Combinatorics, Probability and Computing (2026), **35**, pp. 356–374
doi:10.1017/S0963548326100364

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Trace reconstruction of matrices and hypermatrices

Wenjie Zhong[1] and Xiande Zhang[1,2]

[1]School of Mathematical Sciences, University of Science and Technology of China, Hefei, China and [2]Hefei National Laboratory, University of Science and Technology of China, Hefei, China
Corresponding author: Xiande Zhang; Email: drzhangx@ustc.edu.cn

(Received 29 November 2024; revised 5 January 2026; accepted 5 January 2026; first published online 10 March 2026)

Abstract

A *trace* of a sequence is generated by deleting each bit of the sequence independently with a fixed probability. The well-studied *trace reconstruction* problem asks how many traces are required to reconstruct an unknown binary sequence with high probability. In this paper, we study the multidimensional version of this problem for matrices and hypermatrices, where a trace is generated by deleting each row/column of the matrix or each slice of the hypermatrix independently with a constant probability. Previously, Krishnamurthy, Mazumdar, McGregor and Pal showed that $\exp(\widetilde{O}(n^{d/(d+2)}))$ traces suffice to reconstruct any unknown $n \times n$ matrix (for $d = 2$) and any unknown $n^{\times d}$ hypermatrix. By developing a dimension reduction procedure and establishing a multivariate version of the Littlewood-type result that lower bounds sparse complex polynomials around 1, we improve this upper bound by showing that $\exp(\widetilde{O}(n^{3/7}))$ traces suffice to reconstruct any unknown $n \times n$ matrix, and $\exp(\widetilde{O}(n^{3/5}))$ traces suffice to reconstruct any unknown $n^{\times d}$ hypermatrix. In contrast to the earlier bound, our new exponent is bounded away from 1 even as d becomes very large.

Keywords: Trace reconstruction; matrices; hypermatrices; Littlewood-type problems

2020 MSC Codes: Primary: 05D99, Secondary: 60C05, 68Q87

1. Introduction

Reconstructing a combinatorial object from a limited amount of sub-information is a fundamental problem in computer science and has been widely studied; for example, the sequence reconstruction problem initiated by Levenshtein in 1997 [19, 26, 32–34, 42], the deck problem introduced by Kalashnik in 1973 [17, 18, 25, 27, 29, 43], and the graph reconstruction problem with the famous Ulam's conjecture [4, 5, 20, 28, 31, 39].

Motivated by the study of reconstructing DNA sequences, the trace reconstruction problem is a probabilistic version of the sequence reconstruction problem, which was first introduced by Batu et al. [3] to deal with the multiple sequence alignment problem in computational biology. The goal of this problem is to determine the minimum number of *traces* $T(n)$ that are required to reconstruct an unknown string $x \in \{0, 1\}^n$ with high probability. Here, a trace is a random subsequence of the unknown x obtained by deleting each bit of x with a fixed probability q independently and concatenating the surviving bits in their original order. Note that the original positions in x of the surviving bits are unknown. The term *with high probability* means that the probability can be arbitrarily close to 1 as the string length n grows. The trace reconstruction problem can also be viewed as a random version of the fundamental problem related to the deletion channel in communication theory: how many independent copies need to be sent through the deletion channel so that the receiver can determine the original message.

© The Author(s), 2026. Published by Cambridge University Press.

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

For the upper bound of $T(n)$, Holenstein et al. [24] first showed that $\exp(\sqrt{n}\,\mathrm{poly}(\log n))$ traces suffice. Using tools from complex analysis, Nazarov and Peres [38] as well as De et al. [16] independently proved that $T(n) \le \exp(O(n^{1/3}))$. Recently, this was further improved to $\exp(O(n^{1/5}\log^5 n))$ by Chase [12]. As for the lower bound, Batu et al. [3] first proved that $\Omega(n)$ traces are necessary. Then Holden and Lyons [22] later proved that $T(n) \ge \Omega(n^{5/4}/\sqrt{\log n})$, which was recently improved to $\Omega(n^{3/2}/\log^7 n)$ by Chase [11]. More works on the trace reconstruction problem can be found in [1, 2, 8, 10, 13–15, 23, 30, 36, 37, 40].

For a generalisation of the trace reconstruction problem to matrices/hypermatrices, the problem can be thought as reconstructing a (vertex-labelled) graph/hypergraph from samples of subgraphs/subhypergraphs, which is a well-studied but difficult problem in graph theory. For matrices, a trace of $X \in \{0,1\}^{n\times n}$ is a random submatrix of X by deleting each row and each column independently with probability q. By extending the analytic approach in [38], Krishnamurthy et al. [30] showed that $\exp(\widetilde{O}(n^{1/2}))$ traces suffice to recover an arbitrary matrix.[1] For a general higher dimension d, a trace is defined to be a random sub-hypermatrix obtained by deleting each slice, i.e., a $(d-1)$-dimensional sub-hypermatrix of full size, independently with a constant probability q. The authors [30] similarly proved that $\exp(\widetilde{O}(n^{d/(d+2)}))$ traces suffice to recover an arbitrary d-dimensional hypermatrix $X \in \{0,1\}^{n\times d}$. Note that this bound gets closer to the trivial upper bound $\exp(O(n))$ when the dimension d becomes big.

In this paper, we aim to improve the upper bounds above. We show that $\exp(\widetilde{O}(n^{3/7}))$ traces are enough for trace reconstruction of a matrix and $\exp(\widetilde{O}(n^{5/9}))$ traces are enough for trace reconstruction of a 3-dimensional hypermatrix. For general dimension d, we further improve the upper bound $\exp(\widetilde{O}(n^{d/(d+2)}))$ to $\exp(\widetilde{O}(n^{3/5}))$ with the main exponential term $n^{3/5}$ independent of d. Our results are stated as follows.

Theorem 1.1. *For any fixed deletion probability $q \in (0,1)$, let $T_d(n)$ be the minimum number of traces that suffice to reconstruct an arbitrary hypermatrix in $\{0,1\}^{n\times d}$ with high probability. Then*

(1) $T_2(n) = \exp(O(n^{3/7}\log^{10/3} n))$;

(2) $T_3(n) = \exp(O(n^{5/9}\log^{5/2} n))$; *and*

(3) for any fixed dimension $d \ge 4$, $T_d(n) = \exp(O(n^{3/5}\log n))$.

Note that all implicit constants in the $O(\cdot)$ notation may depend on the deletion probability q and the dimension d, but are independent of n.

To get the upper bound $\exp(\widetilde{O}(n^{3/5}))$ in Theorem 1.1 (3), we generalise the Littlewood-type result for single-variable polynomials in [6] to multi-variable polynomials in the following theorem, which we think is interesting itself. We actually concern about a stronger version with sparse property, which was established by Chase [12, Theorem 6.2] for single-variable polynomials. Let $h(z_1,\dots,z_d) = \sum c_{k_1\cdots k_d} z_1^{k_1}\cdots z_d^{k_d}$ be a d-variable complex polynomial with each coefficient $c_{k_1\cdots k_d} \in \{0,\pm 1\}$. We say h is *s-sparse*, if there is some j with $1 \le j \le d$ such that $|k_j - k_j'| \ge s$ whenever two coefficients $c_{k_1\cdots k_d} = c_{k_1'\cdots k_d'} \ne 0$.

Theorem 1.2. *Let $d \ge 2$ and $h(z_1,\dots,z_d) = \sum_{k\in[n]^d} c_k z_1^{k_1}\cdots z_d^{k_d}$ be a nonzero n^μ-sparse polynomial with $\mu \in [0,1)$ and each $c_k \in \{0,\pm 1\}$. Then for any $\Delta \ge 1$ and any L with $1 \le L \le n^\Delta$,*

$$\max_{z_1,\dots,z_d\in\gamma(L)} |h| \ge e^{-O(\Delta L n^{1-\mu}\log n)}.$$

Here $[n] := \{0,1,\dots,n-1\}$ and $\gamma(L) := \{e^{i\theta} : -\pi/L \le \theta \le \pi/L\}$.

[1] For functions f and g, we say $f = \widetilde{O}(g)$ if $|f| \le C|g|\log^C |g|$ for some constant C.

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

Note that when $\mu = 0$, the sparse condition in Theorem 1.2 is trivial. Then we can get rid of the constraint $L \le n^{\Delta}$ and obtain a stronger result

$$\max_{z_1,\dots,z_d \in \gamma(L)} |h| \ge e^{-O(Ln\log n)}.$$

When $L \ge Cn^{\frac{1}{d-1}}$ for a large constant C, this greatly improves the lower bound $e^{-O(L^d \log n)}$ given in [30, Lemma 22].

We further remark that as established by Chase [12], there are intriguing similarities between trace reconstruction and the k-deck problem,[2] including their proof methods. Unlike the results of this paper, the best-known upper bound on k for the d-dimensional k-deck problem is $k = O(n^{\frac{d}{d+1}})$ [43], which approaches the trivial bound n when d grows. The problem of whether an absolute constant $\alpha \in (0,1)$ exists such that $k = O(n^{\alpha})$ for all d was raised in [43]. We wonder whether our method for trace reconstruction is applicable to improve the upper bound in the k-deck problem.

Our paper is organised as follows. In Section 2, we first recall the proof idea of Nazarov and Peres [38] and Chase [12] for trace reconstruction of sequences, then we set up the general framework for trace reconstruction of (hyper)matrices, including the concepts of multidimensional generating function (identity) and the key tools for our trace reconstruction. In Section 3, we design a dimension reduction procedure, which helps to analyse the recursive structure and sparsity of certain generating functions. In Section 4, we improve the previous upper bounds for trace reconstruction of matrices and cubes, that is Theorem 1.1 (1)–(2). In Section 5, we prove Theorems 1.2 and 1.1 (3) for $d \ge 4$.

2. Preliminaries

In this section, we first briefly review the proof framework of Nazarov and Peres [38] and Chase [12] for trace reconstruction of sequences. Then based on their ideas, we set up necessary notations and the general framework for trace reconstruction of (hyper)matrices.

For any integer ℓ, let $[\ell] := \{0, 1, \dots, \ell - 1\}$ and $[-\ell, \ell] := \{-\ell, -(\ell-1), \dots, -1, 0, 1, \dots, \ell\}$. For a number a and a set S of numbers, let $a + S := \{a + s : s \in S\}$ and $aS = \{a \cdot s : s \in S\}$. Let $\gamma := \{e^{i\theta} : -\pi \le \theta \le \pi\}$ be the unit circle in the complex plane, and $\gamma(L) := \{e^{i\theta} : -\pi/L \le \theta \le \pi/L\}$ for any $L \ge 1$. Numbers $p, q \in (0,1)$ are always fixed and satisfy $p = 1 - q$. By [38, equation (2.3)], for any $z \in \gamma(L)$, the norm of $w = \frac{z-q}{p}$ satisfies

$$|w| \le \exp(O(L^{-2})). \tag{1}$$

2.1 Trace reconstruction of sequences

To obtain the upper bound $\exp(O(n^{1/3}))$, Nazarov and Peres [38] used *single-bit* statistics to distinguish between any two distinct sequences $x, y \in \{0,1\}^n$. The main idea is to find a certain index j such that the number of traces with a 1 at this position will differ substantially enough in expectation for x and y, then the rest is the standard Chernoff bound argument. To establish the existence of such a j, they used the following simple but useful relation between the entries of traces and the entries of the original sequence,

$$\mathbb{E}\left[\sum_{j\ge 0} \widetilde{X}_j w^j\right] = p \sum_{k\ge 0}^{n-1} x_k z^k, \tag{2}$$

which is valid for any $w, z \in \mathbb{C}$ satisfying $z = pw + q$. Here $x = (x_0, \dots, x_{n-1}) \in \{0,1\}^n$ is the original sequence, $\widetilde{X} = (\widetilde{X}_0, \widetilde{X}_1, \widetilde{X}_2, \dots)$ is a random trace of x ($\widetilde{X}$ is padded with zeros to the right)

[2] The k-deck problem for sequences is to find the minimum value of k such that we can reconstruct any binary sequence of length n from the multi-set of all subsequences of length k.

