The Power of Convex Relaxation: Near-Optimal Matrix Completion

Emmanuel J. Candès, *Associate Member, IEEE*, and Terence Tao

***Abstract*—This paper is concerned with the problem of recovering an unknown matrix from a small fraction of its entries. This is known as the *matrix completion* problem, and comes up in a great number of applications, including the famous *Netflix Prize* and other similar questions in collaborative filtering. In general, accurate recovery of a matrix from a small number of entries is impossible, but the knowledge that the unknown matrix has low rank radically changes this premise, making the search for solutions meaningful. This paper presents optimality results quantifying the minimum number of entries needed to recover a matrix of rank r exactly by any method whatsoever (the information theoretic limit). More importantly, the paper shows that, under certain incoherence assumptions on the singular vectors of the matrix, recovery is possible by solving a convenient convex program as soon as the number of entries is on the order of the information theoretic limit (up to logarithmic factors). This convex program simply finds, among all matrices consistent with the observed entries, that with minimum nuclear norm. As an example, we show that on the order of $nr\log(n)$ samples are needed to recover a random $n \times n$ matrix of rank r by any method, and to be sure, nuclear norm minimization succeeds as soon as the number of entries is of the form $nr\,\mathrm{polylog}(n)$.**

***Index Terms*—Duality in optimization, free probability, low-rank matrices, matrix completion, nuclear norm minimization, random matrices and techniques from random matrix theory, semidefinite programming.**

I. Introduction

A. Motivation

Imagine we have an $n_1 \times n_2$ array of real[1] numbers and that we are interested in knowing the value of each of the $n_1 n_2$ entries in this array. Suppose, however, that we only get to see a small number of the entries so that most of the elements about which we wish information are simply missing. Is it possible from the available entries to guess the many entries that we have not seen? This problem is now known as the *matrix completion* problem [7], and comes up in a great number of applications, including the famous *Netflix Prize* and other similar questions in collaborative filtering [12]. In a nutshell, collaborative filtering is the task of making automatic predictions about the interests of a user by collecting taste information from many users. Netflix is a commercial company implementing collaborative filtering, and seeks to predict users' movie preferences from just a few ratings per user. There are many other such recommendation systems proposed by Amazon, Barnes and Noble, and Apple Inc. to name just a few. In each instance, we have a partial list about a user's preferences for a few rated items, and would like to predict his/her preferences for all items from this and other information gleaned from many other users.

In mathematical terms, the problem may be posed as follows: we have a data matrix $M \in \mathbb{R}^{n_1 \times n_2}$ which we would like to know as precisely as possible. Unfortunately, the only information available about M is a sampled set of entries M_{ij}, $(i,j) \in \Omega$, where Ω is a subset of the complete set of entries $[n_1] \times [n_2]$ (here, and in the sequel, $[n]$ denotes the list $\{1,\ldots,n\}$). Clearly, this problem is ill-posed for there is no way to guess the missing entries without making any assumption about the matrix M.

An increasingly common assumption in the field is to suppose that the unknown matrix M has low rank or has approximately low rank. In a recommendation system, this makes sense because often times, only a few factors contribute to an individual's taste. In [7], the authors showed that this premise radically changes the problem, making the search for solutions meaningful. Before reviewing these results, we would like to emphasize that the problem of recovering a low-rank matrix from a sample of its entries, and by extension from fewer linear functionals about the matrix, comes up in many application areas other than collaborative filtering. For instance, the completion problem also arises in computer vision. There, many pixels may be missing in digital images because of occlusion or tracking failures in a video sequence. Recovering a scene and inferring camera motion from a sequence of images is a matrix completion problem known as the structure-from-motion problem [9], [24]. Other examples include system identification in control [20], multiclass learning in data analysis [1]–[3], global positioning—e.g., of sensors in a network—from partial distance information [5], [22], [23], remote sensing applications in signal processing where we would like to infer a full covariance matrix from partially observed correlations [26], and many statistical problems involving succinct factor models.

Manuscript received March 11, 2009; revised August 12, 2009. Current version published April 21, 2010. E. J. Candès was supported in part by ONR grants N00014-09-1-0469 and N00014-08-1-0749 and in part by the NSF Waterman Award. T. Tao was supported in part by a grant from the MacArthur Foundation, in part by NSF grant DMS-0649473, and in that part by the NSF Waterman Award.

E. J. Candès is with the Department of Applied and Computational Mathematics, California Institute of Technology, Pasadena, CA 91125 USA (e-mail: emmanuel@acm.caltech.edu).

T. Tao is with the Department of Mathematics, University of California, Los Angeles, CA 90095 USA (e-mail: tao@math.ucla.edu).

Communicated by J. Romberg, Associate Editor for Signal Processing.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2010.2044061

[1]Much of the discussion below, as well as our main results, applies also to the case of complex matrix completion, with some minor adjustments in the absolute constants; but for simplicity we restrict attention to the real case.

B. Minimal Sampling

This paper is concerned with the theoretical underpinnings of matrix completion and more specifically in quantifying the minimum number of entries needed to recover a matrix of rank r exactly. This number generally depends on the matrix we wish to recover. For simplicity, assume that the unknown rank-r matrix M is $n \times n$. Then it is not hard to see that matrix completion is impossible unless the number of samples m is at least $2nr - r^2$, as a matrix of rank r depends on this many degrees of freedom. The singular value decomposition (SVD)

$$M = \sum_{k \in [r]} \sigma_k u_k v_k^* \tag{I.1}$$

where $\sigma_1, \ldots, \sigma_r \geq 0$ are the singular values, and the singular vectors $u_1, \ldots, u_r \in \mathbb{R}^{n_1} = \mathbb{R}^n$ and $v_1, \ldots, v_r \in \mathbb{R}^{n_2} = \mathbb{R}^n$ are two sets of orthonormal vectors, is useful to reveal these degrees of freedom. Informally, the singular values $\sigma_1 \geq \cdots \geq \sigma_r$ depend on r degrees of freedom, the left singular vectors u_k on $(n-1)+(n-2)+\cdots+(n-r) = nr - r(r+1)/2$ degrees of freedom, and similarly for the right singular vectors v_k. If $m < 2nr - r^2$, no matter which entries are available, there can be an infinite number of matrices of rank at most r with exactly the same entries, and so exact matrix completion is impossible. In fact, if the observed locations are sampled at random, we will see later that the minimum number of samples is better thought of as being on the order of $nr \log n$ rather than nr because of a coupon collector's effect.

In this paper, we are interested in identifying large classes of matrices which can provably be recovered by a tractable algorithm from a number of samples approaching the above limit, i.e., from about $nr \log n$ samples. Before continuing, it is convenient to introduce some notation that will be used throughout: let $\mathcal{P}_\Omega : \mathbb{R}^{n \times n} \to \mathbb{R}^{n \times n}$ be the orthogonal projection onto the subspace of matrices which vanish outside of Ω ($(i,j) \in \Omega$ if and only if M_{ij} is observed); that is, $Y = \mathcal{P}_\Omega(X)$ is defined as

$$Y_{ij} = \begin{cases} X_{ij}, & (i,j) \in \Omega \\ 0, & \text{otherwise} \end{cases}$$

so that the information about M is given by $\mathcal{P}_\Omega(M)$. The matrix M can, in principle, be recovered from $\mathcal{P}_\Omega(M)$ if it is the unique matrix of rank less than or equal to r that is consistent with the data. In other words, if M is the unique solution to

$$\begin{aligned} &\text{minimize} && \operatorname{rank}(X) \\ &\text{subject to} && \mathcal{P}_\Omega(X) = \mathcal{P}_\Omega(M). \end{aligned} \tag{I.2}$$

Knowing when this happens is a delicate question which shall be addressed later. For the moment, note that attempting recovery via (I.2) is not practical as rank minimization is in general an NP-hard problem for which there are no known algorithms capable of solving problems in practical time once, say, $n \geq 10$.

In [7], it was proved 1) that matrix completion is not as ill-posed as previously thought and 2) that exact matrix completion is possible by convex programming. The authors of [7] proposed recovering the unknown matrix by solving the nuclear norm minimization problem

$$\begin{aligned} &\text{minimize} && \|X\|_* \\ &\text{subject to} && \mathcal{P}_\Omega(X) = \mathcal{P}_\Omega(M) \end{aligned} \tag{I.3}$$

where the *nuclear norm* $\|X\|_*$ of a matrix X is defined as the sum of its singular values

$$\|X\|_* := \sum_i \sigma_i(X) \tag{I.4}$$

[problem (I.3) is a semidefinite program [11]]. They proved that if Ω is sampled uniformly at random among all subset of cardinality m and M obeys a low coherence condition which we will review later, then with large probability, the unique solution to (I.3) is exactly M, provided that the number of samples obeys

$$m \geq C n^{6/5} r \log n \tag{I.5}$$

(to be completely exact, there is a restriction on the range of values that r can take on).

In (I.5), the number of samples per degree of freedom is not logarithmic or polylogarithmic in the dimension, and one would like to know whether better results approaching the $nr \log n$ limit are possible. This paper provides a positive answer. In detail, this work develops many useful matrix models for which nuclear norm minimization is guaranteed to succeed as soon as the number of entries is of the form $nr\operatorname{polylog}(n)$.

C. Main Results

A contribution of this paper is the development simple hypotheses about the matrix M which make it recoverable by semidefinite programming from nearly minimally sampled entries. To state our assumptions, we recall the SVD of M (I.1) and denote by P_U (resp. P_V) the orthogonal projections onto the column (resp. row) space of M; i.e., the span of the left (resp. right) singular vectors. Note that

$$P_U = \sum_{i \in [r]} u_i u_i^*; \quad P_V = \sum_{i \in [r]} v_i v_i^*. \tag{I.6}$$

Next, define the matrix E as

$$E := \sum_{i \in [r]} u_i v_i^*. \tag{I.7}$$

We observe that E interacts well with P_U and P_V, in particular, obeying the identities

$$P_U E = E = E P_V; \quad E^* E = P_V; \quad E E^* = P_U.$$

One can view E as a sort of matrix-valued "sign pattern" for M (compare (I.7) with (I.1)), and is also closely related to the subgradient $\partial \|M\|_*$ of the nuclear norm at M (see (III.2)).

It is clear that some assumptions on the singular vectors u_i, v_i (or on the spaces U, V) are needed in order to have a hope of efficient matrix completion. For instance, if u_1 and v_1 are Kronecker delta functions at positions i, j respectively, then the singular value σ_1 can only be recovered if one actually samples the

(i,j) coordinate, which is only likely if one is sampling a significant fraction of the entire matrix. Thus, we need the vectors u_i, v_i to be "spread out" or "incoherent" in some sense. In our arguments, it will be convenient to phrase incoherence assumption using the projection matrices P_U, P_V and the sign pattern matrix E. More precisely, our assumptions are as follows.

A1 There exists $\mu_1 > 0$ such that for all pairs $(a,a') \in [n_1] \times [n_1]$ and $(b,b') \in [n_2] \times [n_2]$

$$\left|\langle e_a, P_U e_{a'}\rangle - \frac{r}{n_1} 1_{a=a'}\right| \le \mu_1 \frac{\sqrt{r}}{n_1} \tag{I.8a}$$

$$\left|\langle e_b, P_V e_{b'}\rangle - \frac{r}{n_2} 1_{b=b'}\right| \le \mu_1 \frac{\sqrt{r}}{n_2}. \tag{I.8b}$$

A2 There exists $\mu_2 > 0$ such that for all $(a,b) \in [n_1] \times [n_2]$

$$|E_{ab}| \le \mu_2 \frac{\sqrt{r}}{\sqrt{n_1 n_2}}. \tag{I.9}$$

We will say that the matrix M obeys the strong incoherence property with parameter μ if one can take μ_1 and μ_2 both less than or equal to μ (this property is related to, but slightly different from, the *incoherence property*, which will be discussed in Section I-F1).

Remark. Our assumptions only involve the singular vectors $u_1, \ldots, u_r, v_1, \ldots, v_r$ of M; the singular values $\sigma_1, \ldots, \sigma_r$ are completely unconstrained. This lack of dependence on the singular values is a consequence of the geometry of the nuclear norm [and, in particular, the fact that the subgradient $\partial \|X\|_*$ of this norm is independent of the singular values, see (III.2)].

It is not hard to see that μ must be greater than 1. For instance, (I.9) implies

$$r = \sum_{(a,b) \in [n_1] \times [n_2]} |E_{ab}|^2 \le \mu_2^2 r$$

which forces $\mu_2 \ge 1$. The Frobenius norm identities

$$r = \|P_U\|_F^2 = \sum_{a,a' \in [n_1]} |\langle e_a, P_U e_{a'}\rangle|^2$$

and (I.8a), (I.8b) also place a similar lower bound on μ_1.

We will show that 1) matrices obeying the strong incoherence property with a small value of the parameter μ can be recovered from fewer entries and that 2) many matrices of interest obey the strong incoherence property with a small μ. We will shortly develop three models: the uniformly bounded orthogonal model, the low-rank low-coherence model, and the random orthogonal model, which all illustrate the point that if the singular vectors of M are "spread out" in the sense that their amplitudes all have about the same size, then the parameter μ is low. In some sense, "most" low-rank matrices obey the strong incoherence property with $\mu = O\left(\sqrt{\log n}\right)$, where $n = \max(n_1, n_2)$. Here, $O(\cdot)$ is the standard asymptotic notation, which is reviewed in Section I-H.

Our first matrix completion result is as follows.

Theorem 1.1 (Matrix Completion I): Let $M \in \mathbb{R}^{n_1 \times n_2}$ be a fixed matrix of rank $r = O(1)$ obeying the strong incoherence property with parameter μ. Write $n := \max(n_1, n_2)$. Suppose we observe m entries of M with locations sampled uniformly at random. Then there is a positive numerical constant C such that if

$$m \ge C \mu^4 n (\log n)^2 \tag{I.10}$$

then M is the unique solution to (I.3) with probability at least $1 - n^{-3}$. In other words: with high probability, nuclear-norm minimization recovers all the entries of M with no error.

