2\mu-1}, \omega) \neq 0$. We set $\Gamma_f(y) = \prod_{\mu=1}^{t_g} \bar{\gamma}_{m,\mu}(y)$.

For $\mu = t_g + 1$ we have by the Vandermonde factorization (34, 33) $\gamma_{m,t_g+1}(y) = \det(C_m)\Big(\prod_{j=1}^{t_g} \beta_j^3\Big)\Psi_{t_g}(y)^2$. Therefore, $\gamma_{m,t_g+1}(\omega) \neq 0$.

The degree $-Q''$ in Theorem 3.1 is

$$\le 4 \sum_{j=1}^{t} \delta_j \le 4 \sum_{j=1}^{t} (\delta_t - j + 1) = 2t(2\delta_t - t + 1).$$

Multiplying by 2 and $2t \ge t_g$ (24) yields (41). □

D. APPENDIX: NOTATION

This appendix is not included in the ISSAC 2024 Proceedings.

Symbols for main quantities (in alphabetic order):	
$\mathcal{A}_{\nu,i}$	the early termination Hankel matrix [14, Theorem 4] (55)
a_i, a_{2i-1}	the values of the interpolants $f(x)$ (3), $g(y)$ (24) at input ω^i, ω^{2i-1}
$\hat{a}_i, \hat{a}_{2i-1}$	the values including possible errors
$\hat{a}_{\nu,i}, \hat{a}_{\nu,2i-1}$	the values including possible errors in block ν (Algorithms 4.1,B.1)
α_i, α_{2i-1}	the values of the interpolants $f(x)$ (3), $g(y)$ (24) at variable-powers x^i, y^{2i-1}
$\hat{\alpha}$	the symbolic error added to a value
B	$\geq t$, an upper bound on the sparsity of f
$\mathcal{B}_{t+1}, \bar{\mathcal{B}}_{t+1}$	Vandermonde matrix factors of $\mathcal{H}_{t+1}$ (14)
$\mathcal{B}_m, \bar{\mathcal{B}}_m$	Vandermonde matrix factors of $\mathcal{H}_m$ (33)
β_j	the terms in the sparse interpolants (13, 32)
C, C_m	diagonal matrices with term coefficients on the diagonal (14, 33)
c_j	the coefficient of the j-th term of f (3,23)
D	$\geq \lvert\delta_j\rvert$, an upper bound on the absolute values of the degree of f (Section 4.1)
$\Delta_{m,\mu}(\hat{\alpha})$	the determinant of $\hat{H}_{m,\mu}$ (Theorems 2.7, 3.3)
δ_j	$\in \mathbb{Z}$ the term degrees (3,23)
E	an upper bound on the number of errors that is input to the algorithm
η_j	the term degrees of $g(y)$ (31)
$f(x)$	the interpolant polynomial (3,23)
$g(y)$	the sparse polynomial in power basis derived from the sparse Chebyshev interpolant (24)
$\gamma_{t+1,\mu}, \gamma_{m,\mu}$	the coefficients of $\hat{\alpha}$ of $\Delta_{t+1,\mu}(\hat{\alpha}), \Delta_{m,\mu}(\hat{\alpha})$ (Theorem 2.4, Lemma 3.2)
$\bar{\gamma}_{t+1,\mu}, \bar{\gamma}_{m,\mu}$	$\gamma_{t+1,\mu}, \gamma_{m,\mu}$ divided by Ψ_t, Ψ_{t_g} (Lemmas 2.5, 3.2)
Γ_f	the product of $\bar{\gamma}_{t+1,\mu}, \bar{\gamma}_{m,\mu}$ for all μ (Theorems 2.7, 3.3)
H_{t+1}, H_m	the Prony Hankel matrices (4,27)

Notation continued (in alphabetic order):	
$\hat{H}_{t+1,\mu}, \hat{H}_{m,\mu}$	the Prony Hankel matrices with one symbolic value $\hat{\alpha}$ standing in for an error (6,28)
$\mathcal{H}_{t+1}, \mathcal{H}_m$	the Prony Hankel matrices with symbolic ω (8,29)
$\hat{\mathcal{H}}_{t+1,\mu}, \hat{\mathcal{H}}_{m,\mu}$	the Prony Hankel matrices with symbolic ω and symbolic error $\hat{\alpha}$ (see 9,30)
Hankel$_\tau$	notation for $\tau \times \tau$ Hankel matrices (2)
θ	$= \lfloor E/2 + 1 \rfloor$ number of blocks (Algorithms 4.1 and B.1)
I	the locations of errors (Algorithms 4.1 and B.1)
K	a field of scalars in which the coefficients lie
ℓ	the index of a single error in a block of $2B + 1$ values
$\Lambda(z)$	the term locator polynomial (5,26)
λ_j	$\in \mathrm{K}$ the coefficients of $\Lambda(z)$ (45)
m	$= t_g + 1$ the dimension of the Hankel matrices (28,29)
μ	the index of a value in the Hankel matrix on one or two anti-diagonals (6,28)
N	the number of the argument/value pairs used for interpolation
R	the maximum error rate (Table 1)
S_ν	finite sets from which random elements are sampled (Algorithms 4.1 and B.1)
$T_n(x)$	the Chebyshev polynomial of the first kind of degree n
t, t_g	the actual number of terms of f, g
u, v	the row/column index for the minor
x, y	the variables in the sparse interpolants (3,23,24) and symbolic values for ω
ϕ_j	the coefficients of the term locator polynomial for symbolic $\omega = y$ (48)
$\Psi_t(x), \Psi_{t_g}(y)$	the product of all term difference (21,39)
z	the variable in the term locator polynomial (5,26)
ω	$\in \mathrm{K}_{\neq 0, \neq \pm 1}, \mathbb{R}_{\neq 0, \neq \pm 1}$, evaluation argument base value for the polynomials f, g
ω_ν	$\nu = 1, 2, \ldots, \theta$ evaluation argument base values for multiple blocks (Algorithms 4.1 and B.1)