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

through the deletion channel with probability q. Applying equation (2) with $a = (a_0, \ldots, a_{n-1}) := x - y$, one obtains

$$\mathbb{E}\left[\sum_{j\geq 0}(\widetilde{X}_j - \widetilde{Y}_j)w^j\right] = p\sum_{k=0}^{n-1} a_k z^k \triangleq pA(z). \tag{3}$$

Then it suffices to show that the polynomial $A(z)$ is not too small for some z close to 1 on the unit circle. Indeed, by showing that $|A(z)| \geq e^{-c_1 L}$ and $|w| = |(z-q)/p| \leq e^{c_2/L^2}$ for some $z \in \gamma(L)$, one can deduce the existence of j satisfying $|\mathbb{E}[\widetilde{X}_j - \widetilde{Y}_j]| \geq \exp(-O(n^{1/3}))$ from equaiton (3) by using pigeonhole principle and setting $L = \lfloor n^{1/3} \rfloor$.

To further improve the upper bound $\exp(O(n^{1/3}))$ to $\exp(\widetilde{O}(n^{1/5}))$, Chase [12] used the *multiple-bit* statistics to distinguish sequences $x, y \in \{0,1\}^n$ when they coincide on a long prefix, that is, y looks like x from the beginning. Note that this is the hard case to distinguish x and y.

The idea of *multiple-bit* statistics is to find a set of ℓ indices, say $0 \leq j_0 < j_1 < \cdots < j_{\ell-1} \leq n-1$, such that the number of traces with a certain subsequence, say $W \in \{0,1\}^\ell$, on the index set will differ substantially enough in expectation for x and y. To find such a set of indices, Chase generalised equation (3) to the following similar but much more complicated identity,[3]

$$\mathbb{E}\left[\sum_{j}(1_{\widetilde{X}_j=W} - 1_{\widetilde{Y}_j=W})w^{\odot j}\right] = p^\ell \sum_{k}(1_{x_k=W} - 1_{y_k=W})z^{\odot k} \triangleq p^\ell B(z), \tag{4}$$

which is valid for any $w = (w_0, \ldots, w_{\ell-1}), z = (z_0, \ldots, z_{\ell-1}) \in \mathbb{C}^\ell$ satisfying $z_i = pw_i + q$, $0 \leq i \leq \ell - 1$. Here, the two indices $j = (j_0, j_1, \ldots, j_{\ell-1})$ and $k = (k_0, k_1, \ldots, k_{\ell-1})$ of the two sums run over

$$\mathcal{I}(n,\ell) := \{(j_0, j_1, \ldots, j_{\ell-1}) \in \mathbb{Z}^\ell : 0 \leq j_0 < j_1 < \cdots < j_{\ell-1} \leq n-1\},$$

which is the collection of all sets of ℓ positions among the n positions. Then $x_k := (x_{k_0}, x_{k_1}, \ldots, x_{k_{\ell-1}})$, and $z^{\odot k}$ is defined as

$$z^{\odot k} := z_0^{k_0} z_1^{k_1-k_0-1} \cdots z_i^{k_i-k_{i-1}-1} \cdots z_{\ell-1}^{k_{\ell-1}-k_{\ell-2}-1}.$$

When $\ell = 1$ and $W = 1$, equation (4) reduces to equation (3).

As before, one needs to show that $B(z)$ in equation (4) is not too small on a certain point, which is a multivariable power series. Note that when k is a set of consecutive positions, for example, $k = k_0 + [\ell]$, then $z^{\odot k} = z_0^{k_0}$ is single-variable. The following corollary from Chase [12] tells that the partial sum over such consecutive positions is enough to control the total sum $B(z)$.

Lemma 2.1 (Corollary 6.4, Chase [12]). *For any distinct $x, y \in \{0,1\}^n$ and any $p \in (0,1)$, if for some $W \in \{0,1\}^\ell$ with $\ell \leq n$, some $z_0 \in \gamma$ and some constant $C > 0$, we have*

$$|B'(z_0)| := \left|\sum_{k\geq 0}\left(1_{x_{k+[\ell]}=W} - 1_{y_{k+[\ell]}=W}\right) z_0^k\right| \geq \exp(-C\ell \log^5 n), \tag{5}$$

then there are $z_1, \ldots, z_{\ell-1} \in [1-2p, 1]$ and a constant $C' > 0$ such that

$$\left|\sum_{k\in\mathcal{I}(n,\ell)}(1_{x_k=W} - 1_{y_k=W})z^{\odot k}\right| \geq \exp(-C'\ell \log^5 n),$$

where $z = (z_0, z_1, \ldots, z_{\ell-1})$.

Because x and y coincide on a long prefix, the polynomial $B'(z_0)$ in equation (5) could be very sparse for some carefully chosen W, i.e., a lot of zero coefficients for lower degrees. Combining the

[3] In this paper, we abuse the notations to make formulas tidy, whose meaning can be got from the content.

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

following result with $l = 2n^{1/5}$, $\mu = 1/5$ and some complex analysis, Chase [12] gave a better lower bound $|\mathbb{E}[1_{\widetilde{X}_j=W} - 1_{\widetilde{Y}_j=W}]| \geq \exp(-\widetilde{O}(n^{1/5}))$ for some j. This implies that $\exp(\widetilde{O}(n^{1/5}))$ traces suffice to distinguish between any given pair of sequences x and y, and thus suffice to reconstruct the original unknown sequence.

Theorem 2.2 (Theorem 6.2, Chase [12]). *For any $\mu \in (0,1)$, there is some constant $C > 0$ such that for any $n \geq 2$ and any polynomial $f(z) = 1 - \epsilon z^d + \sum_{j=n^\mu}^{n} c_j z^j$ with $1 \leq d < n^\mu$, $\epsilon \in \{0,1\}$ and $|c_j| \leq 1$ for each j, it holds that*

$$\max_{|\theta| \leq n^{-2\mu}} |f(e^{i\theta})| \geq \exp(-Cn^\mu \log^5 n).$$

2.2 Set up for higher dimensions

In this subsection, we set up necessary notations and preliminary results for trace reconstruction of (hyper)matrices. For a fixed integer $d \geq 2$, we write $\{0,1\}^{n^{\times d}}$ instead of $\{0,1\}^{n\times\cdots\times n}$ for convenience, each element of which is an $n^{\times d}$-hypermatrix. We call n the length and d the dimension.

For $X \in \{0,1\}^{n^{\times d}}$, the position of every entry is indexed by an element $k = (k_1, k_2, \ldots, k_d) \in [n]^d$, and this entry is denoted by X_k. Next, we generalise this indexing notation by allowing each coordinate k_i to be replaced with a tuple of coordinates along that direction, so that the index specifies not just an entry, but a sub-hypermatrix. Formally, for a sub-hypermatrix of X of length ℓ obtained by projecting onto the first r dimensions, we can still describe its position using one combined index $k = (k_1, k_2, \ldots, k_d)$, where each k_i with $1 \leq i \leq r$ is now a tuple $(k_{i0}, k_{i1}, \ldots, k_{i,\ell-1}) \in \mathcal{I}(n, \ell)$, while for $r+1 \leq i \leq d$, the coordinates k_i remain single elements of $[n]$. Then the sub-hypermatrix is also denoted by X_k. Let $\mathcal{I}(n^{\times d}, \ell^{\times r})$ be the collection of all such positions k for fixed $0 < \ell \leq n$ and $0 \leq r \leq d$. For example, when $X \in \{0,1\}^{n^{\times 2}}$ is an $n \times n$ matrix, if $k = ((1,4,5),2)$, then $X_k = (X_{(1,2)}, X_{(4,2)}, X_{(5,2)})$, which is a sub-matrix formed by the 1st, 4th and 5th entries in the second column. When X_k is a block, then each of the r former k_is for $1 \leq i \leq r$ must be of the form $k_{i0} + [\ell]$. In this case, we simply denote the position by $k + [\ell]^r$ with $k = (k_1, k_2, \ldots, k_d) \in [n]^d$ indicating the first corner entry's position. Note that when $\ell = 1$ or $r = 0$, $\mathcal{I}(n^{\times d}, 1) = [n]^d$.

Similarly for $0 \leq r \leq d$, let $\mathbb{C}(d, \ell^{\times r}) = \mathbb{C}^\ell \times \cdots \times \mathbb{C}^\ell \times \mathbb{C} \times \cdots \times \mathbb{C}$, where $\mathbb{C}^\ell$ repeats r times and $\mathbb{C}$ repeats $d - r$ times. So any $(z_1, \ldots, z_d) \in \mathbb{C}(d, \ell^{\times r})$ satisfies $z_i = (z_{i0}, \ldots, z_{i,\ell-1}) \in \mathbb{C}^\ell$ for $1 \leq i \leq r$ and $z_i \in \mathbb{C}$ for $r+1 \leq i \leq d$. When $\ell = 1$ or $r = 0$, $\mathbb{C}(d,1) = \mathbb{C}^d$.

Now, for a $W \in \{0,1\}^{\ell^{\times r}}$ and a hypermatrix $X \in \{0,1\}^{n^{\times d}}$, we define the *$W$-generating function of X* as

$$g(z) = \sum_k 1_{X_k = W} z_1^{\odot k_1} \cdots z_r^{\odot k_r} \cdot z_{r+1}^{k_{r+1}} \cdots z_d^{k_d},$$

where $k = (k_1, \ldots, k_d)$ runs through $\mathcal{I}(n^{\times d}, \ell^{\times r})$, and $z = (z_1, \ldots, z_d) \in \mathbb{C}(d, \ell^{\times r})$. In fact, this is a polynomial over $\mathbb{C}$ with $r\ell + d - r$ variables. When $d = 1$, $r = 0$ and $W = 1$, it reduces to $A(z)$ in equation (3). When $d = r = 1$, it reduces to $B(z)$ in equation (4). Note that when $r < d$, this function is determined by all $\ell^{\times r}$-subhypermatrices inside the first r dimensions of X. For instance, when $d = 2$ and $r = 1$, g is the generating function of columns of length ℓ in the matrix X.

Accordingly, we have the following *W-generating identity of X*, for any $W \in \{0,1\}^{\ell^{\times r}}$ and $X \in \{0,1\}^{n^{\times d}}$, which generalises equations (3) and (4),

$$\mathbb{E}\left[\sum_j 1_{\widetilde{X}_j = W} w_1^{\odot j_1} \cdots w_r^{\odot j_r} \cdot w_{r+1}^{j_{r+1}} \cdots w_d^{j_d}\right] = p^{r\ell+d-r} g(z). \tag{6}$$

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

Here $j=(j_1,\dots,j_d)$ runs through $\mathcal{I}(n^{\times d},\ell^{\times r})$, and $w=(w_1,\dots,w_d)\in\mathbb{C}(d,\ell^{\times r})$ satisfies $z=pw+q$, i.e., each pair of corresponding entries in z and w satisfies this relation. From now on, all appeared w accompanied by z satisfy this relation. We move the proof of equation (6) to Appendix A.