This result is noteworthy for two reasons. The first is that the matrix model is deterministic and only needs the strong incoherence assumption. The second is more substantial. Consider the class of bounded rank matrices obeying $\mu = O(1)$. We shall see that no method whatsoever can recover those matrices unless the number of entries obeys $m \ge c_0\, n \log n$ for some positive numerical constant c_0; that is, the information theoretic limit. Thus, Theorem 1.1 asserts that exact recovery by nuclear-norm minimization occurs nearly as soon as it is information theoretically possible. Indeed, if the number of samples is slightly larger, by a logarithmic factor, than the information theoretic limit, then (I.3) fills in the missing entries with no error.

We stated Theorem 1.1 for bounded ranks, but our proof gives a result for all values of r. Indeed, the argument will establish that the recovery is exact with high probability provided that

$$m \ge C \mu^4 n r^2 (\log n)^2. \tag{I.11}$$

When $r = O(1)$, this is Theorem 1.1. We will prove a stronger and near-optimal result below (Theorem 1.2) in which we replace the quadratic dependence on r with linear dependence. The reason why we state Theorem 1.1 first is that its proof is somewhat simpler than that of Theorem 1.2, and we hope that it will provide the reader with a useful lead-in to the claims and proof of our main result.

Theorem 1.2 (Matrix Completion II): Under the same hypotheses as in Theorem 1.1, there is a numerical constant C such that if

$$m \ge C \mu^2 n r \log^6 n \tag{I.12}$$

M is the unique solution to (I.3) with probability at least $1 - n^{-3}$.

This result is general and nonasymptotic.

The proof of Theorems 1.1, I.2 will occupy the bulk of the paper, starting at Section III.

D. A Surprise

We find it unexpected that nuclear norm-minimization works so well, for reasons we now pause to discuss. For simplicity, consider matrices with a strong incoherence parameter μ polylogarithmic in the dimension. We know that for the rank minimization program (I.2) to succeed, or equivalently for the problem to be well posed, the number of samples must exceed a constant times $nr \log n$. However, Theorem 1.2 proves that the convex relaxation is rigorously exact nearly as soon as our problem has a unique low-rank solution. The surprise here is that admittedly, there is *a priori* no good reason to suspect that convex relaxation might work so well. There is *a priori* no good reason to suspect that the gap between what combinatorial and

convex optimization can do is this small. In this sense, we find these findings a little unexpected.

The reader will note an analogy with the recent literature on compressed sensing, which shows that under some conditions, the sparsest solution to an underdetermined system of linear equations is that with minimum ℓ_1 norm.

E. Model Matrices

We now discuss model matrices which obey the conditions (I.8) and (I.9) for small values of the strong incoherence parameter μ. For simplicity we restrict attention to the square matrix case $n_1 = n_2 = n$.

1) Uniformly Bounded Model: In this section, we shall show, roughly speaking, that almost all $n \times n$ matrices M with singular vectors obeying the size property

$$\|u_k\|_{\ell_\infty}, \|v_k\|_{\ell_\infty} \leq \sqrt{\mu_B/n} \tag{I.13}$$

with $\mu_B = O(1)$ also satisfy the assumptions **A1** and **A2** with $\mu_1, \mu_2 = O\left(\sqrt{\log n}\right)$. This justifies our earlier claim that when the singular vectors are spread out, then the strong incoherence property holds for a small value of μ.

We define a random model obeying (I.13) as follows: take two arbitrary families of n orthonormal vectors $[u_1, \ldots, u_n]$ and $[v_1, \ldots, v_n]$ obeying (I.13). We allow the u_i and v_i to be deterministic; for instance, one could have $u_i = v_i$ for all $i \in [n]$.

1) Select r left singular vectors $u_{\alpha(1)}, \ldots, u_{\alpha(r)}$ at random with replacement from the first family, and r right singular vectors $v_{\beta(1)}, \ldots, v_{\beta(r)}$ from the second family, also at random. We do *not* require that the β are chosen independently from the α; for instance one could have $\beta(k) = \alpha(k)$ for all $k \in [r]$.
2) Set $M := \sum_{k \in [r]} \epsilon_k \sigma_k u_{\alpha(k)} v^*_{\beta(k)}$, where the signs $\epsilon_1, \ldots, \epsilon_r \in \{-1, +1\}$ are chosen independently at random (with probability 1/2 of each choice of sign), and $\sigma_1, \ldots, \sigma_r > 0$ are arbitrary distinct positive numbers (which are allowed to depend on the previous random choices).

We emphasize that the only assumptions about the families $[u_1, \ldots, u_n]$ and $[v_1, \ldots, v_n]$ is that they have small components. For example, they may be the same. Also note that this model allows for any kind of dependence between the left and right singular selected vectors. For instance, we may select the same columns as to obtain a symmetric matrix as in the case where the two families are the same. Thus, one can think of our model as producing a generic matrix with uniformly bounded singular vectors.

We now show that P_U, P_V, and E obey (I.8) and (I.9), with $\mu_1, \mu_2 = O\left(\mu_B \sqrt{\log n}\right)$, with large probability. For (I.9), observe that

$$E = \sum_{k \in [r]} \epsilon_k u_{\alpha(k)} v^*_{\beta(k)}$$

and $\{\epsilon_k\}$ is a sequence of i.i.d. ± 1 symmetric random variables. Then Hoeffding's inequality shows that $\mu_2 = O\left(\mu_B \sqrt{\log n}\right)$; see [7] for details.

For (I.8), we will use a beautiful concentration-of-measure result of McDiarmid.

Theorem 1.3 : [19] Let $\{a_1, \ldots, a_n\}$ be a sequence of scalars obeying $|a_i| \leq \alpha$. Choose a random set S of size s without replacement from $\{1, \ldots, n\}$ and let $Y = \sum_{i \in S} a_i$. Then for each $t \geq 0$

$$\mathbb{P}(|Y - \mathbb{E}Y| \geq t) \leq 2e^{-\frac{t^2}{2s\alpha^2}}. \tag{I.14}$$

From (I.6), we have

$$P_U = \sum_{k \in S} u_k u_k^*$$

where $S := \{\alpha(1), \ldots, \alpha(r)\}$. For any fixed $a, a' \in [n]$, set

$$Y := \langle P_U e_a, P_U e_{a'} \rangle = \sum_{k \in S} \langle e_a, u_k \rangle \langle u_k, e_{a'} \rangle$$

and note that $\mathbb{E}Y = \frac{r}{n} 1_{a=a'}$. Since $|\langle e_a, u_k \rangle \langle u_k, e_{a'} \rangle| \leq \mu_B/n$, we apply (I.14) and obtain

$$\mathbb{P}\left(\left| \langle P_U e_a, P_U e_{a'} \rangle - 1_{\{a=a'\}} r/n \right| \geq \lambda \mu_B \frac{\sqrt{r}}{n} \right) \leq 2e^{-\lambda^2/2}.$$

Taking λ proportional to $\sqrt{\log n}$ and applying the union bound for $a, a' \in [n]$ proves (I.8) with probability at least $1 - n^{-3}$ (say) with $\mu_1 = O\left(\mu_B \sqrt{\log n}\right)$.

Combining this computation with Theorems 1.1, 1.2, we have established the following corollary (here and below, MC is a shorthand for matrix completion):

Corollary 1.4 (MC, Uniformly Bounded Model): Let M be a matrix sampled from a uniformly bounded model. Under the hypotheses of Theorem 1.1, if

$$m \geq C \mu_B^2 n r \log^7 n$$

M is the unique solution to (I.3) with probability at least $1 - n^{-3}$. As we shall see below, when $r = O(1)$, it suffices to have

$$m \geq C \mu_B^4 n \log^2 n.$$

Remark. For large values of the rank, the assumption that the ℓ_∞ norm of the singular vectors is $O\left(1/\sqrt{n}\right)$ is not sufficient to conclude that (I.8) holds with $\mu_1 = O\left(\sqrt{\log n}\right)$. Thus, the extra randomization step (in which we select the r singular vectors from a list of n possible vectors) is in some sense necessary. As an example, take $[u_1, \ldots, u_r]$ to be the first r columns of the Hadamard transform where each row corresponds to a frequency. Then $\|u_k\|_{\ell_\infty} = 1/\sqrt{n}$, but if $r \leq n/2$, the first two rows of $[u_1, \ldots, u_r]$ are identical. Hence

$$\langle P_U e_1, P_U e_2 \rangle = r/n.$$

Obviously, this does not scale like $\sqrt{r}/n$. Similarly, the sign flip (step 2) is also necessary as otherwise, we could have $E = P_U$ as in the case where $[u_1, \ldots, u_n] = [v_1, \ldots, v_n]$ and the same columns are selected. Here

$$\max_a E_{aa} = \max_a \|P_U e_a\|^2 \geq \frac{1}{n} \sum_a \|P_U e_a\|^2 = \frac{r}{n}$$

which does not scale like $\sqrt{r}/n$ either.

2) Low-Rank Low-Coherence Model: When the rank is small, the assumption that the singular vectors are spread is sufficient to show that the parameter μ is small. To see this, suppose that the singular vectors obey (I.13). Then

$$\left|\langle P_U e_a, P_U e_{a'}\rangle - 1_{\{a=a'\}}\frac{r}{n}\right| \le \max_{a\in[n]} \|P_U e_a\|^2 \le \frac{\mu_B r}{n}. \tag{I.15}$$

The first inequality follows from the Cauchy–Schwarz inequality

$$|\langle P_U e_a, P_U e_{a'}\rangle| \le \|P_U e_a\|\|P_U e_{a'}\|$$

for $a \neq a'$ and from the Frobenius norm bound

$$\max_{a\in[n]} \|P_U e_a\|^2 \ge \frac{1}{n}\|P_U\|_F^2 = \frac{r}{n}.$$

This gives $\mu_1 \le \mu_B\sqrt{r}$. Also, by another application of Cauchy–Schwarz, we have

$$|E_{ab}| \le \max_{a\in[n]} \|P_U e_a\| \max_{b\in[n]} \|P_V e_b\| \le \frac{\mu_B r}{n} \tag{I.16}$$

so that we also have $\mu_2 \le \mu_B\sqrt{r}$. In short, $\mu \le \mu_B\sqrt{r}$.

Our low-rank low-coherence model assumes that $r = O(1)$ and that the singular vectors obey (I.13). When $\mu_B = O(1)$, this model obeys the strong incoherence property with $\mu = O(1)$. In this case, Theorem 1.1 specializes as follows.

Corollary 1.5 (MC, Low-Rank Low-Coherence Model): Let M be a matrix of bounded rank ($r = O(1)$) whose singular vectors obey (I.13). Under the hypotheses of Theorem 1.1, if

$$m \ge C\mu_B^4 n \log^2 n$$

then M is the unique solution to (I.3) with probability at least $1 - n^{-3}$.

3) Random Orthogonal Model: Our last model is borrowed from [7] and assumes that the column matrices $[u_1, \ldots, u_r]$ and $[v_1, \ldots, v_r]$ are independent random orthogonal matrices, with no assumptions whatsoever on the singular values $\sigma_1, \ldots, \sigma_r$. Note that this is a special case of the uniformly bounded model since this is equivalent to selecting two $n \times n$ random orthonormal bases, and then selecting the singular vectors as in Section I-E1. Since we know that the maximum entry of an $n \times n$ random orthogonal matrix is bounded by a constant times $\sqrt{\frac{\log n}{n}}$ with large probability, then Section I-E1 shows that this model obeys the strong incoherence property with $\mu = O(\log n)$. Theorems 1.1, 1.2 then give:

Corollary 1.6 (MC, Random Orthogonal Model): Let M be a matrix sampled from the random orthogonal model. Under the hypotheses of Theorem 1.1, if

$$m \ge Cnr\log^8 n$$

then M is the unique solution to (I.3) with probability at least $1 - n^{-3}$. The exponent 8 can be lowered to 7 when $r \ge \log n$ and to 6 when $r = O(1)$.

As mentioned earlier, we have a lower bound $m \ge 2nr - r^2$ for matrix completion, which can be improved to $m \ge Cnr\log n$ under reasonable hypotheses on the matrix M. Thus, the hypothesis on m in Corollary 1.6 cannot be substantially improved. However, it is likely that by specializing the proofs of our general results (Theorems 1.1 and 1.2) to this special case, one may be able to improve the power of the logarithm here, though it seems that a substantial effort would be needed to reach the optimal level of $nr\log n$ even in the bounded rank case. Speaking of logarithmic improvements, we have shown that $\mu = O(\log n)$, which is sharp since for $r = 1$, one cannot hope for better estimates. For r much larger than $\log n$, however, one can improve this to $\mu = O\left(\sqrt{\log n}\right)$. As far as μ_1 is concerned, this is essentially a consequence of the Johnson-Lindenstrauss lemma. For $a \neq a'$, write

$$\langle P_U e_a, P_U e_{a'}\rangle = \frac{1}{4}\left(\|P_U e_a + P_U e_{a'}\|^2 - \|P_U e_a - P_U e_{a'}\|^2\right).$$

We claim that for each $a \neq a'$

$$\left|\|P_U(e_a \pm e_{a'})\|^2 - \frac{2r}{n}\right| \le C\frac{\sqrt{r\log n}}{n} \tag{I.17}$$

with probability at least $1 - n^{-5}$, say. This inequality is, indeed, well known. Observe that $\|P_U x\|$ has the same distribution than the Euclidean norm of the first r components of a vector uniformly distributed on the $n-1$ dimensional sphere of radius $\|x\|$. Then we have [4]

$$\mathbb{P}\left(\sqrt{\frac{r}{n}}(1-\epsilon)\|x\| \le \|P_U x\| \le \sqrt{\frac{r}{n}}(1-\epsilon)^{-1}\|x\|\right) \le 2e^{-\epsilon^2 r/4} + 2e^{-\epsilon^2 n/4}.$$

Choosing $x = e_a \pm e_{a'}$, $\epsilon = C_0\sqrt{\frac{\log n}{r}}$, and applying the union bound proves the claim as long as r is sufficiently larger than $\log n$. Finally, since a bound on the diagonal term $\|P_U e_a\|^2 - r/n$ in (I.8) follows from the same inequality by simply choosing $x = e_a$, we have $\mu_1 = O\left(\sqrt{\log n}\right)$. Similar arguments for μ_2 exist but we forgo the details.