To state the general framework of trace reconstruction of hypermatrices, we define a function $\theta(w)=\max\{|w|,1\}$ for all $w\in\mathbb{C}$. Then for simplicity, no matter $w\in\mathbb{C}$, or in $\mathbb{C}^\ell$, or in $\mathbb{C}(d,\ell^{\times r})$, we define $\theta(w)$ to be the product of θ-values of all complex numbers in w.

Lemma 2.3. *For any deletion probability $q\in(0,1)$, and any hypermatrix $X\in\{0,1\}^{n^{\times d}}$ through the deletion channel, let $m=\Omega(\log n)$ be a positive integer. If for any other $Y\in\{0,1\}^{n^{\times d}}$, there is some $W\in\{0,1\}^{\ell^{\times r}}$ with $\ell=O(m/\log n)$ and $0\le r\le d$, such that the W-generating function[4] g of $X-Y$ satisfies*

$$|g(z)|\ge\exp(-Cm)\ \text{for some } w\in\mathbb{C}(d,\ell^{\times r})\ \text{with}\ \theta(w)\le\exp(Cm/n)$$

for some constant $C>0$, then $\exp(O(m))$ traces suffice to reconstruct X with high probability.

Proof. By equation (6), we write the W-generating identity of $X-Y$:

$$\mathbb{E}\Big[\sum_j\big(1_{\widetilde{X}_j=W}-1_{\widetilde{Y}_j=W}\big)w_1^{\odot j_1}\cdots w_r^{\odot j_r}\cdot w_{r+1}^{j_{r+1}}\cdots w_d^{j_d}\Big]=p^{r\ell+d-r}g(z).$$

For the right hand side, $|p^{r\ell+d-r}g(z)|\ge\exp(-O(\ell+m))\ge\exp(-O(m))$. Then by the identity,

$$\begin{aligned}\exp(-O(m))&\le\left|\mathbb{E}\Big[\sum_j\big(1_{\widetilde{X}_j=W}-1_{\widetilde{Y}_j=W}\big)w_1^{\odot j_1}\cdots w_r^{\odot j_r}\cdot w_{r+1}^{j_{r+1}}\cdots w_d^{j_d}\Big]\right|\\&\le\sum_j\left|\mathbb{E}\big[1_{\widetilde{X}_j=W}-1_{\widetilde{Y}_j=W}\big]\right|\theta(w)^n\\&\le\sum_j\left|\mathbb{E}\big[1_{\widetilde{X}_j=W}-1_{\widetilde{Y}_j=W}\big]\right|\exp(Cm).\end{aligned}$$

By pigeonhole principle, we can find some $j\in\mathcal{I}(n^{\times d},\ell^{\times r})$ and some constant $C_1>0$ such that

$$\left|\mathbb{E}\big[1_{\widetilde{X}_j=W}-1_{\widetilde{Y}_j=W}\big]\right|\ge\exp(-C_1m).$$

Suppose that T i.i.d. traces $\widetilde{U}^1,\dots,\widetilde{U}^T$ of the original hypermatrix X are observed. We establish a simple algorithm that on input T traces and a pair (X,Y), outputs X if

$$\left|\frac{1}{T}\sum_{t=1}^T\widetilde{U}_j^t-\mathbb{E}_X[\widetilde{X}_j]\right|<\left|\frac{1}{T}\sum_{t=1}^T\widetilde{U}_j^t-\mathbb{E}_Y[\widetilde{Y}_j]\right|$$

for the index set j fixed above. By the union bound and Hoeffding's inequality,

$$\mathbb{P}_X[X\text{ cannot be recovered}]\le\sum_{Y\ne X}\mathbb{P}_X[X\text{ is not output from }(X,Y)]\le2^{n^d}\exp\left(-\frac{T}{2}\exp(-2C_1m)\right).$$

Taking $T=\exp(C_2m)$ with $C_2>2C_1+\frac{2d\log n}{m}$ makes the above probability tend to 0. □

Lemma 2.3 reduces the trace reconstruction problem to the existence of a smaller hypermatrix W such that the W-generating function of $X-Y$ has a big value at some restricted point. Next, we give a useful result about lower bounding a complex polynomial, which will be repeatedly used to derive lower bounds of W-generating functions.

[4] The W-generating function of $X-Y$ is the one of X minus the one of Y.

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

Lemma 2.4. *Let m be a sufficiently large integer and $a = a(m) \in (0, 1]$. For a polynomial $f(z) = z^{m_0}(c_0 + c_1 z + \cdots) \in \mathbb{C}[z]$ with $m_0 \le m$, if $|c_0| \ge e^{-O(m^a)}$ and $\sum_i |c_i| \le e^{O(m^a)}$, then there exist some $w \in \mathbb{C}$ with $|w| \le 1$ and some constant $C > 0$, such that*

$$|f(z)| \ge \exp\left(-Cm^{\frac{1+2a}{3}}\right), \quad \text{where } z = pw + q.$$

In particular, when $|c_0| = 1$ and $|c_i| \le 1$, there exists some w with $|w| \le 1$, such that $|f(z)| \ge \exp(-O(m^{1/3}))$.

Proof. Denote $f(z) = z^{m_0} f_1(z)$. Then $|f_1(z)| \le \sum_i |c_i| \le e^{O(m^a)}$ for any z with $|z| \le 1$. For some positive integer L, define a polynomial

$$F(z) = \prod_{1 \le b \le L} f_1(z e^{2\pi i \frac{b}{L}}).$$

By the maximum modulus principle, there exists some $z' \in \rho\gamma$ with $\rho = 1 - \frac{7}{pL^2}$ such that

$$|F(z')| \ge |F(0)| = |f_1(0)|^L = |c_0|^L \ge e^{-O(m^a L)}.$$

We may choose b in $\{1, 2, \ldots, L\}$ such that $z := z' e^{2\pi i \frac{b}{L}} \in \rho\gamma(L)$. Fixing this z, we have

$$e^{-O(m^a L)} \le |F(z')| \le |f_1(z)| \cdot e^{O(m^a (L-1))}.$$

Then $|f_1(z)| \ge e^{-O(m^a L)}$. Taking $L = \lceil \frac{4}{p} m^{\frac{1-a}{3}} \rceil$, we have

$$|f(z)| = \rho^{m_0} |f_1(z)| \ge \left(1 - \frac{7}{pL^2}\right)^m \cdot \exp(-O(m^a L)) \ge \exp\left(-Cm^{\frac{1+2a}{3}}\right)$$

for some constant $C > 0$.

It is left to show that the corresponding $w = \frac{z-q}{p}$ satisfies $|w| \le 1$, which is true by the following fact:

$$|w| \le 1, \ \text{whenever } z \in \rho\gamma(L) \text{ with } L \ge \frac{4}{p} \text{ and } \rho = 1 - \frac{7}{pL^2}. \tag{7}$$

Indeed, since $z = \rho e^{i\theta}$ with $|\theta| \le \pi/L$, we have

$$|w|^2 = \left|1 + \frac{\rho e^{i\theta} - 1}{p}\right|^2 \le 1 + \frac{2}{p}(\rho - 1) + \frac{1}{p^2}|\rho e^{i\theta} - 1|^2 = 1 + \frac{2}{p}(\rho - 1) + \frac{1}{p^2}(\rho^2 - 2\rho\cos\theta + 1)$$
$$\le 1 + \frac{2}{p}(\rho - 1) + \frac{1}{p^2}((\rho - 1)^2 + \theta^2) \le \left(1 + \frac{\rho - 1}{p}\right)^2 + \frac{\pi^2}{p^2 L^2} < 1.$$

When $|c_0| = 1$ and $|c_i| \le 1$, we prove the result slightly differently. Write $z = \rho z' \in \rho\gamma$ with the same $\rho = 1 - \frac{7}{pL^2}$. Then $f(z) = z^{m_0} f'(z')$, where $f'(z') = c_0 + \rho c_1 z' + \cdots + \rho^i c_i (z')^i + \cdots$ with $|\rho^i c_i| \le 1$. Apply Corollary 3.2 of Borwein and Erdélyi [6] to get $|f'(z')| \ge e^{-O(L)}$ for some $z' \in \gamma(L)$. Fixing z' and taking $L = m^{1/3}$, we have

$$|f(z)| = \rho^{m_0} |f'(z')| \ge \left(1 - \frac{7}{pL^2}\right)^m \cdot \exp(-O(L)) \ge \exp(-O(m^{1/3})).$$

The corresponding $w = \frac{z-q}{p}$ satisfies $|w| \le 1$ by (7). The proof is completed. □

Before closing this section, we introduce the so-called W-contiguous generating function. For any distinct hypermatrices $X, Y \in \{0, 1\}^{n \times d}$ and any hypermatrix $W \in \{0, 1\}^{\ell \times d}$ with $\ell \le n$, we

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

define the *W-contiguous generating function of* $X - Y$ by

$$h(z_1, \ldots, z_d) = \sum_k \left[1_{X_{k+[\ell]^d}=W} - 1_{Y_{k+[\ell]^d}=W}\right] z_1^{k_1} \cdots z_d^{k_d}, \tag{8}$$

where $k = (k_1, \ldots, k_d)$ runs through $[n]^d$. Note that W is of the same dimension d as X, Y but of a shorter length. When $d = 1$, the function h reduces to the function B' in equation (5).

3. Dimension reduction

Recall that in the sequence version, Chase [12] classified a pair of sequences into two cases depending on whether or not they look alike at the beginning. When two sequences x and y coincide with each other on a prefix of length $\Theta(n^{1/5})$, that is, $\Theta(n^{1/5})$ contiguous zeros at the beginning of $a = x - y$, Chase applied the W-generating identity to distinguish them by establishing the existence of a powerful W-generating function; for the other case, that is, x does not look like y at the beginning, they can be easily distinguished by a trick of Peres and Zhai [40]. It is a natural thought to apply this case-by-case discussion to hypermatrices. However, in the high-dimensional version, there are many intermediate states between alike and unlike; roughly say, two hypermatrices might look alike along some dimensions but unlike along other dimensions. To facilitate the application of the generating identities, we introduce a dimension reduction procedure to find out these dimensions, thereby efficiently classifying a pair of hypermatrices.

Specifically, we design a dimension reduction procedure on $A = X - Y \in \{0, \pm 1\}^{n^{\times d}}$, to measure the similarities between X and Y. Roughly speaking, we reduce A to a sub-hypermatrix with one dimension lower; one can view it as a slice of A, which separates the thinnest all-zero part of A from the other part. Repeating this procedure on the sub-hypermatrix iteratively until the dimension reduces to zero. Then the thicknesses of the all-zero parts (λ_i's below) in this reduction will be our criterion for a classification. This procedure will provide a nice structure of all related generating functions and enable us to analyse bounds of those functions case-by-case. We give a formal definition of dimension reductions below.