F. Comparison With Other Work

1) Nuclear Norm Minimization: The mathematical study of matrix completion began with [7], which made slightly different incoherence assumptions than in this paper. Namely, let us say that the matrix M obeys the *incoherence property* with a parameter $\mu_0 > 0$ if

$$\|P_U e_a\|^2 \le \frac{\mu_0 r}{n_1}, \quad \|P_V e_b\|^2 \le \frac{\mu_0 r}{n_2} \tag{I.18}$$

for all $a \in [n_1]$, $b \in [n_2]$. Again, this implies $\mu_0 \ge 1$.

In [7], it was shown that if a fixed matrix M obeys the incoherence property with parameter μ_0, then nuclear minimization succeeds with large probability if

$$m \ge C\mu_0 n^{6/5} r\log n \tag{I.19}$$

provided that $\mu_0 r \le n^{1/5}$.

Now consider a matrix M obeying the strong incoherence property with $\mu = O(1)$. Then since $\mu_0 \ge 1$, (I.19) guarantees exact reconstruction only if $m \ge Cn^{6/5} r\log n$ (and

$r = O(n^{1/5})$) while our results only need $nr\text{polylog}(n)$ samples. Hence, our results provide a substantial improvement over (I.19) at least in the regime which permits minimal sampling.

We would like to note that there are obvious relationships between the best incoherence parameter μ_0 and the best strong incoherence parameters μ_1, μ_2 for a given matrix M, which we take to be square for simplicity. On the one hand, (I.8) implies that

$$\|P_U e_a\|^2 \leq \frac{r}{n} + \frac{\mu_1\sqrt{r}}{n}$$

so that one can take $\mu_0 \leq 1 + \mu_1/\sqrt{r}$. This shows that one can apply results from the incoherence model [in which we only know (I.18)] to our model (in which we assume strong incoherence). On the other hand

$$|\langle P_U e_a, P_U e_{a'}\rangle| \leq \|P_U e_a\|\|P_U e_{a'}\| \leq \frac{\mu_0 r}{n}$$

so that $\mu_1 \leq \mu_0\sqrt{r}$. Similarly, $\mu_2 \leq \mu_0\sqrt{r}$ so that one can transfer results in the other direction as well. The point of using **A1** rather than (I.18) is that it will prove useful in giving simple estimates about the coefficients of a linear transformation, which plays a crucial role in the analysis.

We would like to mention another important paper [21] inspired by compressed sensing, and which also recovers low-rank matrices from partial information. The model in [21], however, assumes some sort of Gaussian measurements and is completely different from the completion problem discussed in this paper.

2) Spectral Methods: An interesting new approach to the matrix completion problem has been recently introduced in [14].[2] This algorithm starts by trimming each row and column with too many entries; i.e., one replaces the entries in those rows and columns by zero. Then one computes the SVD of the trimmed matrix and truncate it as to only keep the top r singular values (note that one would need to know r *a priori*). Then under some conditions (including the incoherence property (I.18) with $\mu = O(1)$), this work shows that accurate—not exact—recovery is possible from a minimal number of samples, namely, on the order of $O(nr)$ samples. Having said this, this work is not directly comparable to ours because it operates in a different regime. First, the results, unlike ours, are asymptotic and valid only in a regime where the dimensions of the matrix tend to infinity in a fixed ratio. Second, there is a strong assumption about the range of the singular values the unknown matrix can take on while we make no such assumption; they must be clustered so that no singular value can be too large or too small compared to the others. Finally, this work only shows approximate recovery—not exact recovery as we do here—although exact recovery results have been announced. This work is of course very interesting because it may show that methods—other than convex optimization—can also achieve minimal sampling bounds.

G. Lower Bounds

We would like to conclude the tour of the results introduced in this paper with a simple lower bound, which highlights the fundamental role played by the coherence in controlling what is information-theoretically possible.

Theorem 1.7 (Uniqueness Implies a Miminimal Sampling Rate): Fix $1 \leq m, r \leq n$ and $\mu_0 \geq 1$, let $0 < \delta < 1/2$, and suppose that we do not have the condition

$$m \geq n^2\left(1 - e^{-\frac{\mu_0 r}{n}\log\left(\frac{n}{2\delta}\right)}\right). \tag{I.20}$$

Easier to read, suppose we do not have

$$m \geq (1-\epsilon)\mu_0 nr\log\left(\frac{n}{2\delta}\right) \tag{I.21}$$

where $\epsilon := \frac{1}{2}\frac{\mu_0 r}{n}\log\left(\frac{n}{2\delta}\right)$. Then there exist infinitely many pairs of distinct $n \times n$ matrices $M \neq M'$ of rank at most r and obeying the incoherence property (I.18) with parameter μ_0 such that $\mathcal{P}_\Omega(M) = \mathcal{P}_\Omega(M')$ with probability at least δ. Here, each entry is observed with probability $p = m/n^2$ independently from the others.

Clearly, even if one knows the rank and the coherence of a matrix ahead of time, then no algorithm can be guaranteed to succeed based on the knowledge of $\mathcal{P}_\Omega(M)$ only, since they are many candidates which are consistent with these data. We prove this theorem in Section II. Informally, Theorem 1.7 asserts that (I.20) is a necessary condition for matrix completion to work with high probability if all we know about the matrix M is that it has rank at most r and the incoherence property with parameter μ_0.

Recall that the number of degrees of freedom of a rank-r matrix is $2nr(1 - r/2n)$. Hence, to recover an arbitrary rank-r matrix with the incoherence property with parameter μ_0 with any decent probability by any method whatsoever, the minimum number of samples must be about the number of degrees of freedom times $\mu_0 \log n$; in other words, the oversampling factor is directly proportional to the coherence. Since $\mu_0 \geq 1$, this justifies our earlier assertions that $nr\log n$ samples are really needed.

In the *Bernoulli model* used in Theorem 1.7, the number of entries is a binomial random variable sharply concentrated around its mean m. There is very little difference between this model and the *uniform model* which assumes that Ω is sampled uniformly at random among all subsets of cardinality m. Results holding for one hold for the other with only very minor adjustments. Because we are concerned with essential difficulties, not technical ones, we will often prove our results using the Bernoulli model, and indicate how the results may easily be adapted to the uniform model.

H. Notation

Before continuing, we provide here a brief summary of the notation used throughout the paper. To simplify the notation, we shall work exclusively with square matrices, thus

$$n_1 = n_2 = n.$$

The results for nonsquare matrices (with $n = \max(n_1, n_2)$) are proven in exactly the same fashion, but will add more subscripts to a notational system which is already quite complicated, and we will leave the details to the interested reader. We will also

[2] A journal version [13] has appeared since the original submission of our paper

assume that $n \geq C$ for some sufficiently large absolute constant C, as our results are vacuous in the regime $n = O(1)$.

Throughout, we will always assume that m is at least as large as $2nr$, thus

$$2r \leq np, \quad p := m/n^2. \tag{I.22}$$

A variety of norms on matrices $X \in \mathbb{R}^{n \times n}$ will be discussed. The *spectral norm* (or *operator norm*) of a matrix is denoted by

$$\|X\| := \sup_{x \in \mathbb{R}^n : \|x\|=1} \|Xx\| = \sup_{1 \leq j \leq n} \sigma_j(X).$$

The Euclidean inner product between two matrices is defined by the formula

$$\langle X, Y \rangle := \mathrm{trace}(X^* Y)$$

and the corresponding Euclidean norm, called the *Frobenius norm* or *Hilbert–Schmidt norm*, is denoted

$$\|X\|_F := \langle X, X \rangle^{1/2} = \left(\sum_{j=1}^{n} \sigma_j(X)^2 \right)^{1/2}.$$

The *nuclear norm* of a matrix X is denoted

$$\|X\|_* := \sum_{j=1}^{n} \sigma_j(X).$$

For vectors, we will only consider the usual Euclidean ℓ_2 norm which we simply write as $\|x\|$.

Further, we will also manipulate linear transformations which act on the space $\mathbb{R}^{n \times n}$ matrices such as $\mathcal{P}_\Omega$, and we will use calligraphic letters for these operators as in $\mathcal{A}(X)$. In particular, the identity operator on this space will be denoted by $\mathcal{I} : \mathbb{R}^{n \times n} \to \mathbb{R}^{n \times n}$, and should *not* be confused with the identity matrix $I \in \mathbb{R}^{n \times n}$. The only norm we will consider for these operators is their spectral norm (the top singular value)

$$\|\mathcal{A}\| := \sup_{X : \|X\|_F \leq 1} \|\mathcal{A}(X)\|_F.$$

Thus, for instance

$$\|\mathcal{P}_\Omega\| = 1.$$

We use the usual asymptotic notation, for instance writing $O(M)$ to denote a quantity bounded in magnitude by CM for some absolute constant $C > 0$. We will sometimes raise such notation to some power, for instance $O(M)^M$ would denote a quantity bounded in magnitude by $(CM)^M$ for some absolute constant $C > 0$. We also write $X \lesssim Y$ for $X = O(Y)$, and $\mathrm{poly}(X)$ for $O(1 + |X|)^{O(1)}$.

We use 1_E to denote the indicator function of an event E, e.g., $1_{a=a'}$ equals 1 when $a = a'$ and 0 when $a \neq a'$.

If A is a finite set, we use $|A|$ to denote its cardinality.

We record some (standard) conventions involving empty sets. The set $[n] := \{1, \ldots, n\}$ is understood to be the empty set when $n = 0$. We also make the usual conventions that an empty sum $\sum_{x \in \emptyset} f(x)$ is zero, and an empty product $\prod_{x \in \emptyset} f(x)$ is one. Note, however, that a k-fold sum such as $\sum_{a_1, \ldots, a_k \in [n]} f(a_1, \ldots, a_k)$ does not vanish when $k = 0$, but is instead equal to a single summand $f()$ with the empty tuple $() \in [n]^0$ as the input; thus, for instance, the identity

$$\sum_{a_1, \ldots, a_k \in [n]} \prod_{i=1}^{k} f(a_i) = \left(\sum_{a \in [n]} f(a) \right)^k$$

is valid both for positive integers k and for $k = 0$ (and both for nonzero f and for zero f, recalling of course that $0^0 = 1$). We will refer to sums over the empty tuple as *trivial sums* to distinguish them from *empty sums*.

II. Lower Bounds

This section proves Theorem 1.7, which asserts that no method can recover an arbitrary $n \times n$ matrix of rank r and coherence at most μ_0 unless the number of random samples obeys (I.20). As stated in the theorem, we establish lower bounds for the Bernoulli model, which then apply to the model where exactly m entries are selected uniformly at random, see the Appendix for details.

It may be best to consider a simple example first to understand the main idea behind the proof of Theorem 1.7. Suppose that $r = 1$, $\mu_0 > 1$ in which case $M = xy^*$. For simplicity, suppose that y is fixed, say $y = (1, \ldots, 1)$, and x is chosen arbitrarily from the cube $\left[1, \sqrt{\mu_0}\right]^n$ of $\mathbb{R}^n$. One easily verifies that M obeys the coherence property with parameter μ_0 (and in fact also obeys the strong incoherence property with a comparable parameter). Then to recover M, we need to see at least one entry per row. For instance, if the first row is unsampled, one has no information about the first coordinate x_1 of x other than that it lies in $\left[1, \sqrt{\mu_0}\right]$, and so the claim follows in this case by varying x_1 along the infinite set $\left[1, \sqrt{\mu_0}\right]$.

Now under the Bernoulli model, the number of observed entries in the first row—and in any fixed row or column—is a binomial random variable with a number of trials equal to n and a probability of success equal to p. Therefore, the probability π_0 that any row is unsampled is equal to $\pi_0 = (1 - p)^n$. By independence, the probability that all rows are sampled at least once is $(1 - \pi_0)^n$, and any method succeeding with probability greater $1 - \delta$ would need

$$(1 - \pi_0)^n \geq 1 - \delta$$

or $-n\pi_0 \geq n \log(1 - \pi_0) \geq \log(1 - \delta)$. When $\delta < 1/2$, $\log(1 - \delta) \geq -2\delta$, and, thus, any method would need

$$\pi_0 \leq \frac{2\delta}{n}.$$

This is the desired conclusion when $\mu_0 > 1, r = 1$.

This type of simple analysis easily extends to general values of the rank r and of the coherence. Without loss of generality, assume that $\ell := \frac{n}{\mu_0 r}$ is an integer, and consider a (self-adjoint) $n \times n$ matrix M of rank r of the form

$$M := \sum_{k=1}^{r} \sigma_k u_k u_k^*$$

where the σ_k are drawn arbitrarily from $(0,1]$ (say), and the singular vectors $u_1,\dots,u_r$ are defined as follows:

$$u_k := \sqrt{\frac{1}{\ell}} \sum_{i\in B_k} e_i$$
$$B_k = \{(k-1)\ell+1,(k-1)\ell+2,\dots,k\ell\}$$

that is to say, u_k vanishes everywhere except on a support of ℓ consecutive indices. Clearly, this matrix is incoherent with parameter μ_0 in the sense of (I.18). Because the supports of the singular vectors are disjoint, M is a block-diagonal matrix with diagonal blocks of size $\ell\times\ell$. We now argue as before. Recovery with positive probability is impossible unless we have sampled at least one entry per row of each diagonal block, since otherwise we would be forced to guess at least one of the σ_k based on no information (other than that σ_k lies in $[0,1]$), and the theorem will follow by varying this singular value. Now the probability π_1 that the first row of the first block—and any fixed row of any fixed block—is unsampled is equal to $(1-p)^\ell$. Therefore, any method succeeding with probability greater $1-\delta$ would need

$$(1-\pi_1)^n \geq 1-\delta$$

which implies $\pi_1 \leq 2\delta/n$ just as before. With $\pi_1 = (1-p)^\ell$, a simple algebraic manipulation gives (I.20) under the Bernoulli model. The second part of the theorem, namely, (I.21) follows from $1-e^{-x} > x - x^2/2$ whenever $x \geq 0$.

III. Strategy and Novelty

This section outlines the strategy for proving our main results, Theorems 1.1 and 1.2. The proofs of these theorems are the same up to a point where the arguments to estimate the moments of a certain random matrix differ. In this section, we present the common part of the proof, leading to two key moment estimates, while the proofs of these crucial estimates are the object of later sections.

One can, of course, prove our claims for the Bernoulli model with $p = m/n^2$ and transfer the results to the uniform model, by using the arguments in the appendix. For example, the probability that the recovery via (I.3) is not exact is at most twice that under the Bernoulli model.

A. Duality

We begin by recalling some calculations from [7, Section 3]. From standard duality theory, we know that the correct matrix $M \in \mathbb{R}^{n\times n}$ is a solution to (I.3) if and only if there exists a dual certificate $Y \in \mathbb{R}^{n\times n}$ with the property that $\mathcal{P}_\Omega(Y)$ is a subgradient of the nuclear norm at M, which we write as

$$\mathcal{P}_\Omega(Y) \in \partial\|M\|_*. \tag{III.1}$$

We recall the projection matrices P_U, P_V and the companion matrix E defined by (I.6), (I.7). It is known [16], [25] that

$$\partial\|M\|_* = \Big\{E+W : W\in\mathbb{R}^{n\times n},\ P_U W = 0,\ WP_V = 0,\ \|W\|\leq 1\Big\}. \tag{III.2}$$

There is a more compact way to write (III.2). Let $T \subset \mathbb{R}^{n\times n}$ be the span of matrices of the form $u_k y^*$ and $x v_k^*$ and let $T^\perp$ be its orthogonal complement. Let $\mathcal{P}_T : \mathbb{R}^{n\times n} \to T$ be the orthogonal projection onto T; one easily verifies the explicit formula

$$\mathcal{P}_T(X) = P_U X + X P_V - P_U X P_V \tag{III.3}$$

and note that the complementary projection $\mathcal{P}_{T^\perp} := \mathcal{I} - \mathcal{P}_T$ is given by the formula

$$\mathcal{P}_{T^\perp}(X) = (I-P_U)X(I-P_V). \tag{III.4}$$

In particular, $\mathcal{P}_{T^\perp}$ is a contraction

$$\|\mathcal{P}_{T^\perp}\| \leq 1. \tag{III.5}$$

Then $Z \in \partial\|M\|_*$, if and only if

$$\mathcal{P}_T(Z) = E, \text{and } \|\mathcal{P}_{T^\perp}(Z)\| \leq 1.$$

With these preliminaries in place, [7] establishes the following result.

Lemma 3.1 (Dual Certificate Implies Matrix Completion): Let the notation be as above. Suppose that the following two conditions hold.

1) There exists $Y \in \mathbb{R}^{n\times n}$ obeying:
   a) $\mathcal{P}_\Omega(Y) = Y$;
   b) $\mathcal{P}_T(Y) = E$;
   c) $\|\mathcal{P}_{T^\perp}(Y)\| < 1$.
2) The restriction $\mathcal{P}_\Omega \restriction_T : T \to \mathcal{P}_\Omega(\mathbb{R}^{n\times n})$ of the (sampling) operator $\mathcal{P}_\Omega$ restricted to T is injective.

Then M is the unique solution to the convex program (I.3).

Proof: See [7, Lemma 3.1]. ∎

The second sufficient condition, namely, the injectivity of the restriction to $\mathcal{P}_\Omega$ has been studied in [7]. We recall a useful result.

Theorem 3.2 (Rudelson Selection Estimate): [7, Theorem 4.1] Suppose Ω is sampled according to the Bernoulli model and put $n := \max(n_1,n_2)$. Assume that M obeys (I.18). Then there is a numerical constant C_R such that for all $\beta > 1$, we have the bound

$$p^{-1}\|\mathcal{P}_T\mathcal{P}_\Omega\mathcal{P}_T - p\mathcal{P}_T\| \leq a \tag{III.6}$$

with probability at least $1-3n^{-\beta}$ provided that $a < 1$, where a is the quantity

$$a := C_R\sqrt{\frac{\mu_0 nr(\beta\log n)}{m}}. \tag{III.7}$$

We will apply this theorem with $\beta := 4$ (say). The statement (III.6) is stronger than the injectivity of the restriction of $\mathcal{P}_\Omega$ to T. Indeed, take m sufficiently large so that $a < 1$. Then if $X \in T$, we have

$$\|\mathcal{P}_T\mathcal{P}_\Omega(X) - pX\|_F < ap\|X\|_F$$

and obviously, $\mathcal{P}_\Omega(X)$ cannot vanish unless $X = 0$.

In order for the condition $a < 1$ to hold, we must have

$$m \geq C_0 \mu_0 nr \log n \tag{III.8}$$

for a suitably large constant C_0. However, this follows from the hypotheses in either Theorem 1.1 or Theorem 1.2, for reasons that we now pause to explain. In either of these theorems, we have

$$m \geq C_1 \mu nr \log n \tag{III.9}$$

for some large constant C_1. Recall from Section I-F1 that $\mu_0 \leq 1+\mu_1/\sqrt{r} \leq 1+\mu/\sqrt{r}$, and so (III.9) implies (III.8) whenever $\mu_0 \geq 2$ (say). When $\mu_0 < 2$, we can also deduce (III.8) from (III.9) by applying the trivial bound $\mu \geq 1$ noted in the introduction.

In summary, to prove Theorem 1.1 or Theorem 1.2, it suffices (under the hypotheses of these theorems) to exhibit a dual matrix Y obeying the first sufficient condition of Lemma 3.1, with probability at least $1 - n^{-3}/2$ (say). This is the objective of the remaining sections of the paper.

B. Dual Certificate

Whenever the map $\mathcal{P}_\Omega \restriction_T : T \to \mathcal{P}_\Omega(\mathbb{R}^{n\times n})$ restricted to T is injective, the linear map

$$\begin{aligned} T &\to T \\ X &\mapsto \mathcal{P}_T \mathcal{P}_\Omega \mathcal{P}_T(X) \end{aligned}$$

is invertible, and we denote its inverse by $(\mathcal{P}_T\mathcal{P}_\Omega\mathcal{P}_T)^{-1} : T \to T$. Introduce the dual matrix $Y \in \mathcal{P}_\Omega(\mathbb{R}^{n\times n}) \subset \mathbb{R}^{n\times n}$ defined via

$$Y = \mathcal{P}_\Omega \mathcal{P}_T (\mathcal{P}_T \mathcal{P}_\Omega \mathcal{P}_T)^{-1} E. \tag{III.10}$$

By construction, $\mathcal{P}_\Omega(Y) = Y$, $\mathcal{P}_T(Y) = E$, and, therefore, we will establish that M is the unique minimizer if one can show that

$$\|\mathcal{P}_{T^\perp}(Y)\| < 1. \tag{III.11}$$

The dual matrix Y would then certify that M is the unique solution, and this is the reason why we will refer to Y as a *candidate certificate*. This certificate was also used in [7].

Before continuing, we would like to offer a little motivation for the choice of the dual matrix Y. It is not difficult to check that (III.10) is actually the solution to the following problem:

$$\begin{aligned} \text{minimize} \quad & \|Z\|_F \\ \text{subject to} \quad & \mathcal{P}_T \mathcal{P}_\Omega(Z) = E. \end{aligned}$$

Note that by the Pythagorean identity, Y obeys

$$\|Y\|_F^2 = \|\mathcal{P}_T(Y)\|_F^2 + \|\mathcal{P}_{T^\perp}(Y)\|_F^2 = r + \|\mathcal{P}_{T^\perp}(Y)\|_F^2.$$

The interpretation is now clear: among all matrices obeying $\mathcal{P}_\Omega(Z) = Z$ and $\mathcal{P}_T(Z) = E$, Y is that element which minimizes $\|\mathcal{P}_{T^\perp}(Z)\|_F$. By forcing the Frobenius norm of $\mathcal{P}_{T^\perp}(Y)$ to be small, it is reasonable to expect that its spectral norm will be sufficiently small, as well. In that sense, Y defined via (III.10) is a very suitable candidate.

Even though this is a different problem, our candidate certificate resembles—and is inspired by—that constructed in [8] to show that ℓ_1 minimization recovers sparse vectors from minimally sampled data.

C. Neumann Series

We now develop a useful formula for the candidate certificate, and begin by introducing a normalized version $\mathcal{Q}_\Omega : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n}$ of $\mathcal{P}_\Omega$, defined by the formula

$$\mathcal{Q}_\Omega := \frac{1}{p}\mathcal{P}_\Omega - \mathcal{I} \tag{III.12}$$

where $\mathcal{I} : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n}$ is the identity operator on matrices (*not* the identity matrix $I \in \mathbb{R}^{n\times n}$!). Note that with the Bernoulli model for selecting Ω, that $\mathcal{Q}_\Omega$ has expectation zero.

From (III.12) we have $\mathcal{P}_T\mathcal{P}_\Omega\mathcal{P}_T = p\mathcal{P}_T(\mathcal{I} + \mathcal{Q}_\Omega)\mathcal{P}_T$, and owing to Theorem 3.2, one can write $(\mathcal{P}_T\mathcal{P}_\Omega\mathcal{P}_T)^{-1}$ as the convergent Neumann series

$$p(\mathcal{P}_T\mathcal{P}_\Omega\mathcal{P}_T)^{-1} = \sum_{k\geq 0}(-1)^k(\mathcal{P}_T\mathcal{Q}_\Omega\mathcal{P}_T)^k.$$

From the identity $\mathcal{P}_{T^\perp}\mathcal{P}_T = 0$, we conclude that $\mathcal{P}_{T^\perp}\mathcal{P}_\Omega\mathcal{P}_T = p(\mathcal{P}_{T^\perp}\mathcal{Q}_\Omega\mathcal{P}_T)$. One can, therefore, express the candidate certificate Y (III.10) as

$$\begin{aligned} \mathcal{P}_{T^\perp}(Y) &= \sum_{k\geq 0}(-1)^k \mathcal{P}_{T^\perp}\mathcal{Q}_\Omega(\mathcal{P}_T\mathcal{Q}_\Omega\mathcal{P}_T)^k(E) \\ &= \sum_{k\geq 0}(-1)^k \mathcal{P}_{T^\perp}(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E) \end{aligned}$$

where we have used $\mathcal{P}_T^2 = \mathcal{P}_T$ and $\mathcal{P}_T(E) = E$. By the triangle inequality and (III.5), it thus suffices to show that

$$\sum_{k\geq 0}\left\|(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E)\right\| < 1$$

with probability at least $1 - n^{-3}/2$.

It is not hard to bound the tail of the series thanks to Theorem 3.2. First, this theorem bounds the spectral norm of $\mathcal{P}_T\mathcal{Q}_\Omega\mathcal{P}_T$ by the quantity a in (III.7). This gives that for each $k \geq 1$, $\left\|(\mathcal{P}_T\mathcal{Q}_\Omega\mathcal{P}_T)^k(E)\right\|_F < a^k\|E\|_F = a^k\sqrt{r}$ and, therefore

$$\begin{aligned} \left\|(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E)\right\|_F &= \|\mathcal{Q}_\Omega\mathcal{P}_T(\mathcal{P}_T\mathcal{Q}_\Omega\mathcal{P}_T)^k(E)\|_F \\ &\leq \|\mathcal{Q}_\Omega\mathcal{P}_T\|a^k\sqrt{r}. \end{aligned}$$

Second, this theorem also bounds $\|\mathcal{Q}_\Omega\mathcal{P}_T\|$ (recall that this is the spectral norm) since

$$\begin{aligned} \|\mathcal{Q}_\Omega\mathcal{P}_T\|^2 &= \max_{\|X\|_F\leq 1}\langle \mathcal{Q}_\Omega\mathcal{P}_T(X), \mathcal{Q}_\Omega\mathcal{P}_T(X)\rangle \\ &= \langle X, \mathcal{P}_T\mathcal{Q}_\Omega^2\mathcal{P}_T(X)\rangle. \end{aligned}$$

Expanding the identity $\mathcal{P}_\Omega^2 = \mathcal{P}_\Omega$ in terms of $\mathcal{Q}_\Omega$, we obtain

$$\mathcal{Q}_\Omega^2 = \frac{1}{p}[(1-2p)\mathcal{Q}_\Omega + (1-p)\mathcal{I}] \tag{III.13}$$

and, thus, for all $\|X\|_F \leq 1$

$$\begin{aligned} p\langle X, \mathcal{P}_T\mathcal{Q}_\Omega^2\mathcal{P}_T(X)\rangle &= (1-2p)\langle X, \mathcal{P}_T\mathcal{Q}_\Omega\mathcal{P}_T(X)\rangle \\ &\quad + (1-p)\|\mathcal{P}_T(X)\|_F^2 \\ &\leq a+1. \end{aligned}$$

Hence, $\|\mathcal{Q}_\Omega\mathcal{P}_T\| \leq \sqrt{(a+1)/p}$. For each $k_0 \geq 0$, this gives

$$\sum_{k\geq k_0} \left\|(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E)\right\|_F \leq \sqrt{\frac{3r}{2p}} \sum_{k\geq k_0} a^k \leq \sqrt{\frac{6r}{p}}a^{k_0}$$

provided that $a < 1/2$. With $p = m/n^2$ and a defined by (III.7) with $\beta = 4$, we have

$$\sum_{k\geq k_0} \left\|(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E)\right\|_F \leq \sqrt{n} \times O\left(\frac{\mu_0 nr\log n}{m}\right)^{\frac{k_0+1}{2}}$$

with probability at least $1-n^{-4}$. When $k_0+1 \geq \log n$, $n^{\frac{1}{k_0+1}} \leq n^{\frac{1}{\log n}} = e$, and thus for each such a k_0

$$\sum_{k\geq k_0} \left\|(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E)\right\|_F \leq O\left(\frac{\mu_0 nr\log n}{m}\right)^{\frac{k_0+1}{2}} \quad \text{(III.14)}$$

with the same probability.