For any hypermatrices $A \in \{0, \pm 1\}^{n^{\times d}}$, let f be the generating function of A, that is $f(z_1, z_2, \ldots, z_d) = \sum_k A_k z_1^{k_1} \cdots z_d^{k_d}$, where $k = (k_1, \ldots, k_d)$ runs over $[n]^d$. Now, we define a sequence of hypermatrices $A^d = A, A^{d-1}, \ldots, A^1, A^0 = \pm 1$, associated with a sequence of integers $\lambda_d \le \lambda_{d-1} \le \ldots \le \lambda_1$ as follows. Each A^i will be a nonzero sub-hypermatrix of A on some position $(k_1, \ldots, k_d)$ in $\mathcal{I}(n^{\times d}, n^{\times i})$ for $0 \le i \le d$, but we index its entry position only using the first i parameters $(k_1, \ldots, k_i)$. So in fact, A^i will be of dimension i.

For each $i \ge 1$, we define the reduction from A^i to A^{i-1} iteratively. Suppose we have obtained a sequence of nonzero hypermatrices $A^d = A, A^{d-1}, \ldots, A^i$, and a sequence of non-negative integers $\lambda_d \le \lambda_{d-1} \le \ldots \le \lambda_{i+1}$. Let λ_i be the least integer such that

$$\text{some entry } A^i_{k_1,\ldots,k_i} \neq 0 \text{ with } \min\{k_1, \ldots, k_i\} = \lambda_i \text{ or } \max\{k_1, \ldots, k_i\} = n - 1 - \lambda_i.$$

Clearly $\lambda_i \le \lfloor \frac{n-1}{2} \rfloor$. After a permutation on the set of dimensions and possibly an element reversion along some dimension, we have

$$\text{any entry } A^i_{k_1,\ldots,k_i} = 0 \text{ with } k_i < \lambda_i; \text{and some entry } A^i_{k_1,\ldots,k_i} \neq 0 \text{ with } k_i = \lambda_i.$$

Then let A^{i-1} be a sub-hypermatrix of A^i by restricting $k_i = \lambda_i$, that is a slice of A^i. Clearly $A^{i-1} \neq O$. Let $f_i(z_1, \ldots, z_i)$ be the generating function of A^i, then it can be written as

$$f_i(z_1, \ldots, z_i) = z_i^{\lambda_i}(f_{i-1}(z_1, \ldots, z_{i-1}) + z_i \cdot *), \tag{9}$$

where f_{i-1} is the generating function of A^{i-1} and the symbol $*$ denotes an uncertain polynomial.

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

After d steps, we succeed to make a dimension reduction $\mathcal{R}: A \to A^{d-1} \to \cdots \to A^1 \to A^0 = \pm 1$, with a sequence of integers $0 \le \lambda_d \le \lambda_{d-1} \le \cdots \le \lambda_1 \le \lfloor \frac{n-1}{2} \rfloor$, such that each A^{i-1} is a slice of A^i whose small side contains only zero entries. If $A = X - Y$, then we say the two hypermatrices X and Y are $(\lambda_1, \lambda_2, \ldots, \lambda_d)$-*identical* with respect to the dimension reduction $\mathcal{R}: A = X - Y \to A^{d-1} \to \cdots \to A^1 \to \pm 1$. Note that in the case that $\lambda_{r+1} < l \le \lambda_r$ for some $r \ge 1$ and some proper threshold l, it roughly means that on some r dimensions X looks like Y, but on the other dimensions, X does not look like Y.

Before giving a construction of the required W in Lemma 2.3, we introduce the conception of periodic hypermatrices. For any positive integers $s < \ell$, we say a hypermatrix $W \in \{0,1\}^{\ell \times d}$ is s-*periodic*, if W has a nonzero period $t \in [-s, s]^d$, that is, for any $k \in [\ell]^d$ with $k + t \in [\ell]^d$, we have $W_k = W_{k+t}$. Otherwise, we say W is s-*aperiodic*.

Lemma 3.1. *Suppose that distinct hypermatrices $X, Y \in \{0,1\}^{n \times d}$ are $(\lambda_1, \lambda_2, \ldots, \lambda_d)$-identical with respect to a dimension reduction $\mathcal{R}: A^d = X - Y \to A^{d-1} \to \cdots \to A^1 \to \pm 1$. If $\lambda_r \ge \ell$ for some $r \ge 1$ and an odd number $\ell \le \lfloor \frac{n-1}{2} \rfloor$, then there exists a hypermatrix $W \in \{0,1\}^{\ell \times r}$, such that the followings hold.*

(a) For each $r \le i \le d$, let g_i be the W-generating function of A^i. Then

$$g_{i+1}(z_1, \ldots, z_{i+1}) = z_{i+1}^{\lambda_{i+1}} (g_i(z_1, \ldots, z_i) + z_{i+1} \cdot *), \ r \le i \le d-1, \tag{10}$$

where $*$ denotes uncertain polynomials;

(b) Let h be the W-contiguous generating function of A^r. Then h is nonzero and $\lfloor \frac{\ell-1}{4} \rfloor$-sparse.

Proof. Property (a) trivially holds for any W by the definitions of λ_i.

For Property (b), let $A^r = X^r - Y^r$, where X^r and Y^r are the corresponding r-dimensional sub-hypermatrices of X and Y, respectively. We will find the hypermatrix W in X^r or Y^r. Let $H = \{j \in [n]^r : A^r_j \ne 0\}$ be the collection of positions with nonzero entries in A^r. View H as a point set in the Euclidean space E^r. Then there is an $(r-1)$-dimensional hyperplane α such that $\alpha \cap H = j$ for some $j \in H$ and the whole set H lies on exactly one side of α. Geometrically, the hyperplane α is tangent to H. Since $\lambda_r \ge \ell$, we have $j + [-\frac{\ell-1}{2}, \frac{\ell-1}{2}]^r := \jmath \subset [n]^r$. Let $W_1 = X^r_\jmath$ and $W_2 = Y^r_\jmath$. Then $W_1 \ne W_2$ since $X^r_j \ne Y^r_j$. So if we take $W \in \{W_1, W_2\}$, then the W-contiguous generating function

$$h(z_1, \ldots, z_r) = \sum_{k \in [n]^r} \left[1_{X^r_{k+[\ell]^r} = W} - 1_{Y^r_{k+[\ell]^r} = W} \right] z_1^{k_1} z_2^{k_2} \cdots z_r^{k_r},$$

is nonzero.

It is left to show the sparsity of h. Denote $s = \lfloor \frac{\ell-1}{4} \rfloor$. First, we claim that if W is s-aperiodic, then h is s-sparse. Otherwise, suppose that there exist distinct $k', k'' \in [n]^r$ with $|k'_i - k''_i| < s$ for all $1 \le i \le r$, such that, without loss of generality, $X^r_{k'+[\ell]^r} = X^r_{k''+[\ell]^r} = W$. Then for any $k \in [\ell]^r$ with $k + (k'' - k') \in [\ell]^r$, $W_k = X^r_{k''+k} = X^r_{k'+k+(k''-k')} = W_{k+(k''-k')}$. This implies that W has a period $(k'' - k') \in [-s, s]^r$, contradicting to the aperiodicity of W.

By the claim, we need to show that one of W_1 and W_2 is s-aperiodic. Suppose that both W_1 and W_2 are s-periodic, and let $p_1, p_2 \in [-s, s]^r$ be their periods, respectively. Then $j + p_1 + p_2 \in \jmath$. Choose suitable p_1 from $\{\pm p_1\}$ and p_2 from $\{\pm p_2\}$, such that $p_1 + p_2 \ne 0$ and they point to the same side of α against H. On this side, corresponding entries in X^r and Y^r are equal except $X^r_j \ne Y^r_j$. However, combining the periodicity of W_1 and W_2, we have

$$X^r_j = X^r_{j+p_1} = Y^r_{j+p_1} = Y^r_{j+p_1+p_2} = X^r_{j+p_1+p_2} = X^r_{j+p_2} = Y^r_{j+p_2} = Y^r_j,$$

a contradiction. So we complete the proof. □

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

In what follows, under the notation of a dimension reduction $\mathcal{R}: A \to A^{d-1} \to \cdots \to A^1 \to \pm 1$, we always denote f_i the generating function of A^i, g_i the W-generating function of A^i for some related W, and $*$ an uncertain polynomial.

4. Trace reconstruction of matrices and cubes

In this section, we will give upper bounds for trace reconstruction of matrices and cubes, proving Theorem 1.1 (1)-(2). For matrices, we only need to show that for any matrix pair (X, Y), we can find the existence of a matrix W so that the W-generating function of $X - Y$ satisfies the conditions in Lemma 2.3 with $m = n^{3/7} \log^{10/3} n$.

Lemma 4.1. *For any distinct matrices $X, Y \in \{0,1\}^{n\times n}$, there exists some $W \in \{0,1\}^{\ell \times r}$ with $\ell = 4n^{1/7} + 1$ and $0 \le r \le 1$, such that the W-generating function $g(z_1, z_2)$ of $X - Y$ satisfies*

$$|g(z_1, z_2)| \ge \exp\left(-Cn^{3/7} \log^{10/3} n\right) \text{ for some } w = (w_1, w_2) \in \mathbb{C}(2, \ell^{\times r}) \text{ with } \theta(w) \le \exp\left(Cn^{-4/7}\right),$$

where $C > 0$ is a constant.

Proof. Suppose that X and Y are (λ_1, λ_2)-identical with respect to a dimension reduction $\mathcal{R}: A = X - Y \to A^1 \to \pm 1$.

Case 1. $\lambda_1 < \ell$.

Set $r = 0$ and $W = 1$. Let $f(z_1, z_2)$ be the generating function of A. It is sufficient to show that

$$|f(z_1, z_2)| \ge e^{-O(\ell^{5/9})} \text{ for some } w_1, w_2 \in \mathbb{C} \text{ with } |w_1|, |w_2| \le 1.$$

By equation (9),

$$f(z_1, z_2) = z_2^{\lambda_2}(f_1(z_1) + z_2 \cdot *), \ \ f_1(z_1) = z_1^{\lambda_1}(\pm 1 + z_1 \cdot *).$$

Applying Lemma 2.4 for $m = \ell$ and $|c_0| = 1, |c_i| \le 1$, we have

$$|f_1(z_1)| \ge e^{-O(\ell^{1/3})} \text{ for some } w_1 \in \mathbb{C} \text{ with } |w_1| \le 1.$$

Fix w_1 and z_1, and let $f'(z_2) := f(z_1, z_2)$. We would like to apply Lemma 2.4 to $f'(z_2)$ again. Since $m_0 = \lambda_2 \le \lambda_1 < \ell$, $|c_0| = |f_1(z_1)| \ge e^{-O(\ell^{1/3})}$, and $\sum_i |c_i|$ is at most the number of nonzero terms in A, which is upper bounded by $n^2 \le e^{O(\ell^{1/3})}$, then by Lemma 2.4 with $m = l$ and $a = 1/3$, we have

$$|f(z_1, z_2)| = |f'(z_2)| \ge e^{-O(\ell^{5/9})} \text{ for some } w_2 \in \mathbb{C} \text{ with } |w_2| \le 1.$$

Case 2. $\lambda_1 \ge \ell$.