To summarize this section, we conclude that since both our results assume that $m \geq c_0\mu_0 nr\log n$ for some sufficiently large numerical constant c_0 (see the discussion at the end of Section III-A), it now suffices to show that

$$\sum_{k=0}^{\lfloor \log n\rfloor} \left\|(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega E\right\| \leq \frac{1}{2} \quad \text{(III.15)}$$

(say) with probability at least $1-n^{-3}/4$.

D. Centering

We have already normalized $\mathcal{P}_\Omega$ to have "mean zero" in some sense by replacing it with $\mathcal{Q}_\Omega$. Now we perform a similar operation for the projection $\mathcal{P}_T : X \mapsto P_U X + XP_V - P_U X P_V$. The eigenvalues of $\mathcal{P}_T$ are centered around

$$\rho' := \text{trace}(\mathcal{P}_T)/n^2 = 2\rho - \rho^2, \quad \rho := r/n \quad \text{(III.16)}$$

which follows from the fact that $\mathcal{P}_T$ is an orthogonal projection onto a space of dimension $2nr-r^2$. Therefore, we simply split $\mathcal{P}_T$ as

$$\mathcal{P}_T = \mathcal{Q}_T + \rho'\mathcal{I} \quad \text{(III.17)}$$

so that the eigenvalues of $\mathcal{Q}_T$ are centered around zero. From now on, ρ and ρ' will always be the numbers defined above.

Lemma 3.3 (Replacing $\mathcal{P}_T$ With $\mathcal{Q}_T$): Let $0 < \sigma < 1$. Consider the event

$$\left\|(\mathcal{Q}_\Omega\mathcal{Q}_T)^k\mathcal{Q}_\Omega(E)\right\| \leq \sigma^{\frac{k+1}{2}}, \quad \text{for all } 0 \leq k < k_0. \quad \text{(III.18)}$$

Then on this event, we have that for all $0 \leq k < k_0$,

$$\left\|(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E)\right\| \leq (1+4^{k+1})\,\sigma^{\frac{k+1}{2}} \quad \text{(III.19)}$$

provided that $8nr/m < \sigma^{3/2}$.

From (III.19) and the geometric series formula, we obtain the corollary

$$\sum_{k=0}^{k_0-1} \left\|(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E)\right\| \leq 5\sqrt{\sigma}\frac{1}{1-4\sqrt{\sigma}}. \quad \text{(III.20)}$$

Let σ_0 be such that the right-hand side is less than 1/4, say. Applying this with $\sigma = \sigma_0$, we conclude that to prove (III.15) with probability at least $1-n^{-3}/4$, it suffices by the union bound to show that (III.18) holds for this value of σ (note that the hypothesis $8nr/m < \sigma^{3/2}$ follows from the hypotheses in either Theorem 1.1 or Theorem 1.2).

Lemma 3.3, which is proven in the Appendix, is useful because the operator $\mathcal{Q}_T$ is easier to work with than $\mathcal{P}_T$ in the sense that it is more homogeneous, and obeys better estimates. If we split the projections P_U, P_V as

$$P_U = \rho I + Q_U, \quad P_V = \rho I + Q_V \quad \text{(III.21)}$$

then $\mathcal{Q}_T$ obeys

$$\mathcal{Q}_T(X) = (1-\rho)Q_U X + (1-\rho)XQ_V - Q_U X Q_V.$$

Let $U_{a,a'}$, $V_{b,b'}$ denote the matrix elements of Q_U, Q_V

$$U_{a,a'} := \langle e_a, Q_U e_{a'}\rangle = \langle e_a, P_U e_{a'}\rangle - \rho 1_{a=a'} \quad \text{(III.22)}$$

and similarly for $V_{b,b'}$. The coefficients $c_{ab,a'b'}$ of $\mathcal{Q}_T$ obey

$$\begin{aligned} c_{ab,a'b'} &:= \langle e_a e_b^*, \mathcal{Q}_T\rangle(e_{a'}e_{b'}^*) \\ &= (1-\rho)1_{b=b'}U_{a,a'} + (1-\rho)1_{a=a'}V_{b,b'} \\ &\quad - U_{a,a'}V_{b,b'}. \end{aligned} \quad \text{(III.23)}$$

An immediate consequence of this, under the assumptions (I.8), is the estimate

$$|c_{ab,a'b'}| \lesssim (1_{a=a'} + 1_{b=b'})\frac{\mu\sqrt{r}}{n} + \frac{\mu^2 r}{n^2}. \quad \text{(III.24)}$$

When $\mu = O(1)$, these coefficients are bounded by $O(\sqrt{r}/n)$ when $a = a'$ or $b = b'$ while in contrast, if we stayed with $\mathcal{P}_T$ rather than $\mathcal{Q}_T$, the diagonal coefficients would be as large as r/n. However, our lemma states that bounding $\left\|(\mathcal{Q}_\Omega\mathcal{Q}_T)^k\mathcal{Q}_\Omega(E)\right\|$ automatically bounds $\left\|(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E)\right\|$ by nearly the same quantity. This is the main advantage of replacing $\mathcal{P}_T$ by $\mathcal{Q}_T$ in our analysis.

E. Key Estimates

To summarize the previous discussion, and in particular the bounds (III.20) and (III.14), we see that everything reduces to bounding the spectral norm of $(\mathcal{Q}_\Omega\mathcal{Q}_T)^k\mathcal{Q}_\Omega(E)$ for $k = 0, 1, \ldots, \lfloor \log n\rfloor$. Providing good upper bounds on these quantities is the crux of the argument. We use the moment

method, controlling a spectral norm of a matrix by the trace of a high power of that matrix. We will prove two moment estimates which ultimately imply our two main results (Theorems 1.1 and 1.2), respectively. The first such estimate is as follows:

Theorem 3.4 (Moment Bound I): For a fixed $k \geq 0$, set $A = (\mathcal{Q}_\Omega \mathcal{Q}_T)^k \mathcal{Q}_\Omega(E)$. Under the assumptions of Theorem 1.1, we have that for each $j > 0$

$$\mathbb{E}\left[\operatorname{trace}(A^*A)^j\right] = O\big(j(k+1)\big)^{2j(k+1)} n\Big(\frac{nr_\mu^2}{m}\Big)^{j(k+1)}$$
$$r_\mu := \mu^2 r \tag{III.25}$$

provided that $m \geq nr_\mu^2$ and $n \geq c_0 j(k+1)$ for some numerical constant c_0.

By Markov's inequality, this result automatically estimates the norm of $(\mathcal{Q}_\Omega \mathcal{Q}_T)^k \mathcal{Q}_\Omega(E)$ and immediately gives the following corollary.

Corollary 3.5 (Existence of Dual Certificate I): Under the assumptions of Theorem 1.1, the matrix Y (III.10) is a dual certificate, and obeys $\|\mathcal{P}_{T^\perp}(Y)\| \leq 1/2$ with probability at least $1 - n^{-3}$ provided that m obeys (I.10).

Proof: Set $A = (\mathcal{Q}_\Omega \mathcal{Q}_T)^k \mathcal{Q}_\Omega(E)$ with $k \leq \log n$, and set $\sigma \leq \sigma_0$. By Markov's inequality

$$\mathbb{P}(\|A\| \geq \sigma^{\frac{k+1}{2}}) \leq \frac{\mathbb{E}\|A\|^{2j}}{\sigma^{j(k+1)}}$$

Now choose $j > 0$ to be the smallest integer such that $j(k+1) \geq \log n$. Since

$$\|A\|^{2j} \leq \operatorname{trace}(A^*A)^j$$

Theorem 3.4 gives

$$\mathbb{P}\left(\|A\| \geq \sigma^{\frac{k+1}{2}}\right) \leq \gamma^{j(k+1)}$$

for some

$$\gamma = O\left(\frac{(j(k+1))^2 nr_\mu^2}{\sigma m}\right)$$

where we have used the fact that $n^{\frac{1}{j(k+1)}} \leq n^{\frac{1}{\log n}} = e$. Hence, if

$$m \geq C_0 \frac{nr_\mu^2 (\log n)^2}{\sigma} \tag{III.26}$$

for some numerical constant C_0, we have $\gamma < 1/4$ and

$$\mathbb{P}\left(\left\|(\mathcal{Q}_\Omega \mathcal{Q}_T)^k \mathcal{Q}_\Omega(E)\right\| \geq \sigma^{\frac{k+1}{2}}\right) \leq n^{-4}.$$

Therefore

$$\bigcup_{0 \leq k < \log n} \left\{\left\|(\mathcal{Q}_\Omega \mathcal{Q}_T)^k \mathcal{Q}_\Omega(E)\right\| \geq \sigma^{\frac{k+1}{2}}\right\}$$

has probability less than or equal to $n^{-4} \log n \leq n^{-3}/2$ for $n \geq 2$. Since the corollary assumes $r = O(1)$, then (III.26) together with (III.20) and (III.14) proves the claim thanks to our choice of σ. ∎

Of course, Theorem 1.1 follows immediately from Corollary 3.5 and Lemma 3.1. In the same way, our second result (Theorem 1.2) follows from a more refined estimate stated below.

Theorem 3.6 (Moment Bound II): For a fixed $k \geq 0$, set $A = (\mathcal{Q}_\Omega \mathcal{Q}_T)^k \mathcal{Q}_\Omega(E)$. Under the assumptions of Theorem 1.2, we have that for each $j > 0$ [r_μ is given in (III.25)]

$$\mathbb{E}\big[\operatorname{trace}(A^*A)^j\big] \leq \Big(\frac{(j(k+1))^6 nr_\mu}{m}\Big)^{j(k+1)} \tag{III.27}$$

provided that $n \geq c_0 j(k+1)$ for some numerical constant c_0.

Just as before, this theorem immediately implies the following corollary.

Corollary 3.7 (Existence of Dual Certificate II): Under the assumptions of Theorem 1.2, the matrix Y (III.10) is a dual certificate, and obeys $\|\mathcal{P}_{T^\perp}(Y)\| \leq 1/2$ with probability at least $1 - n^{-3}$ provided that m obeys (I.12).

The proof is identical to that of Corollary 3.5 and is omitted. Again, Corollary 3.7 and Lemma 3.1 immediately imply Theorem 1.2.

We have learned that verifying that Y is a valid dual certificate reduces to (III.25) and (III.27), and we conclude this section by giving a road map to the proofs. In Section IV, we will develop a formula for $\mathbb{E}\operatorname{trace}(A^*A)^j$, which is our starting point for bounding this quantity. Then Section V develops the first and perhaps easier bound (III.25) while Section VI refines the argument by exploiting clever cancellations, and establishes the nearly optimal bound (III.27).

F. Novelty

As explained earlier, this paper derives near-optimal sampling results which are stronger than those in [7]. One of the reasons underlying this improvement is that we use completely different techniques. In detail, [7] constructs the dual certificate (III.10) and proceeds by showing that $\|\mathcal{P}_{T^\perp}(Y)\| < 1$ by bounding each term in the series $\sum_{k \geq 0} \left\|(\mathcal{Q}_\Omega \mathcal{P}_T)^k \mathcal{Q}_\Omega(E)\right\| < 1$. Further, to prove that the early terms (small values of k) are appropriately small, the authors employ a sophisticated array of tools from asymptotic geometric analysis, including noncommutative Khintchine inequalities [17], decoupling techniques of Bourgain and Tzafiri and of de la Peña [10], and large deviations inequalities [15]. They bound each term individually up to $k = 4$ and use the same argument as that in Section III-C to bound the rest of the series. Since the tail starts at $k_0 = 5$, this gives that a sufficient condition is that the number of samples exceeds a constant times $\mu_0 n^{6/5} nr \log n$. Bounding each term $\|(\mathcal{Q}_\Omega \mathcal{P}_T)^k \mathcal{Q}_\Omega(E)\|$ with the tools put forth in [7] for larger values of k becomes increasingly delicate because of the coupling between the indicator variables defining the random set Ω. In addition, the noncommutative Khintchine inequality seems less effective in higher dimensions; that is, for large values of k. Informally speaking, the reason for this seems to be that the types of

random sums that appear in the moments $(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E)$ for large k involve complicated combinations of the coefficients of $\mathcal{P}_T$ that are not simply components of some product matrix, and which do not simplify substantially after a direct application of the Khintchine inequality.

In this paper, we use a very different strategy to estimate the spectral norm of $(\mathcal{Q}_\Omega\mathcal{Q}_T)^k\mathcal{Q}_\Omega(E)$, and employ moment methods, which have a long history in random matrix theory, dating back at least to the classical work of Wigner [27]. We raise the matrix $A := (\mathcal{Q}_\Omega\mathcal{Q}_T)^k\mathcal{Q}_\Omega(E)$ to a large power j so that

$$\sigma_1^{2j}(A) = \|A\|^{2j} \approx \mathrm{trace}(A^*A)^j = \sum_{i\in[n]} \sigma_i^{2j}(A)$$

(the largest element dominates the sum). We then need to compute the expectation of the right-hand side, and reduce matters to a purely combinatorial question involving the statistics of various types of paths in a plane. It is rather remarkable that carrying out these combinatorial calculations nearly give the quantitatively correct answer; the moment method seems to come close to giving the ultimate limit of performance one can expect from nuclear-norm minimization.

As we shall shortly see, the expression $\mathrm{trace}(A^*A)^j$ expands as a sum over "paths" of products of various coefficients of the operators $\mathcal{Q}_\Omega$, $\mathcal{Q}_T$ and the matrix E. These paths can be viewed as complicated variants of Dyck paths. However, it does not seem that one can simply invoke standard moment method calculations in the literature to compute this sum, as in order to obtain efficient bounds, we will need to take full advantage of identities such as $\mathcal{P}_T\mathcal{P}_T = \mathcal{P}_T$ (which capture certain cancellation properties of the coefficients of $\mathcal{P}_T$ or $\mathcal{Q}_T$) to simplify various components of this sum. It is only after performing such simplifications that one can afford to estimate all the coefficients by absolute values and count paths to conclude the argument.

IV. Moments

Let $j \geq 0$ be a fixed integer. The goal of this section is to develop a formula for

$$X := \mathbb{E}\mathrm{trace}(A^*A)^j. \tag{IV.1}$$

This will clearly be of use in the proofs of the moment bounds (Theorems 3.4, 3.6).

A. First Step: Expansion

We first write the matrix A in components as

$$A = \sum_{a,b\in[n]} A_{ab}e_{ab}$$

for some scalars A_{ab}, where e_{ab} is the standard basis for the $n \times n$ matrices and A_{ab} is the (a,b)th entry of A. Then

$$\mathrm{trace}(A^*A)^j = \sum_{\substack{a_1,\ldots,a_j\in[n]\\ b_1,\ldots,b_j\in[n]}} \prod_{i\in[j]} A_{a_ib_i}A_{a_{i+1}b_i}$$

where we adopt the cyclic convention $a_{j+1} = a_1$. Equivalently, we can write

$$\mathrm{trace}(A^*A)^j = \sum \prod_{i\in[j]}\prod_{\mu=0}^{1} A_{a_{i,\mu}b_{i,\mu}} \tag{IV.2}$$

where the sum is over all $a_{i,\mu}, b_{i,\mu} \in [n]$ for $i \in [j], \mu \in \{0,1\}$ obeying the compatibility conditions

$$a_{i,1} = a_{i+1,0}; \quad b_{i,1} = b_{i,0} \text{ for all } i \in [j]$$

with the cyclic convention $a_{j+1,0} = a_{1,0}$.

Example. If $j = 2$, then we can write $\mathrm{trace}(A^*A)^j$ as

$$\sum_{a_1,a_2,b_1,b_2\in[n]} A_{a_1b_1}A_{a_2b_1}A_{a_2b_2}A_{a_1b_2}$$

or equivalently as

$$\sum\prod_{i=1}^{2}\prod_{\mu=0}^{1} A_{a_{i,\mu},b_{i,\mu}}$$

where the sum is over all $a_{1,0}, a_{1,1}, a_{2,0}, a_{2,1}, b_{1,0}, b_{1,1}, b_{2,0}, b_{2,1} \in [n]$ obeying the compatibility conditions

$$a_{1,1} = a_{2,0}; \quad a_{2,1} = a_{1,0}; \quad b_{1,1} = b_{1,0}; \quad b_{2,1} = b_{2,0}.$$

Remark. The sum in (IV.2) can be viewed being taken over all closed paths of length $2j$ in $[n] \times [n]$, where the edges of the paths alternate between "horizontal rook moves" and "vertical rook moves" respectively; see Fig. 1.

Second, write $\mathcal{Q}_T$ and $\mathcal{Q}_\Omega$ in coefficients as

$$\mathcal{Q}_T(e_{a'b'}) = \sum_{ab} c_{ab,a'b'}e_{ab}$$

where $c_{ab,a'b'}$ is given by (III.23), and

$$\mathcal{Q}_\Omega(e_{a'b'}) = \xi_{a'b'}e_{a'b'}$$

where ξ_{ab} are the iid, zero-expectation random variables

$$\xi_{ab} := \frac{1}{p}1_{(a,b)\in\Omega} - 1.$$

With this, we have

$$A_{a_0,b_0} := \sum_{a_1,b_1,\ldots,a_k,b_k\in[n]} \left(\prod_{l\in[k]} c_{a_{l-1}b_{l-1},a_lb_l}\right) \times \left(\prod_{l=0}^{k}\xi_{a_lb_l}\right) E_{a_kb_k} \tag{IV.3}$$

for any $a_0, b_0 \in [n]$. Note that this formula is even valid in the base case $k = 0$, where it simplifies to just $A_{a_0b_0} = \xi_{a_0b_0}E_{a_0b_0}$ due to our conventions on trivial sums and empty products.

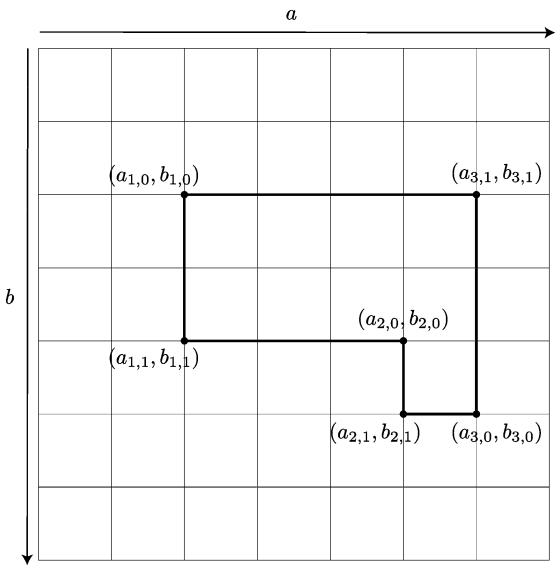

Fig. 1. Typical path in $[n] \times [n]$ that appears in the expansion of $\mathrm{trace}(A^* A)^j$, here with $j = 3$.

Example. If $k = 2$, then

$$A_{a_0,b_0} = \sum_{a_1,a_2,b_1,b_2 \in [n]} \xi_{a_0 b_0} c_{a_0 b_0, a_1, b_1} \times \xi_{a_1 b_1} c_{a_1 b_1, a_2 b_2} \xi_{a_2 b_2} E_{a_2 b_2}.$$

Remark. One can view the right-hand side of (IV.3) as the sum over paths of length $k+1$ in $[n] \times [n]$ starting at the designated point (a_0, b_0) and ending at some arbitrary point (a_k, b_k). Each edge (from (a_i, b_i) to (a_{i+1}, b_{i+1})) may be a horizontal or vertical "rook move" (in that at least one of the a or b coordinates does not change[3]), or a "non-rook move" in which both the a and b coordinates change. It will be important later on to keep track of which edges are rook moves and which ones are not, basically because of the presence of the delta functions $1_{a=a'}$, $1_{b=b'}$ in (III.23). Each edge in this path is weighted by a c factor, and each vertex in the path is weighted by a ξ factor, with the final vertex also weighted by an additional E factor. It is important to note that the path is allowed to cross itself, in which case weights such as ξ^2, ξ^3, etc. may appear, see Fig. 2.

Inserting (IV.3) into (IV.2), we see that X can thus be expanded as

$$\mathbb{E} \sum_{*} \prod_{i \in [j]} \prod_{\mu=0}^{1} \left[\left(\prod_{l \in [k]} c_{a_{i,\mu,l-1} b_{i,\mu,l-1}, a_{i,\mu,l} b_{i,\mu,l}} \right) \cdot \left(\prod_{l=0}^{k} \xi_{a_{i,\mu,l} b_{i,\mu,l}} \right) E_{a_{i,\mu,k} b_{i,\mu,k}} \right] \quad \text{(IV.4)}$$

where the sum $\sum_*$ is over all combinations of $a_{i,\mu,l}, b_{i,\mu,l} \in [n]$ for $i \in [j]$, $\mu \in \{0,1\}$ and $0 \le l \le k$ obeying the compatibility conditions

$$a_{i,1,0} = a_{i+1,0,0}; \quad b_{i,1,0} = b_{i,0,0} \text{ for all } i \in [j] \quad \text{(IV.5)}$$

[3]Unlike the ordinary rules of chess, we will consider the trivial move when $a_{i+1} = a_i$ and $b_{i+1} = b_i$ to also qualify as a "rook move", which is simultaneously a horizontal and a vertical rook move.

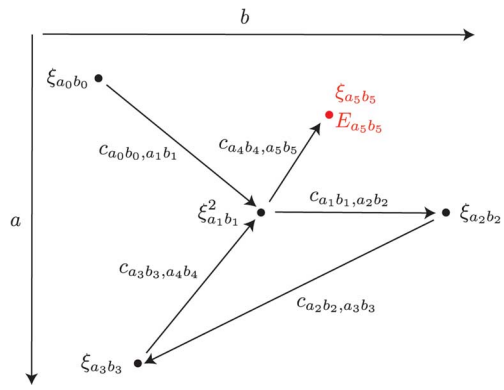

Fig. 2. Typical path appearing in the expansion (IV.3) of $A_{a_0 b_0}$, here with $k = 5$. Each vertex of the path gives rise to a ξ factor (with the final vertex, coloured in red, providing an additional E factor), while each edge of the path provides a c factor. Note that the path is certainly allowed to cross itself (leading to the ξ factors being raised to powers greater than 1, as is for instance the case here at $(a_1, b_1) = (a_4, b_4)$), and that the edges of the path may be horizontal, vertical, or neither.

with the cyclic convention $a_{j+1,0,0} = a_{1,0,0}$.

Example. Continuing our running example $j = k = 2$, we have

$$X = \mathbb{E} \sum_{*} \prod_{i=1}^{2} \prod_{\mu=0}^{1} \Big(\xi_{a_{i,\mu,0} b_{i,\mu,0}} c_{a_{i,\mu,0} b_{i,\mu,0}, a_{i,\mu,1} b_{i,\mu,1}} \cdot \xi_{a_{i,\mu,1} b_{i,\mu,1}} c_{a_{i,\mu,1} b_{i,\mu,1}, a_{i,\mu,2} b_{i,\mu,2}} \xi_{a_{i,\mu,2} b_{i,\mu,2}} E_{a_{i,\mu,2} b_{i,\mu,2}} \Big)$$

where $a_{i,\mu,l}$ for $i = 1, 2$, $\mu = 0, 1$, $l = 0, 1, 2$ obey the compatibility conditions

$$a_{1,1,0} = a_{2,0,0}; \quad a_{2,1,0} = a_{1,0,0}$$
$$b_{1,1,0} = b_{1,0,0}; \quad b_{2,1,0} = b_{2,0,0}.$$

Note that despite the small values of j and k, this is already a rather complicated sum, ranging over $n^{2j(k+1)} = n^{12}$ summands, each of which is the product of $4j(k+1) = 24$ terms.

Remark. The expansion (IV.4) is the sum over a sort of combinatorial "spider", whose "body" is a closed path of length $2j$ in $[n] \times [n]$ of alternating horizontal and vertical rook moves, and whose $2j$ "legs" are paths of length k, emanating out of each vertex of the body. The various "segments" of the legs (which can be either rook or non-rook moves) acquire a weight of c, and the "joints" of the legs acquire a weight of ξ, with an additional weight of E at the tip of each leg. To complicate things further, it is certainly possible for a vertex of one leg to overlap with another vertex from either the same leg or a different leg, introducing weights such as ξ^2, ξ^3, etc.; see Fig. 3. As one can see, the set of possible configurations that this "spider" can be in is rather large and complicated.

B. Second Step: Collecting Rows and Columns

We now group the terms in the expansion (IV.4) into a bounded number of components, depending on how the various horizontal coordinates $a_{i,\mu,l}$ and vertical coordinates $b_{i,\mu,l}$ overlap.

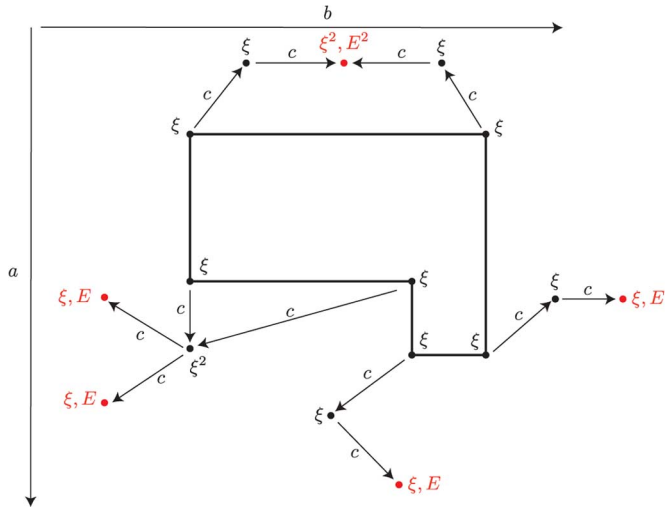

Fig. 3. "Spider" with $j = 3$ and $k = 2$, with the "body" in boldface lines and the "legs" as directed paths from the body to the tips (marked in red).

It is convenient to order the $2j(k+1)$ tuples $(i,\mu,l) \in [j] \times \{0,1\} \times \{0,\ldots,k\}$ lexicographically by declaring $(i,\mu,l) < (i',\mu',l')$ if $i < i'$, or if $i = i'$ and $\mu < \mu'$, or if $i = i'$ and $\mu = \mu'$ and $l < l'$.