Set $r = 1$ and take the sequence $W \in \{0,1\}^{\ell}$ in Lemma 3.1. Let $g(z_1, z_2)$ be the W-generating function of A, where $(z_1, z_2) \in \mathbb{C}(2, \ell^{\times 1})$. By equation (10),

$$g(z_1, z_2) = z_2^{\lambda_2}(g_1(z_1) + z_2 \cdot *),$$

where g_1 is the W-generating function of the sequence A^1. By Lemma 3.1 (b), the W-contiguous generating function of A^1, say $h(z)$, is nonzero and $n^{1/7}$-sparse. Let d_0 be the minimum degree of h. Then we can write

$$h(z) = \pm z^{d_0}\left(1 - \epsilon z^{d_1} + \sum_{j=n^{1/7}}^{n} c_j z^j\right) := \pm z^{d_0} h_0(z)$$

with $1 \le d_1 < n^{1/7}, \epsilon \in \{0,1\}$ and $|c_j| \le 1$ for each j. Clearly, $h_0(z)$ satisfies the condition in Theorem 2.2 for $\mu = 1/7$. Hence, $|h_0(e^{i\theta})| \ge \exp\left(-O(n^{1/7} \log^5 n)\right)$ for some $|\theta| \le n^{-2/7}$. Let $z_0 = e^{i\theta} \in \gamma(\pi n^{2/7}) \subset \gamma(n^{2/7})$. Then $|h(z_0)| = |h_0(z_0)| \ge \exp\left(-O(n^{1/7} \log^5 n)\right)$. Applying

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

Lemma 2.1, we get

$$|g_1(z_1)| \geq e^{-O(n^{1/7}\log^5 n)}$$

for some $z_1 = (z_{10}, \ldots, z_{1,\ell-1})$ with $z_{10} = z_0$ and $z_{1j} \in [1-2p, 1]$, $j \geq 1$. By equation (1), the corresponding $w_1 \in \mathbb{C}^\ell$ satisfies $\theta(w_1) \leq e^{O(n^{-4/7})}$.

Fixing w_1 and z_1, let $g'(z_2) = g(z_1, z_2)$ which is single-variable. We apply Lemma 2.4 to $g'(z_2)$. Since $m_0 = \lambda_2 < n$, $|c_0| = |g_1(z_1)| \geq e^{-O(n^{1/7}\log^5 n)}$, and $\sum_i |c_i|$ is at most the number of nonzero terms in the Littlewood polynomial $g(z_1, z_2)$, which is upper bounded by $n\binom{n}{\ell} \leq e^{O(\ell \log n)} \leq e^{O(n^{1/7}\log^5 n)}$, then by Lemma 2.4 with $m = n$ and $a = \frac{1}{7} + 5\frac{\log\log n}{\log n}$, we have

$$|g(z_1, z_2)| = |g'(z_2)| \geq e^{-O(n^{3/7}\log^{10/3} n)} \text{ for some } w_2 \in \mathbb{C} \text{ with } |w_2| \leq 1. \qquad \square$$

Combining Lemmas 2.3 and 4.1, Theorem 1.1 (1) immediately follows.

For trace reconstruction of cubes, we can make the same classification as for matrices, resulting in the following lemma, whose proof is moved to Appendix B. Hence Theorem 1.1 (2) follows by applying Lemma 2.3 with $m = n^{5/9}\log^{5/2} n$.

Lemma 4.2. *For any distinct cubes $X, Y \in \{0,1\}^{n\times n\times n}$, there exists some $W \in \{0,1\}^{\ell\times r}$ with $\ell = 4n^{1/9} + 1$ and $0 \leq r \leq 1$, such that the W-generating function $g(z_1, z_2, z_3)$ of $X - Y$ satisfies*

$$|g(z)| \geq \exp\left(-Cn^{5/9}\log^{5/2} n\right) \text{ for some } w=(w_1, w_2, w_3) \in \mathbb{C}(3, \ell^{\times r}) \text{ with } \theta(w) \leq \exp\left(\frac{C\log^{5/2} n}{n^{4/9}}\right),$$

where $C > 0$ is a constant.

Following the proof ideas for matrices and cubes, one may get an upper bound $\exp(\widetilde{O}(n^{1-\frac{4}{2d+3}}))$ for hypermatrices of general dimension $d \geq 4$, which is slightly better than the bound $\exp(\widetilde{O}(n^{d/(d+2)}))$ of Krishnamurthy et al. [30]. However, this is still close to the trivial bound $\exp(O(n))$ for high dimensions unfortunately. To settle this problem, we establish a Littlewood-type result for multi-variable polynomials with certain sparse property, that is Theorem 1.2, which generalises the single-variable version in Theorem 2.2. Such a result on lower bounding sparse polynomials at some restricted point is useful, since certain W-contiguous generating function is sparse by Lemma 3.1 (b). See details in the next section.

5. Trace reconstruction of hypermatrices

In this section, we always assume $d \geq 4$ is fixed. First, we recall Theorem 1.2 and give a proof of it. In this proof, we apply a technical method to reduce the sparse multi-variable polynomial to one-variable. We realise this by finding a suitable hyperplane tangent to a sparse set of points with at most two tangent points in the Euclidean space, based on the ideas in [43]. This is different from the proof of Theorem 2.2 for the one-variable case by using complex analysis.

Theorem 1.2. *Let $d \geq 2$ and $h(z_1, \ldots, z_d) = \sum_{k\in[n]^d} c_k z_1^{k_1}\cdots z_d^{k_d}$ be a nonzero n^μ-sparse polynomial with $\mu \in [0,1)$ and each $c_k \in \{0, \pm 1\}$. Then for any $\Delta \geq 1$ and any L with $1 \leq L \leq n^\Delta$,*

$$\max_{z_1,\ldots,z_d\in\gamma(L)} |h| \geq e^{-O(\Delta L n^{1-\mu}\log n)}.$$

Proof. The idea of this proof is to reduce the multi-variable polynomial h to a single-variable polynomial, for which we can find a big positive value at some restricted point by the similar technique as in the proof of Lemma 2.4. The way of reduction is to set $z_i = u^{b_i}$ for some integral point $b = (b_1, \ldots, b_d) \in \mathbb{Z}^d$, then h becomes a polynomial $\hbar = \sum_k c_k u^{b\cdot k}$ in u. By this way, the

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

coefficient of a monomial u^m in $\hbar$ is the sum of c_k over all k's satisfying $b \cdot k = m$, which are located on a hyperplane. However, a randomly chosen b may result in all coefficients in $\hbar$ being zero, thus $\hbar$ is a zero function, and useless. For this reason, we need the integer vector b satisfying the following property,

(P): If m_0 is the smallest integer such that $b \cdot k = m_0$ for some $k \in H := \{k \in [n]^d : c_k \neq 0\}$, then the number of such k's in H is at most two. This could be guaranteed by the sparsity of h.

Note that m_0 might be the possible minimum degree of nonzero monomials in $\hbar$. If there is only one $k \in H$ satisfying $b \cdot k = m_0$, then the coefficient of u^{m_0} is $c_k \neq 0$, thus m_0 is the minimum degree and $\hbar$ is nonzero. However, if there are two such k's, say k^1 and k^2, then the coefficient is $c_{k^1} + c_{k^2}$ which might be zero if $c_{k^1} = -c_{k^2}$. In this case, we will introduce a unit root number v and set $z_i = u^{b_i} v$ for some index i to make sure the coefficient of u^{m_0} nonzero.

Further, since we aim to lower bound h on some point with each z_i close to 1 on the unit circle, or equivalently, we aim to lower bound $\hbar$ on some point $u \in \gamma$ with u^{b_i} close to 1, then each integer b_i should be small, or the vector b should be of a short length.

Now we formally construct b, which will be chosen from the following set

$$\mathcal{N}(R) = \{(b_1, \ldots, b_d) \in \mathbb{Z}^d : \gcd(b_1, \ldots, b_d) = 1, \sqrt{b_1^2 + \cdots + b_d^2} \leq R\},$$

where $R = dn^{1-\mu}$. View H as a point set in the d-dimensional Euclidean space E^d. Take a sphere shell S of radius $\frac{\sqrt{d}}{2}n$ enclosing H, and a circumscribed hyperpolygon P of S that is formed by all $(d-1)$-dimensional hyperplanes with normal vectors in $\mathcal{N}(R)$. By a geometric argument, we obtain a claim below, whose proof is moved to Appendix C.

Claim 1. *For n sufficiently large, each facet of P has a diameter less than n^μ.*

Translate P until P touches H for the first time, that is, $P \cap H \neq \emptyset$ and H is still inside P. Let β be a facet of P touching H, and $b = (b_1, \ldots, b_d) \in \mathcal{N}(R)$ be the normal vector of β. Then H lies on one side of β. Choose $b \in \{\pm b\}$ such that b points to the H-side with respect to β. Then β belongs to the hyperplane $b \cdot x = m_0$, and $m_0 = \min\{b \cdot k : k \in H\}$.

By the claim, β has a diameter less than n^μ. Let $H_1 = \{k \in H : c_k = 1\}$ and $H_2 = \{k \in H : c_k = -1\}$ form a bipartition of H. For each $i = 1, 2$, the Euclidean distance of any two distinct points in H_i is at least n^μ by the n^μ-sparsity of h. Hence $|\beta \cap H_1| \leq 1$, $|\beta \cap H_2| \leq 1$, and thus $|\beta \cap H| \leq 2$ satisfying property (P).

Given b above, we are able to take a variable substitution that $z_1 = u^{b_1} v, z_2 = u^{b_2}, \ldots, z_d = u^{b_d}$ where $v = e^{\frac{\pi i}{2n^\Delta}}$ is a fixed number. Now we write

$$h(z_1, \ldots, z_d) = \sum_{k \in [n]^d} c_k z_1^{k_1} \cdots z_d^{k_d} = \sum_{k \in [n]^d} c_k v^{k_1} u^{b \cdot k} =: \hbar(u).$$

Then $\hbar$ has possible minimum degree m_0, so we write

$$\hbar(u) := u^{m_0}(C_v + u \cdot *) =: u^{m_0} \hbar_0(u).$$

Note that C_v is the coefficient of u^{m_0}, which equals $\sum_{k \in \beta \cap H} c_k v^{k_1}$. When $|\beta \cap H| = 1$, since $v \in \gamma$, we have $|C_v| = |\hbar_0(0)| = 1$. When $|\beta \cap H| = 2$, then $|\beta \cap H_1| = |\beta \cap H_2| = 1$. Denote $k^i = \beta \cap H_i$, $i = 1, 2$. Without loss of generality, we assume the first coordinates $k_1^1 \neq k_1^2$, and assume $k_1^1 > k_1^2$. (For other cases, say $k_i^1 \neq k_i^2$, we just move v to z_i in the variable substitution step). Since β has a diameter less than n^μ, we have $1 \leq t := k_1^1 - k_1^2 < n^\mu$. Then

$$C_v = c_{k^1} v^{k_1^1} + c_{k^2} v^{k_1^2} = \pm v^{k_1^2}(1 - v^t).$$

So

$$|\hbar_0(0)| = |C_v| = |1 - v^t| = |1 - e^{\frac{t\pi i}{2n^\Delta}}| \geq |1 - e^{\frac{\pi i}{2n^\Delta}}| \geq e^{-O(\Delta \log n)},$$

where the first inequality follows from $1 \leq t < n^\mu \leq n^\Delta$.