We then define the indices $s_{i,\mu,l}, t_{i,\mu,l} \in \{1,2,3,\ldots\}$ recursively for all $(i,\mu,l) \in [j]\times\{0,1\}\times[k]$ by setting $s_{1,0,0} = 1$ and declaring $s_{i,\mu,l} := s_{i',\mu',l'}$ if there exists $(i',\mu',l') < (i,\mu,l)$ with $a_{i',\mu',l'} = a_{i,\mu,l}$, or equal to the first positive integer not equal to any of the $s_{i',\mu',l'}$ for $(i',\mu',l') < (i,\mu,l)$ otherwise. Define $t_{i,\mu,l}$ using $b_{i,\mu,l}$ similarly. We observe the *cyclic condition*

$$s_{i,1,0} = s_{i+1,0,0}; \quad t_{i,1,0} = t_{i,0,0} \ \text{ for all } \ i \in [j] \tag{IV.6}$$

with the cyclic convention $s_{j+1,0,0} = s_{1,0,0}$.

Example. Suppose that $j = 2$, $k = 1$, and $n \geq 30$, with the $(a_{i,\mu,l}, b_{i,\mu,l})$ given in lexicographical ordering as

$$\begin{aligned}
(a_{1,0,0}, b_{0,0,0}) &= (17,30)\\
(a_{1,0,1}, b_{0,0,1}) &= (13,27)\\
(a_{1,1,0}, b_{0,1,0}) &= (28,30)\\
(a_{1,1,1}, b_{0,1,1}) &= (13,25)\\
(a_{2,0,0}, b_{1,0,0}) &= (28,11)\\
(a_{2,0,1}, b_{1,0,1}) &= (17,27)\\
(a_{2,1,0}, b_{1,1,0}) &= (17,11)\\
(a_{2,1,1}, b_{1,1,1}) &= (13,27).
\end{aligned}$$

Then we would have

$$\begin{aligned}
(s_{1,0,0}, t_{0,0,0}) &= (1,1)\\
(s_{1,0,1}, t_{0,0,1}) &= (2,2)\\
(s_{1,1,0}, t_{0,1,0}) &= (3,1)\\
(s_{1,1,1}, t_{0,1,1}) &= (2,3)\\
(s_{2,0,0}, t_{1,0,0}) &= (3,4)\\
(s_{2,0,1}, t_{1,0,1}) &= (1,2)\\
(s_{2,1,0}, t_{1,1,0}) &= (1,4)\\
(s_{2,1,1}, t_{1,1,1}) &= (2,2).
\end{aligned}$$

Observe that the conditions (IV.5) hold for this example, which then forces (IV.6) to hold also.

In addition to the property (IV.6), we see from construction of (s,t) that for any $(i,\mu,l) \in [j]\times\{0,1\}\times\{0,\ldots,k\}$, the sets

$$\begin{aligned}
&\{s(i',\mu',l') : (i',\mu',l') \leq (i,\mu,l)\}\\
&\{t(i',\mu',l') : (i',\mu',l') \leq (i,\mu,l)\}
\end{aligned} \tag{IV.7}$$

are initial segments, i.e., of the form $[m]$ for some integer m. Let us call pairs (s,t) of sequences with this property, as well as the property (IV.6), *admissible*; thus, for instance, the sequences in the above example are admissible. Given an admissible pair (s,t), if we define the sets J, K by

$$\begin{aligned}
J &:= \{s_{i,\mu,l} : (i,\mu,l) \in [j] \times \{0,1\} \times \{0,\ldots,k\}\}\\
K &:= \{t_{i,\mu,l} : (i,\mu,l) \in [j] \times \{0,1\} \times \{0,\ldots,k\}\}
\end{aligned} \tag{IV.8}$$

then we observe that $J = [|J|]$, $K = [|K|]$. Also, if (s,t) arose from $a_{i,\mu,l}$, $b_{i,\mu,l}$ in the above manner, there exist unique injections $\alpha : J \to [n]$, $\beta : K \to [n]$ such that $a_{i,\mu,l} = \alpha(s_{i,\mu,l})$ and $b_{i,\mu,l} = \beta(t_{i,\mu,l})$.

Example. Continuing the previous example, we have $J = [3]$, $K = [4]$, with the injections $\alpha : [3] \to [n]$ and $\beta : [4] \to [n]$ defined by

$$\begin{aligned}
&\alpha(1) := 17; \quad \alpha(2) := 13; \quad \alpha(3) := 28\\
&\qquad\qquad \text{and}\\
&\beta(1) := 30; \quad \beta(2) := 27; \quad \beta(3) := 25; \quad \beta(4) := 11.
\end{aligned}$$

Conversely, any admissible pair (s,t) and injections α, β determine $a_{i,\mu,l}$ and $b_{i,\mu,l}$. Because of this, we can thus expand X as shown in the equation at the bottom of the page, where the outer sum is over all admissible pairs (s,t), and the inner sum is over all injections.

$$X = \sum_{(s,t)\text{admissible}} \mathbb{E} \sum_{\alpha,\beta} \prod_{i\in[j]} \prod_{\mu=0}^{1} \left[\left(\prod_{l\in[k]} c_{\alpha(s_{i,\mu,l-1})\beta(t_{i,\mu,l-1}),\alpha(s_{i,\mu,l})\beta(t_{i,\mu,l})} \right) \cdot \left(\prod_{l=0}^{k} \xi_{\alpha(s_{i,\mu,l})\beta(t_{i,\mu,l})} \right) E_{\alpha(s_{i,\mu,k})\beta(t_{i,\mu,k})} \right]$$

Remark. As with the preceding identities, the above formula is also valid when $k = 0$ (with our conventions on trivial sums and empty products), in which case it simplifies to

$$X = \sum_{(s,t)\text{admissible}} \mathbb{E} \sum_{\alpha,\beta} \prod_{i\in[j]} \prod_{\mu=0}^{1} \xi_{\alpha(s_{i,\mu,0})\beta(t_{i,\mu,0})} \times E_{\alpha(s_{i,\mu,0})\beta(t_{i,\mu,0})}.$$

Remark. One can think of (s,t) as describing the combinatorial "configuration" of the "spider" $((a_{i,\mu,l}, b_{i,\mu,l}))_{(i,\mu,l)\in[j]\times\{0,1\}\times\{0,\ldots,k\}}$—it determines which vertices of the spider are equal to, or on the same row or column as, other vertices of the spider. The injections α, β then enumerate the ways in which such a configuration can be "represented" inside the grid $[n] \times [n]$.

C. Third Step: Computing the Expectation

The expansion we have for X looks quite complicated. However, the fact that the ξ_{ab} are independent and have mean zero allows us to simplify this expansion to a significant degree. Indeed, observe that the random variable $\Xi := \prod_{i\in[j]} \prod_{\mu=0}^{1} \prod_{l=0}^{k} \xi_{\alpha(s_{i,\mu,l})\beta(t_{i,\mu,l})}$ has zero expectation if there is any pair in $J \times K$ which can be expressed exactly once in the form $(s_{i,\mu,l}, t_{i,\mu,l})$. Thus, we may assume that no pair can be expressed exactly once in this manner. If δ is a Bernoulli variable with $\mathbb{P}(\delta = 1) = p = 1 - \mathbb{P}(\delta = 0)$, then for each $s \geq 0$, one easily computes

$$\mathbb{E}(\delta - p)^s = p(1-p)\left[(1-p)^{s-1} + (-1)^s p^{s-1}\right]$$

and hence

$$\left|\mathbb{E}\left(\frac{1}{p}\delta - 1\right)^s\right| \leq p^{1-s}.$$

The value of the expectation of Ξ does not depend on the choice of α or β, and the calculation above shows that Ξ obeys

$$|\mathbb{E}\Xi| \leq \frac{1}{p^{2j(k+1)-|\Omega|}}$$

where

$$\Omega := \{(s_{i,\mu,l}, t_{i,\mu,l}) : (i,\mu,l) \in [j] \times \{0,1\} \times \{0,\ldots,k\}\} \subset J \times K. \tag{IV.9}$$

Applying this estimate and the triangle inequality, we can thus bound X by (IV.10)

$$X \leq \sum_{(s,t)\text{ strongly admissible}} (1/p)^{2j(k+1)-|\Omega|} \times \left|\sum_{\alpha,\beta} \prod_{i\in[j]} \prod_{\mu=0}^{1} \left[\left(\prod_{l\in[k]} c_{\alpha(s_{i,\mu,l-1})\beta(t_{i,\mu,l-1}),\alpha(s_{i,\mu,l})\beta(t_{i,\mu,l})}\right) \cdot E_{\alpha(s_{i,\mu,k})\beta(t_{i,\mu,k})}\right]\right| \tag{IV.10}$$

where the sum is over those admissible (s,t) such that each element of Ω is visited at least twice by the sequence $(s_{i,\mu,l}, t_{i,\mu,l})$; we shall call such (s,t) *strongly admissible*. We will use the bound (IV.10) as a starting point for proving the moment estimates (III.25) and (III.27).

Example. The pair (s,t) in the Example in Section IV-B is admissible but not strongly admissible, because not every element of the set Ω (which, in this example, is $\{(1,1),(2,2),(3,1),(2,3),(3,4),(1,2),(1,4)\}$) is visited twice by the (s,t).

Remark. Once again, the formula (IV.10) is valid when $k = 0$, with the usual conventions on empty products (in particular, the factor involving the c coefficients can be deleted in this case).

V. Quadratic Bound in the Rank

This section establishes (III.25) under the assumptions of Theorem 1.1, which is the easier of the two moment estimates. Here we shall just take the absolute values in (IV.10) inside the summation and use the estimates on the coefficients given to us by hypothesis. Indeed, starting with (IV.10) and applying (IV.9), we see that the product $\prod_{i\in[j]} \prod_{\mu=0}^{1} |E_{\alpha(s_{i,\mu,k})\beta(t_{i,\mu,k})}|$ is bounded by $\left(\sqrt{r_\mu}/n\right)^{2j}$, where we recall that $r_\mu = \mu^2 r$. Letting Q be the set of all $(i,\mu,l) \in [j] \times \{0,1\} \times [k]$ such that $s_{i,\mu,l-1} \neq s_{i,\mu,l}$ and $t_{i,\mu,l-1} \neq t_{i,\mu,l}$ and applying (III.24), we see that

$$\prod_{i\in[j]} \prod_{\mu=0}^{1} \prod_{l\in[k]} |c_{\alpha(s_{i,\mu,l-1})\beta(t_{i,\mu,l-1}),\alpha(s_{i,\mu,l})\beta(t_{i,\mu,l})}| \leq \left(\sqrt{r_\mu}/n\right)^{2|Q|} \left(2\sqrt{r_\mu}/n\right)^{2jk-|Q|}.$$

Thinking of the sequence $\{(s_{i,\mu,l}, t_{i,\mu,l})\}$ as a path in $J \times K$, we have that $(i,\mu,l) \in Q$ if and only if the move from $(s_{i,\mu,l-1}, t_{i,\mu,l-1})$ to $(s_{i,\mu,l}, t_{i,\mu,l})$ is neither horizontal nor vertical; per our earlier discussion, this is a "non-rook" move. All in all, this gives

$$X \leq 2^{jk} \sum_{(s,t)\text{ strongly admissible}} (1/p)^{2j(k+1)-|\Omega|} \times \sum_{\alpha,\beta} \left(\sqrt{r_\mu}/n\right)^{2j(k+1)+|Q|}.$$

Example. The example in Section IV-B is admissible, but not strongly admissible. Nevertheless, the above definitions can still be applied, and we see that $Q = \{(1,0,1),(1,1,1),(2,0,1),(2,1,1)\}$ in this case, because all of the four associated moves are non-rook moves.

As the number of injections α, β is at most $n^{|J|}$, $n^{|K|}$, respectively, we thus have the first equation shown at the bottom of the next page, which we rearrange slightly as in the second equation shown at the bottom of the next page. Since (s,t) is strongly admissible and every point in Ω needs to be visited at least twice, we see that

$$|\Omega| \leq j(k+1).$$

Also, since $Q \subset [j] \times \{0,1\} \times [k]$, we have the trivial bound

$$|Q| \leq 2jk.$$

This ensures that

$$\frac{|Q|}{2} + 2|\Omega| - 3j(k+1) \leq 0$$
$$\text{and}$$
$$2j(k+1) - |\Omega| \geq j(k+1).$$

From the hypotheses of Theorem 1.1, we have $np \geq r_\mu^2$, and thus

$$X \leq \left(\frac{2r_\mu^2}{np}\right)^{j(k+1)} \sum_{(s,t) \text{ str. admiss.}} n^{|J|+|K|-|Q|-|\Omega|}.$$

Remark. In the case where $k = 0$ in which $Q = \emptyset$, one can easily obtain a better estimate, namely, (if $np \geq r_\mu$)

$$X \leq \left(\frac{2r_\mu}{np}\right)^{j} \sum_{(s,t) \text{ str. admiss.}} n^{|J|+|K|-|\Omega|}.$$

Call a triple (i,μ,l) *recycled* if we have $s_{i',\mu',l'} = s_{i,\mu,l}$ or $t_{i',\mu',l'} = t_{i,\mu,l}$ for some $(i',\mu',l') < (i,\mu,l)$, and *totally recycled* if $(s_{i',\mu',l'}, t_{i',\mu',l'}) = (s_{i,\mu,l}, t_{i,\mu,l})$ for some $(i',\mu',l') < (i,\mu,l)$. Let Q' denote the set of all $(i,\mu,l) \in Q$ which are recycled.