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

Next, for any L with $1 \le L \le n^{\Delta}$, we will lower bound $|\hbar(u)|$, and consequently lower bound $|h|$ when each z_i belongs to the arc $\gamma(L)$. Define a polynomial

$$F(u) = \prod_{1 \le a \le L'} \hbar_0(ue^{2\pi i \frac{a}{L'}})$$

for some integer L'. Then $|F(0)| = |\hbar_0(0)|^{L'} \ge e^{-O(\Delta L' \log n)}$. By the maximum modulus principle, $|F(u)| \ge |F(0)| \ge e^{-O(\Delta L' \log n)}$ for some $u \in \gamma$. We may choose a such that $ue^{2\pi i \frac{a}{L'}} \in \gamma(L')$, which is still denoted by u. Then

$$e^{-O(\Delta L' \log n)} \le |F(u)| \le |\hbar_0(u)| n^{d(L'-1)} \le |\hbar_0(u)| e^{dL' \log n},$$

where we use the fact that $|\hbar_0(u)| \le n^d$. Taking $L' = 2dLn^{1-\mu}$, we have

$$|h(z_1, \dots, z_d)| = |\hbar(u)| = |\hbar_0(u)| \ge e^{-O(\Delta L n^{1-\mu} \log n)}$$

for some $z_1 = u^{b_1} v, z_2 = u^{b_2}, \dots, z_d = u^{b_d}$ with $u \in \gamma(2dLn^{1-\mu})$, $v = e^{\frac{\pi i}{2n^{\Delta}}} \in \gamma(2n^{\Delta})$ and $|b_i| \le dn^{1-\mu}$ for $1 \le i \le d$. It is left to show that $z_1, \dots, z_d \in \gamma(L)$. Indeed,

$$z_i = u^{b_i} \in \gamma\left(\frac{2dLn^{1-\mu}}{|b_i|}\right) \subseteq \gamma(2L) \subseteq \gamma(L), \quad 2 \le i \le d.$$

For z_1, since $u^{b_1} \in \gamma(2L)$, $v \in \gamma(2n^{\Delta})$ and $L \le n^{\Delta}$, then

$$z_1 = u^{b_1} v \in \gamma(L) \cup \gamma(n^{\Delta}) = \gamma(L).$$

This completes the proof.

Note that any d-variable polynomial of the form $\sum_{k \in [n]^d} c_k z_1^{k_1} \cdots z_d^{k_d}$ is trivially 1-sparse, which is the case of $\mu = 0$ in Theorem 1.2. However, by Claim 1 saying that each facet β of the hyperpolygon P has a diameter less than 1, $|\beta \cap H| = 1$ must happen. So the parameter v becomes unnecessary, then the variable substitution and the remaining arguments can be simplified. This leads to the following corollary, which differs slightly from the case $\mu > 1$. When $L \ge Cn^{\frac{1}{d-1}}$ for a large constant C, Corollary 5.1 greatly improves the lower bound $e^{-O(L^d \log n)}$ in [30, Lemma 22].

Corollary 5.1. *Let $h(z_1, \dots, z_d) = \sum_{k \in [n]^d} c_k z_1^{k_1} \cdots z_d^{k_d}$ be a nonzero polynomial with each $c_k \in \{0, \pm 1\}$. Then*

$$\max_{z_1, \dots, z_d \in \gamma(L)} |h| \ge e^{-O(Ln \log n)}.$$

Next, we prove Theorem 1.1 (3). We first reduce the problem of establishing a lower bound for the W-generating function to that for the corresponding W-contiguous generating function, where W is a full-dimensional sub-hypermatrix. This is a multivariate version of Lemma 2.1.

Lemma 5.2. *For any distinct hypermatrices $X, Y \in \{0,1\}^{n \times r}$ and a hypermatrix $W \in \{0,1\}^{\ell \times r}$ with $\ell \le n$, let $g(z_1, \dots, z_r)$ be the W-generating function of $X - Y$ with $z_i = (z_{i0}, \dots, z_{i,\ell-1}) \in \mathbb{C}^{\ell}$, $1 \le i \le r$, and let $h(z_{10}, \dots, z_{r0})$ be the W-contiguous generating function of $X - Y$. If*

$$|h| \ge e^{-O(\ell \log n)} \text{ for some } z_{i0} \in \gamma, 1 \le i \le r,$$

then fixing $\{z_{i0}\}$, there exist $z_{ij} \in [1 - 2p, 1]$ for $1 \le i \le r$, $1 \le j \le \ell - 1$ such that

$$|g| \ge e^{-O(\ell \log n)}.$$

Proof. For $k = (k_1, \dots, k_r) \in [n]^{r-1} \times \mathcal{I}(n, \ell)$ with $k_r = (k_{r0}, \dots, k_{r,\ell-1}) \in \mathcal{I}(n, \ell)$, let $\bar{k}$ denote the position of an $\ell^{\times r}$-sub-hypermatrix that is contiguous along the first $r - 1$ dimensions starting

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

at $(k_1, \ldots, k_{r-1})$ and is k_r on the last dimension. Consider the partial sum in g over such positions, denoted by

$$\bar{g}(z_1, \ldots, z_r) = \sum_k [1_{X_{\bar{k}}=W} - 1_{Y_{\bar{k}}=W}] z_{10}^{k_1} \cdots z_{r-1,0}^{k_{r-1}} \cdot z_r^{\odot k_r},$$

where k runs over $[n]^{r-1} \times \mathcal{I}(n, \ell)$ and $z_i = (z_{i0}, \ldots, z_{i,\ell-1}) \in \mathbb{C}^\ell$, $1 \le i \le r$. Fix $z_{i0} \in \gamma$, $1 \le i \le r$ such that $|h| \ge e^{-O(\ell \log n)}$. We claim that there exist $z_{rj} \in [1-2p, 1]$ for $1 \le j \le \ell - 1$ such that $|\bar{g}| \ge e^{-O(\ell \log n)}$, that is, the norm of the partial sum in the W-generating function over sub-hypermatrices whose position is contiguous along the first $r-1$ dimensions can also be lower bounded by $e^{-O(\ell \log n)}$. Then using the similar argument, we could remove the contiguous conditions of the rest $r-1$ dimensions one by one. Since r is a constant, we finally obtain $|g| \ge e^{-O(\ell \log n)}$, for some $z_{ij} \in [1-2p, 1]$, $1 \le i \le r$, $1 \le j \le \ell - 1$.

Now we prove the claim. Consider the case when $z_{r1} = z_{r2} = \ldots = z_{r,\ell-1}$. Then $\bar{g}$ becomes a single-variable polynomial

$$\bar{g}(z_{r1}) = \sum_k [1_{X_{\bar{k}}=W} - 1_{Y_{\bar{k}}=W}] z_{10}^{k_1} \cdots z_{r-1,0}^{k_{r-1}} \cdot z_{r0}^{k_{r0}} z_{r1}^{k_{r,\ell-1} - k_{r0} - (\ell-1)}.$$

Note that when $z_{r1} = 0$, we have $z_{r1}^{k_{r,\ell-1} - k_{r0} - (\ell-1)} = 1$ only when $k_{r,\ell-1} - k_{r0} - (\ell - 1) = 0$, that is, $k_r = k_{r0} + [\ell]$. So, $\bar{g}(0)$ keeps the terms corresponding to contiguous sub-hypermatrices. Thus $\bar{g}(0) = h(z_{10}, \ldots, z_{r0})$. Denote $\bar{h}(z_{r1}) = \binom{n}{\ell}^{-r} \bar{g}(z_{r1})$. Since each coefficient of $\bar{h}(z_{r1})$ has norm at most 1, then by [7, Theorem 5.1], there are absolute constants $c_1, c_2 > 0$, such that

$$\begin{aligned} \max_{z_{r1} \in [1-2p,1]} |\bar{h}(z_{r1})| &\ge |\bar{h}(0)|^{c_1/(2p)} e^{-c_2/(2p)} \ge \left(\binom{n}{\ell}^{-r} e^{-O(\ell \log n)} \right)^{c_1/(2p)} e^{-c_2/(2p)} \\ &\ge e^{-O(\ell \log n)}. \end{aligned}$$

Taking an z_{r1} realising this maximum, we have

$$|\bar{g}(z_{r1})| = \binom{n}{\ell}^r |\bar{h}(z_{r1})| \ge e^{-O(\ell \log n)}.$$

Thus the claim is proved. □

In Lemma 5.3 below, we prove the existence of a hypermatrix W such that the W-generating function has a big norm at some restricted point. Theorem 1.1 (3) follows immediately by combining Lemmas 5.3 and 2.3 with $m = n^{3/5} \log n$.

Lemma 5.3. *For any distinct hypermatrices $X, Y \in \{0,1\}^{n \times d}$, there exists some $W \in \{0,1\}^{\ell \times r}$ with $\ell = 4n^{3/5} + 1$ and $0 \le r \le d$, such that the W-generating function g of $X - Y$ satisfies*

$$|g(z)| \ge \exp(-Cn^{3/5} \log n) \text{ for some } w \in \mathbb{C}(d, \ell^{\times r}) \text{ with } \theta(w) \le \exp\left(\frac{C}{n^{2/5}}\right),$$

where $C > 0$ is a constant.

Proof. Let $A^d = X - Y$. Suppose that X and Y are $(\lambda_1, \lambda_2, \ldots, \lambda_d)$-identical with respect to a dimension reduction $\mathcal{R} : A^d \to A^{d-1} \to \cdots \to A^1 \to \pm 1$.

Case 1. $\lambda_2 < \ell$. Set $r = 0$ and $W = 1$. Let f_i be the generating function of A^i for $1 \le i \le d$. Then

$$f_{i+1}(z_1, \ldots, z_{i+1}) = z_{i+1}^{\lambda_{i+1}} (f_i(z_1, \ldots, z_i) + z_{i+1} \cdot *), \ 1 \le i \le d-1.$$

Since $f_1(z_1)$ is a Littlewood polynomial, we can apply [6, Corollary 3.2] to get

$$|f_1(z_1)| \ge e^{-O(\ell)} \text{ for some } z_1 \in \gamma(\ell).$$

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

Then the corresponding w_1 satisfies $|w_1| \le e^{O(\ell^{-2})}$ by equation (1). Fix w_1 and z_1. Since $\lambda_2 < \ell$, we can apply Lemma 2.4 to $f_2(z_1, z_2)$ with $m = \ell$ and $a = 1$ to get

$$|f_2(z_1, z_2)| \ge e^{-O(\ell)} \text{ for some } w_2 \in \mathbb{C} \text{ with } |w_2| \le 1.$$

Repeatedly applying Lemma 2.4 $(d-1)$ times, we finally obtain

$$|f_d| \ge e^{-O(\ell)} \text{ for some } \{w_i\} \text{ with } |w_i| \le 1, 2 \le i \le d \text{ and } |w_1| \le e^{O(\ell^{-2})}.$$

Case 2. $\lambda_{r+1} < \ell \le \lambda_r$ for some $r \ge 2$.

Take the hypermatrix $W \in \{0,1\}^{\ell \times r}$ in Lemma 3.1 and let $g(z)$ be the W-generating function of $X - Y$, where $z = (z_1, \dots, z_d) \in \mathbb{C}(d, \ell^{\times r})$. We will show that for some $w = (w_1, \dots, w_d) \in \mathbb{C}(d, \ell^{\times r})$,

$$|g(z)| \ge e^{-O(n^{3/5} \log n)} \text{ with } \prod_{i=1}^{r} \theta(w_i) \le e^{O(n^{-2/5})} \text{ and } |w_i| \le 1, r+1 \le i \le d.$$

Let g_i be the W-generating function of the i-dimensional sub-hypermatrix A^i for $r \le i \le d-1$. Then we have the same recursions as in equation (2). Let $h(z_{10}, \dots, z_{r0})$ be the W-contiguous generating function of A^r. By Lemma 3.1 (b), h is nonzero and $n^{3/5}$-sparse. We apply Theorem 1.2 for $\mu = 3/5, L = n^{1/5}, \Delta = 1$ to get

$$|h(z_{10}, \dots, z_{r0})| \ge e^{-O(n^{3/5} \log n)} \text{ for some } z_{10}, \dots, z_{r0} \in \gamma(n^{1/5}).$$

Then by Lemma 5.2, for some $z_{10}, \dots, z_{r0} \in \gamma(n^{1/5})$ and $z_{ij} \in [1-2p, 1]$, $1 \le i \le r$, $1 \le j \le l-1$,

$$|g_r(z_1, \dots, z_r)| \ge e^{-O(n^{3/5} \log n)}.$$

By equation (1), we have $\prod_{i=1}^{r} \theta(w_i) \le e^{O(n^{-2/5})}$ correspondingly. Fixing $w_1, \dots, w_r$ and $z_1, \dots, z_r$, and let $g'(z_{r+1}) = g_{r+1}(z_1, \dots, z_r, z_{r+1})$. We apply Lemma 2.4 to $g'(z_{r+1})$. Since $m_0 = \lambda_{r+1} < \ell \le n^{3/5} \log n$, $|c_0| = |g_r| \ge e^{-O(n^{3/5} \log n)}$, and $\sum_i |c_i| \le n\binom{n}{\ell}^r \le e^{O(\ell \log n)} \le e^{O(n^{3/5} \log n)}$, by Lemma 2.4 with $m = n^{3/5} \log n$ and $a = 1$, we have

$$|g_{r+1}(z_1, \dots, z_r, z_{r+1})| = |g'(z_{r+1})| \ge e^{-O(n^{3/5} \log n)} \text{ for some } w_{r+1} \in \mathbb{C} \text{ with } |w_{r+1}| \le 1.$$

Applying Lemma 2.4 $(d-r)$ times, we finally obtain

$$|g| \ge e^{-O(n^{3/5} \log n)} \text{ with } \prod_{i=1}^{r} \theta(w_i) \le e^{O(n^{-2/5})} \text{ and } |w_i| \le 1, r+1 \le i \le d.$$

Combining Cases 1 and 2, we complete the proof. □

Remark 5.4. Chase (see the footnote of [9, p. 5]) observed that padding the beginning of each string with sufficiently many 0s eliminates the need to invoke the result of Peres and Zhai [40], which was used to handle the easy case where two strings don't resemble each other from the beginning. This modification yields the same upper bound of $T(n)$, but with a bigger constant hidden in the $O(\cdot)$ notation. Similarly, by padding the boundary of the hypermatrices with sufficiently many 0s, one may restrict the $(\lambda_1, \dots, \lambda_d)$-pattern to the case $\lambda_i \ge \ell$ for all $1 \le i \le d$, thereby avoiding the use of Lemma 2.4 and simplifying our proofs. We nevertheless retain the dimension reduction process in Section 3 to classify pairs of hypermatrices as it provides a nice structure of all related generating functions and may be useful for other multidimensional variants.

Data availability statement

No data was used for the research described in the article.

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

Acknowledgements

The research of X. Zhang is supported by the National Key Research and Development Programs of China 2023YFA1010201 and 2020YFA0713100, the NSFC under Grants No. 12171452 and No. 12231014, and the Quantum Science and Technology-National Science and Technology Major Project 2021ZD0302902.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Ban, F., Chen, X., Freilich, A., Servedio, R. and Sinha, S. (2019) Beyond trace reconstruction: population recovery from the deletion channel. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 745–768.
[2] Ban, F., Chen, X., Servedio, R. and Sinha, S. (2019) Efficient average-case population recovery in the presence of insertions and deletions. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2019)*.
[3] Batu, T., Kannan, S., Khanna, S. and McGregor, A. (2004) Reconstructing strings from random traces. In *Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pp. 910–918.
[4] Bollobás, B. (1990) Almost every graph has reconstruction number three. *J. Graph Theory* **14**(1) 1–4.
[5] Bondy, J. A. and Hemminger, R. L. (1977) Graph reconstruction – a survey. *J. Graph Theory* **1**(3) 227–268.
[6] Borwein, P. and Erdélyi, T. (1997) Littlewood-type problems on subarcs of the unit circle. *Indiana Univer. Math. J.*, 1323–1346.
[7] Borwein, P., Erdélyi, T. and Kós, G. (1999) Littlewood-type problems on [0, 1]. *Proc. Lond. Math. Soc.* **79**(1) 22–26.
[8] Brakensiek, J., Li, R. and Spang, B. (2020) Coded trace reconstruction in a constant number of traces. In*2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 482–493.
[9] Chase, Z. (2020) New upper bounds for trace reconstruction. arXiv preprint arXiv: 2009.03296.
[10] Chase, Z. and Peres, Y. (2021) Approximate trace reconstruction of random strings from a constant number of traces. arXiv preprint arXiv:2107.06454.
[11] Chase, Z. (2021) New lower bounds for trace reconstruction. *Ann. l'Inst. Henri Poincaré-Probab. Stat.* **57**(2) 627–643.
[12] Chase, Z. (2021) Separating words and trace reconstruction. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pp. 21–31.
[13] Cheraghchi, M., Gabrys, R., Milenkovic, O. and Ribeiro, J. (2020) Coded trace reconstruction. *IEEE Trans. Inform. Theory* **66**(10) 6084–6103.
[14] Davies, S., Rácz, M. Z., Schiffer, B. G. and Rashtchian, C. (2021) Approximate trace reconstruction: algorithms. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pp. 2525–2530.
[15] Davies, S., Racz, M. and Rashtchian, C. (2021) Reconstructing trees from traces. *Ann. Appl. Probab.* **31**(6) 2772–2810.
[16] De, A., O'Donnell, R. and Servedio, R. A. (2017) Optimal mean-based algorithms for trace reconstruction. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pp. 1047–1056.
[17] Dudık, M. and Schulman, L. J. (2003) Reconstruction from subsequences. *J. Combin. Theory, Ser. A* **103**(2) 337–348.
[18] Foster, W. and Krasikov, I. (2000) An improvement of a Borwein–Erdélyi–Kós result. *Methods Appl. Anal.* **7**(4) 605–614.
[19] Gabrys, R. and Yaakobi, E. (2018) Sequence reconstruction over the deletion channel. *IEEE Trans. Inform. Theory* **64**(4) 2924–2931.
[20] Groenland, C., Guggiari, H. and Scott, A. (2021) Size reconstructibility of graphs. *J. Graph Theory* **96**(2) 326–337.
[21] Hoeffding, W. (1963) Probability Inequalities for Sums of Bounded Random Variables. *J. Am. Stat. Assoc.* **58**(301) 13–30.
[22] Holden, N. and Lyons, R. (2020) Lower bounds for trace reconstruction. *Ann. Appl. Probab.* **30**(2) 503–525.
[23] Holden, N., Pemantle, R., Peres, Y. and Zhai, A. (2020) Subpolynomial trace reconstruction for random strings and arbitrary deletion probability. *Math. Stat. Learn.* **2**(3) 275–309.
[24] Holenstein, T., Mitzenmacher, M., Panigrahy, R. and Wieder, U. (2008) Trace reconstruction with constant deletion probability and related results. In *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pp. 389–398.
[25] Kalashnik, L. (1973) The reconstruction of a word from fragments. *Numer. Math. Comput. Technol.* **4** 56–57.
[26] Konstantinova, E., Levenshtein, V. and Siemons, J. (2007) Reconstruction of permutations distorted by single transposition errors. *arXiv preprint arXiv:math/0702191*.
[27] Kós, G., Ligeti, P. and Sziklai, P. (2009) Reconstruction of matrices from submatrices. *Math. Comput.* **78**(267) 1733–1747.
[28] Kostochka, A. V. and West, D. B. (2020) On reconstruction of graphs from the multiset of subgraphs obtained by deleting *l* vertices. *IEEE Trans. Inform. Theory* **67**(6) 3278–3286.

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

[29] Krasikov, I. and Roditty, Y. (1997) On a reconstruction problem for sequences. *J. Combin. Theory, Ser. A* **77**(2) 344–348.
[30] Krishnamurthy, A., Mazumdar, A., McGregor, A. and Pal, S. (2021) Trace reconstruction: generalized and parameterized. *IEEE Trans. Inform. Theory* **67**(6) 3233–3250.
[31] Lauri, J. and Scapellato, R. (2016) *Topics in Graph Automorphisms and Reconstruction*, Vol. **432**. Cambridge University Press.
[32] Levenshtein, V. (1997) Reconstruction of objects from the minimum number of distorted patterns. *Dokl. Akad. Nauk* **354**(5) 593–596.
[33] Levenshtein, V. (2001) Efficient reconstruction of sequences. *IEEE Trans. Inform. Theory* **47**(1) 2–22.
[34] Levenshtein, V. (2001) Efficient reconstruction of sequences from their subsequences or supersequences. *J. Combin. Theory, Ser. A* **93**(2) 310–332.
[35] McGregor, A., Price, E. and Vorotnikova, S. (2014) Trace reconstruction revisited. In *European Symposium on Algorithms*. Springer, pp. 689–700.
[36] Narayanan, S. (2020) Population recovery from the deletion channel: nearly matching trace reconstruction bounds. arXiv preprint arXiv: 2004.06828.
[37] Narayanan, S. and Ren, M. (2021) Circular trace reconstruction. In *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*.
[38] Nazarov, F. and Peres, Y. (2017) Trace reconstruction with exp $(O(n^{1/3}))$ samples. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pp. 1042–1046.
[39] O'Neil, P. V. (1970) Ulam's conjecture and graph reconstructions. *Amer. Math. Mon.* **77**(1) 35–43.
[40] Peres, Y. and Zhai, A. (2017) Average-case reconstruction for the deletion channel: subpolynomially many traces suffice. In *2017 IEEE. 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 228–239.
[41] Robson, J. M. (1989) Separating strings with small automata. *Inform. Process. Lett.* **30**(4) 209–214.
[42] Ye, Z., Liu, X., Zhang, X. and Ge, G. (2023) Reconstruction of sequences distorted by two insertions. *IEEE Trans. Inform. Theory* **69**(8) 4977–4992.
[43] Zhong, W. and Zhang, X. (2025) Reconstruction of hypermatrices from subhypermatrices. *J. Combin. Theory Ser. A* **209** 105966.

A. Proof of equation (6)

Proof. For $r+1 \le i \le d$, from $z_i = pw_i + q$, we have $pz_i^{k_i} = p(pw_i+q)^{k_i} = \sum_{j_i} \binom{k_i}{j_i} p^{j_i+1} q^{k_i-j_i} \cdot w_i^{j_i}$. For $1 \le i \le r$, we have

$$
\begin{aligned}
&p^{\ell} z_i^{\odot k_i} = p^{\ell} z_{i0}^{k_{i0}} z_{i1}^{k_{i1}-k_{i0}-1} \cdots z_{i,\ell-1}^{k_{i,\ell-1}-k_{i,\ell-2}-1} \\
&= p^{\ell} (pw_{i0}+q)^{k_{i0}} (pw_{i1}+q)^{k_{i1}-k_{i0}-1} \cdots (pw_{i,\ell-1}+q)^{k_{i,\ell-1}-k_{i,\ell-2}-1} \\
&= p^{\ell} \sum_{j_{i0}} \binom{k_{i0}}{j_{i0}} p^{j_{i0}} q^{k_{i0}-j_{i0}} w_{i0}^{j_{i0}} \cdot \Bigg\{ \sum_{j_{i1}>j_{i0}} \binom{k_{i1}-k_{i0}-1}{j_{i1}-j_{i0}-1} p^{j_{i1}-j_{i0}-1} q^{(k_{i1}-k_{i0})-(j_{i1}-j_{i0})} w_{i1}^{j_{i1}-j_{i0}-1} \\
&\cdot \Bigg[\cdots \Bigg(\sum_{j_{i,\ell-1}>j_{i,\ell-2}} \binom{k_{i,\ell-1}-k_{i,\ell-2}-1}{j_{i,\ell-1}-j_{i,\ell-2}-1} p^{j_{i,\ell-1}-j_{i,\ell-2}-1} q^{(k_{i,\ell-1}-k_{i,\ell-2})-(j_{i,\ell-1}-j_{i,\ell-2})} w_{i,\ell-1}^{j_{i,\ell-1}-j_{i,\ell-2}-1} \Bigg) \Bigg] \Bigg\} \\
&= \sum_{j_i} \binom{k_{i0}}{j_{i0}} \prod_{h=1}^{\ell-1} \binom{k_{ih}-k_{i,h-1}-1}{j_{ih}-j_{i,h-1}-1} p^{j_{i,\ell-1}+1} q^{k_{i,\ell-1}-j_{i,\ell-1}} \cdot w_i^{\odot j_i}.
\end{aligned}
$$

Therefore, the left hand side of the W-generating identity is

$$
\begin{aligned}
&\sum_j \cdot \sum_k 1_{\widetilde{X}_k = W} \Bigg[\binom{k_{1,0}}{j_{1,0}} \prod_{h=1}^{\ell-1} \binom{k_{1,h}-k_{1,h-1}-1}{j_{1,h}-j_{1,h-1}-1} p^{j_{1,\ell-1}+1} q^{k_{1,\ell-1}-j_{1,\ell-1}} \cdot w_1^{\odot j_1} \Bigg] \\
&\cdots \Bigg[\binom{k_{r,0}}{j_{r,0}} \prod_{h=1}^{\ell-1} \binom{k_{r,h}-k_{r,h-1}-1}{j_{r,h}-j_{r,h-1}-1} p^{j_{r,\ell-1}+1} q^{k_{r,\ell-1}-j_{r,\ell-1}} \cdot w_r^{\odot j_r} \Bigg] \\
&\cdot \Bigg[\binom{k_{r+1}}{j_{r+1}} p^{j_{r+1}+1} q^{k_{r+1}-j_{r+1}} \cdot w_{r+1}^{j_{r+1}} \Bigg] \cdots \Bigg[\binom{k_d}{j_d} p^{j_d+1} q^{k_d-j_d} \cdot w_d^{j_d} \Bigg]
\end{aligned}
$$

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

$$
\begin{aligned}
&= \sum_k 1_{\widetilde{X}_k = W} \sum_j \cdots = \sum_k 1_{\widetilde{X}_k = W} \sum_{j_0} \sum_{j_1} \cdots \sum_{j_d} \cdots \\
&= \sum_k 1_{\widetilde{X}_k = W} \left(p^\ell z_1^{\odot k_1}\right) \cdots \left(p^\ell z_r^{\odot k_r}\right) \cdot \left(p z_{r+1}^{k_{r+1}}\right) \cdots \left(p z_d^{k_d}\right) \\
&= p^{r\ell + d - r} g(z_1, \ldots, z_d).
\end{aligned}
$$

□

B. Proof of Lemma 4.2

Proof. Suppose that X and Y are $(\lambda_1, \lambda_2, \lambda_3)$-identical with respect to a dimension reduction $\mathcal{R} : A = X - Y \to A^2 \to A^1 \to \pm 1$.

Case 1. $\lambda_1 < \ell$.

Set $r = 0$ and $W = 1$. Let $f(z_1, z_2, z_3)$ be the generating function of A. Similar to Case 1 of matrices, we apply Lemma 2.4 three times to get

$$|f| \geq e^{-O(\ell^{19/27})} \text{ for some } w_1, w_2, w_3 \in \mathbb{C} \text{ with } |w_1|, |w_2|, |w_3| \leq 1.$$

Case 2. $\lambda_1 \geq \ell$.

Set $r = 1$ and take the sequence $W \in \{0, 1\}^\ell$ in Lemma 3.1. Let $g(z_1, z_2, z_3), g_2(z_1, z_2), g_1(z_1)$ be the W-generating function of A, A^2, A^1, respectively, where $(z_1, z_2, z_3) \in \mathbb{C}(3, \ell^{\times 1})$. By equation (10), we write

$$g(z_1, z_2, z_3) = z_3^{\lambda_3} \left(g_2(z_1, z_2) + z_3 g_2'(z_1, z_2)\right), \text{ and } g_2(z_1, z_2) = z_2^{\lambda_2}(g_1(z_1) + z_2 g_1'(z_1)),$$

where g_2' and g_1' are polynomials. Similar to Case 2 of matrices, we have

$$|g_1| \geq e^{-O(n^{1/9} \log^5 n)} \text{ for some } w_1 \in \mathbb{C}^l \text{ with } \theta(w_1) \leq e^{O(n^{-4/9})}.$$

Fix w_1 and z_1, and define the polynomial for some integer L,

$$F(z_2, z_3) = \prod_{1 \leq a, b \leq L} g(z_1, z_2 e^{2\pi i \frac{a}{L}}, z_3 e^{2\pi i \frac{b}{L}}).$$

Further, define

$$
\begin{aligned}
G(z_2, z_3) &= \prod_{1 \leq a, b \leq L} \left(g_2\left(z_1, z_2 e^{2\pi i \frac{a}{L}}\right) + z_3 e^{2\pi i \frac{b}{L}} g_2'\left(z_1, z_2 e^{2\pi i \frac{a}{L}}\right)\right), \\
H(z_2) &= \prod_{1 \leq a \leq L} \left(g_1(z_1) + z_2 e^{2\pi i \frac{a}{L}} g_1'(z_1)\right).
\end{aligned}
$$

Then for any $z_2, z_3 \in \gamma$, $|G(z_2, z_3)| = |F(z_2, z_3)|$, $|G(z_2, 0)| = |H(z_2)|^L$ and $|H(0)| = |g_1(z_1)|^L$. By the maximum modulus principle, there exist some $z_2, z_3 \in \gamma$ such that

$$|F(z_2, z_3)| = |G(z_2, z_3)| \geq |G(z_2, 0)| = |H(z_2)|^L \geq |H(0)|^L = |g_1(z_1)|^{L^2} \geq \exp\left(-O\left(n^{1/9} L^2 \log^5 n\right)\right).$$

We may choose a, b such that $z_2 e^{2\pi i \frac{a}{L}}, z_3 e^{2\pi i \frac{b}{L}} \in \gamma(L)$, which are still denoted by z_2, z_3, respectively. Then

$$
\begin{aligned}
\exp\left(-O\left(n^{1/9} L^2 \log^5 n\right)\right) &\leq |F(z_2, z_3)| \leq |g(z_1, z_2, z_3)| \left(n^2 \binom{n}{\ell}\right)^{L^2 - 1} \\
&\leq |g(z_1, z_2, z_3)| \exp\left(7 n^{1/9} L^2 \log n\right),
\end{aligned}
$$

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press

where we use the fact that $|g(z_1, z_2, z_3)| \le n^2\binom{n}{\ell}$. By equation (1), $|w_2|, |w_3| \le \exp(O(L^{-2}))$. Taking $L = n^{2/9}/\log^{5/4} n$,

$$\begin{aligned} |g| &\ge \exp\left(-O(n^{\frac{5}{9}}\log^{\frac{5}{2}} n)\right) \text{ for some } w = (w_1, w_2, w_3) \in \mathbb{C}(3, \ell^{\times r}) \text{ with } \theta(w) \\ &\le \exp\left(O\left(\frac{\log^{\frac{5}{2}} n}{n^{\frac{4}{9}}}\right)\right). \end{aligned}$$

Combining Cases 1 and 2, we complete the proof. □

C. Proof of Claim 1

Proof. Let n be sufficiently large, then $R = dn^{1-\mu}$ is large. Assume that the centre of S is the origin $\mathbf{o}$. Take $\mathbf{x}_0 \in P$ maximising the Euclidean distance from $\mathbf{o}$. Let $\overline{\mathbf{ox}_0}$ be the segment ending at $\mathbf{o}$ and $\mathbf{x}_0$, then take a point $\mathbf{x} \in \overline{\mathbf{ox}_0}$ such that $\|\mathbf{x}\| = R - \sqrt{d}$. Without loss of generality, let $\mathbf{x} = (x_1, \ldots, x_d)$ with $x_1 \ge x_2 \ge \cdots \ge x_d \ge 0$. Clearly $x_1 \ge \frac{R}{\sqrt{d}} - 1$. Take another point $\mathbf{y} \in \overline{\mathbf{ox}_0}$ such that $\mathbf{y} = (p, y_2, \ldots, y_d)$ with $p \ge y_2 \ge \cdots \ge y_d \ge 0$, where p is the largest prime satisfying $p \le x_1$. Clearly $p = (1 - o(1))x_1$ and $\|\mathbf{y}\| = (1 - o(1))(R - \sqrt{d})$. Take $\mathbf{a} = (p, a_2, \ldots, a_d) \in \mathbb{Z}^d$ with $a_i \in [p-1]$ and $|a_i - y_i| \le 1$ for $2 \le i \le d-1$. Clearly, $\gcd(p, a_2, \ldots, a_d) = 1$, $\|\mathbf{a} - \mathbf{y}\| \le \sqrt{d-1}$ and thus $\|\mathbf{a}\| = (1 - o(1))R$. Therefore, $\mathbf{a} \in \mathcal{N}(R)$.

Let θ be the angle formed by $\overline{\mathbf{oa}}$ and $\overline{\mathbf{oy}}$. Since $\|\mathbf{a} - \mathbf{y}\| = o(\|\mathbf{a}\|)$, we have

$$\tan\theta \le (1 + o(1))\frac{\|\mathbf{a} - \mathbf{y}\|}{\|\mathbf{a}\|} \le (1 + o(1))\frac{\sqrt{d-1}}{R}.$$

Extend the segment $\overline{\mathbf{oa}}$ to intersect S at point $\mathbf{a}_0$, then $\|\mathbf{a}_0\| = \frac{\sqrt{d}}{2}n$. Since $\mathbf{a} \in \mathcal{N}(R)$, $\mathbf{a}_0$ is a tangent point of S and some facet α of P. Extend $\overline{\mathbf{ox}_0}$ to intersect α at a point $\mathbf{y}_0$, then $\overline{\mathbf{a}_0\mathbf{y}_0}$ and $\overline{\mathbf{a}_0\mathbf{o}}$ span a right angle. On the other hand, by the extreme property of $\mathbf{x}_0$, the point $\mathbf{y}_0$ is either the point $\mathbf{x}_0$ itself or outside P. Therefore, each facet of P has a diameter at most

$$2\|\mathbf{y}_0 - \mathbf{a}_0\| = 2\|\mathbf{a}_0\|\tan\theta \le (1 + o(1))\frac{\sqrt{d(d-1)}n}{R} < \frac{dn}{R} = n^{\mu}.$$

□

Cite this article: Zhong W and Zhang X (2026). Trace reconstruction of matrices and hypermatrices. *Combinatorics, Probability and Computing* **35**, 356–374. https://doi.org/10.1017/S0963548326100364

https://doi.org/10.1017/S0963548326100364 Published online by Cambridge University Press