Example. The example in Section IV-B is admissible, but not strongly admissible. Nevertheless, the above definitions can still be applied, and we see that the triples

$$(1,1,0),(1,1,1),(2,0,0),(2,0,1),(2,1,0),(2,1,1)$$

are all recycled (because they either reuse an existing value of s or t or both), while the triple $(2,1,1)$ is totally recycled (it visits the same location as the earlier triple $(1,0,1)$). Thus, in this case, we have $Q' = \{(1,1,1),(2,0,1),(2,1,1)\}$.

We observe that if $(i,\mu,l) \in [j] \times \{0,1\} \times [k]$ is not recycled, then it must have been reached from $(i,\mu,l-1)$ by a non-rook move, and thus, (i,μ,l) lies in Q.

Lemma 5.1 (Exponent Bound): For any admissible tuple, we have $|J| + |K| - |Q| - |\Omega| \leq -|Q'| + 1$.

Proof: We let (i,μ,l) increase from $(1,0,0)$ to $(j,1,k)$ and see how each (i,μ,l) influences the quantity $|J| + |K| - |Q\backslash Q'| - |\Omega|$.

First, we see that the triple $(1,0,0)$ initializes $|J|, |K|, |\Omega| = 1$ and $|Q\backslash Q'| = 0$, so $|J| + |K| - |Q\backslash Q'| - |\Omega| = 1$ at this initial stage. Now we see how each subsequent (i,μ,l) adjusts this quantity.

If (i,μ,l) is totally recycled, then J, K, Ω, $Q\backslash Q'$ are unchanged by the addition of (i,μ,l), and so $|J|+|K|-|Q\backslash Q'|-|\Omega|$ does not change.

If (i,μ,l) is recycled but not totally recycled, then one of J, K increases in size by at most one, as does Ω, but the other set of J, K remains unchanged, as does $Q\backslash Q'$, and so $|J| + |K| - |Q\backslash Q'| - |\Omega|$ does not increase. If (i,μ,l) is not recycled at all, then (by (IV.6)) we must have $l > 0$, and then (by definition of Q, Q') we have $(i,\mu,l) \in Q\backslash Q'$, and so $|Q\backslash Q'|$ and $|\Omega|$ both increase by one. Meanwhile, $|J|$ and $|K|$ increase by 1, and so $|J|+|K|-|Q\backslash Q'|-|\Omega|$ does not change. Putting all this together we obtain the claim. ∎

This lemma gives

$$X \leq \left(\frac{2r_\mu^2}{np}\right)^{j(k+1)} \sum_{\text{str. admiss.}} n^{-|Q'|+1}.$$

Remark. When $k = 0$, we have the better bound

$$X \leq \left(\frac{2r_\mu}{np}\right)^{j} \sum_{\text{str. admiss.}} n.$$

To estimate the above sum, we need to count strongly admissible pairs. This is achieved by the following lemma.

Lemma 5.2 (Pair Counting): For fixed $q \geq 0$, the number of strongly admissible pairs (s,t) with $|Q'| = q$ is at most $O(j(k+1))^{2j(k+1)+q}$.

Proof: First, observe that once one fixes q, the number of possible choices for Q' is $\binom{2jk}{q}$, which we can bound crudely by $2^{2j(k+1)} \leq 2^{2j(k+1)+q}$. So we may without loss of generality assume that Q' is fixed. For similar reasons we may assume Q is fixed.

As with the proof of Lemma 5.1, we increment (i,μ,l) from $(1,0,0)$ to $(j,1,k)$ and upper bound how many choices we have available for $s_{i,\mu,l}$, $t_{i,\mu,l}$ at each stage.

There are no choices available for $s_{1,0,0}$, $t_{1,0,0}$, which must both be one. Now suppose that $(i,\mu,l) > (1,0,0)$. There are several cases. If $l = 0$, then by (IV.6) one of $s_{i,\mu,l}$, $t_{i,\mu,l}$ has no

$$X \leq 2^{2jk} \sum_{(s,t) \text{ str. admiss.}} (1/p)^{2j(k+1)-|\Omega|} n^{|J|+|K|} \left(\sqrt{r_\mu}/n\right)^{2j(k+1)+|Q|}$$

$$X \leq 2^{jk} \sum_{(s,t) \text{ str. admiss.}} \left(\frac{r_\mu^2}{np}\right)^{2j(k+1)-|\Omega|} r_\mu^{\frac{|Q|}{2}+2|\Omega|-3j(k+1)} n^{|J|+|K|-|Q|-|\Omega|}$$

choices available to it, while the other has at most $O(j(k+1))$ choices. If $l > 0$ and $(i,\mu,l) \notin Q$, then at least one of $s_{i,\mu,l}$, $t_{i,\mu,l}$ is necessarily equal to its predecessor; there are at most two choices available for which index is equal in this fashion, and then there are $O(j(k+1))$ choices for the other index.

If $l > 0$ and $(i,\mu,l) \in Q \backslash Q'$, then both $s_{i,\mu,l}$ and $t_{i,\mu,l}$ are new, and are thus equal to the first positive integer not already occupied by $s_{i',\mu',l'}$ or $t_{i',\mu',l'}$ respectively for $(i',\mu',l') < (i,\mu,l)$. So there is only one choice available in this case.

Finally, if $(i,\mu,l) \in Q'$, then there can be $O(j(k+1))$ choices for both $s_{i,\mu,l}$ and $t_{i,\mu,l}$.

Multiplying together all these bounds, we obtain that the number of strongly admissible pairs is bounded by

$$O(j(k+1))^{2j+2jk-|Q|+2|Q'|} = O(j(k+1))^{2j(k+1)-|Q\backslash Q'|+|'|}$$

which proves the claim (here we discard the $|Q \setminus Q'|$ factor). ■

Using the above lemma we obtain

$$X \le \left(\frac{2r_\mu^2}{np}\right)^{j(k+1)} n \sum_{q=0}^{2jk} O(j(k+1))^{2j(k+1)+q} n^{-q}.$$

Under the assumption $n \ge c_0 j(k+1)$ for some numerical constant c_0, we can sum the series and obtain Theorem 3.4.

Remark. When $k = 0$, we have the better bound

$$X \le O(j)^{2j} n \left(\frac{2r_\mu}{np}\right)^j.$$

VI. Linear Bound in the Rank

We now prove the more sophisticated moment estimate (III.27) under the hypotheses of Theorem 1.2. Here, we cannot afford to take absolute values immediately, as in the proof of (III.25), but first must exploit some algebraic cancellation properties in the coefficients $c_{ab,a'b'}$, E_{ab} appearing in (IV.10) to simplify the sum.

A. Cancellation Identities

Recall from (III.23) that the coefficients $c_{ab,a'b'}$ are defined in terms of the coefficients $U_{a,a'}$, $V_{b,b'}$ introduced in (III.22). We recall the symmetries $U_{a,a'} = U_{a',a}, V_{b,b'} = V_{b',b}$ and the projection identities

$$\sum_{a'} U_{a,a'} U_{a',a''} = (1-2\rho)\, U_{a,a''} + \rho\,(1-\rho)\, 1_{a=a''} \quad \text{(VI.1)}$$

$$\sum_{b'} V_{b,b'} V_{b',b''} = (1-2\rho)\, V_{b,b''} + \rho\,(1-\rho)\, 1_{b=b''}. \quad \text{(VI.2)}$$

The first identity follows from the matrix identity

$$\sum_{a'} U_{a,a'} U_{a',a''} = \left\langle e_a, Q_U^2 e_{a''} \right\rangle$$

after one writes the projection identity $P_U^2 = P_U$ in terms of Q_U using (III.21), and similarly for the second identity.

In a similar vein, we also have the identities

$$\sum_{a'} U_{a,a'} E_{a',b} = (1-\rho)\, E_{a,b} = \sum_{b'} E_{a,b'} V_{b',b} \quad \text{(VI.3)}$$

which simply come from $Q_U E = P_U E - \rho E = (1-\rho)E$ together with $E Q_V = E P_V - \rho E = (1-\rho)E$. Finally, we observe the two equalities

$$\sum_b E_{a,b} E_{a',b} = U_{a,a'} + \rho 1_{a=a'}$$
$$\sum_a E_{a,b} E_{a,b'} = V_{b,b'} + \rho 1_{b=b'}. \quad \text{(VI.4)}$$

The first identity follows from the fact that $\sum_b E_{a,b} E_{a',b}$ is the (a,a')th element of $EE^* = P_U = Q_U + \rho I$, and the second one similarly follows from the identity $E^*E = P_V = Q_V + \rho I$.

B. Reduction to a Summand Bound

Just as before, our goal is to estimate

$$X := \mathbb{E}\mathrm{trace}(A^*A)^j, \quad A = (\mathcal{Q}_\Omega \mathcal{Q}_T)^k \mathcal{Q}_\Omega E.$$

We recall the bound (IV.10), and expand each of the c coefficients using (III.23) into three terms. To describe the resulting expansion of the sum we need more notation. Define an *admissible quadruplet* $(s,t,\mathcal{L}_U,\mathcal{L}_V)$ to be an admissible pair (s,t), together with two sets $\mathcal{L}_U, \mathcal{L}_V$ with $\mathcal{L}_U \cup \mathcal{L}_V = [j] \times \{0,1\} \times [k]$, such that $s_{i,\mu,l-1} = s_{i,\mu,l}$ whenever $(i,\mu,l) \in ([j] \times \{0,1\} \times [k]) \backslash \mathcal{L}_U$, and $t_{i,\mu,l-1} = t_{i,\mu,l}$ whenever $(i,\mu,l) \in ([j] \times \{0,1\} \times [k]) \backslash \mathcal{L}_V$. If (s,t) is also strongly admissible, we say that $(s,t,\mathcal{L}_U,\mathcal{L}_V)$ is a strongly admissible quadruplet.

The sets $\mathcal{L}_U \backslash \mathcal{L}_V$, $\mathcal{L}_V \backslash \mathcal{L}_U$, $\mathcal{L}_U \cap \mathcal{L}_V$ will correspond to the three terms $1_{b=b'} U_{a,a'}$, $1_{a=a'} V_{b,b'}$, $U_{a,a'} V_{b,b'}$ appearing in (III.23). With this notation, we expand the product

$$\prod_{i\in[j]} \prod_{\mu=0}^{1} \prod_{l\in[k]} c_{\alpha(s_{i,\mu,l-1})\beta(t_{i,\mu,l-1}),\alpha(s_{i,\mu,l})\beta(t_{i,\mu,l})}$$

as

$$\sum_{\mathcal{L}_U,\mathcal{L}_V} (1-\rho)^{|\mathcal{L}_U\backslash\mathcal{L}_V|+|\mathcal{L}_V\backslash\mathcal{L}_U|} (-1)^{|\mathcal{L}_U\cap\mathcal{L}_V|} \left[\prod_{(i,\mu,l)\in\mathcal{L}_U\backslash\mathcal{L}V} 1_{\beta(t_{i,\mu,l-1})=\beta(t_{i,\mu,l})} U_{\alpha(s_{i,\mu,l-1}),\alpha(s_{i,\mu,l})}\right] \left[\prod_{(i,\mu,l)\in\mathcal{L}_V\backslash\mathcal{L}U} 1_{\alpha(s_{i,\mu,l-1})=\alpha(s_{i,\mu,l})} V_{\beta(t_{i,\mu,l-1}),\beta(t_{i,\mu,l})}\right] \left[\prod_{(i,\mu,l)\in\mathcal{L}_U\cap\mathcal{L}_V} U_{\alpha(s_{i,\mu,l-1}),\alpha(s_{i,\mu,l})} V_{\beta(t_{i,\mu,l-1}),\beta(t_{i,\mu,l})}\right]$$

where the sum is over all pairs $(\mathcal{L}_U,\mathcal{L}_V)$ as above. We pause to explain the expansion above as this is likely to be

helpful to the nonspecialist: we are interested in the product $\prod_{i\in[j]}\left(T_1^{(i)}+T_2^{(i)}+T_3^{(i)}\right)$, which can be expanded as

$$\prod_{i\in[j]}\left(T_1^{(i)}+T_2^{(i)}+T_3^{(i)}\right)=\sum_{k_1,k_2,\ldots,k_j\in[3]}\prod_{i\in[j]}T_{k_i}^{(i)}.$$

Another way to look at this formula is to let I_1 be the set of indices i with $k_i=1$ and similarly for I_2 and I_3 so that

$$\prod_{i\in[j]}T_{k_i}^{(i)}=\prod_{i\in I_1}T_1^{(i)}\prod_{i\in I_2}T_2^{(i)}\prod_{i\in I_3}T_3^{(i)}.$$

With this, we have

$$\prod_{i\in[j]}\left(T_1^{(i)}+T_2^{(i)}+T_3^{(i)}\right)=\sum_{I_1,I_2,I_3}\prod_{i\in I_1}T_1^{(i)}\prod_{i\in I_2}T_2^{(i)}\prod_{i\in I_3}T_3^{(i)}$$

where the sum is over all partitions (I_1,I_2,I_3) of $[j]$. This is how we obtain the expansion above in which $(\mathcal{L}_U\backslash\mathcal{L}_V,\mathcal{L}_V\backslash\mathcal{L}_U,\mathcal{L}_U\cap\mathcal{L}_V)$ is the partition of interest. Now, we rearrange this expansion as

$$\sum_{\mathcal{L}_U,\mathcal{L}_V}(1-\rho)^{2jk-|\mathcal{L}_U\cap\mathcal{L}_V|}(-1)^{|\mathcal{L}_U\cap\mathcal{L}_V|}\times\left[\prod_{(i,\mu,l)\in\mathcal{L}_U}U_{\alpha(s_{i,\mu,l-1}),\alpha(s_{i,\mu,l})}\right]\times\left[\prod_{(i,\mu,l)\in\mathcal{L}_V}V_{\beta(t_{i,\mu,l-1}),\beta(t_{i,\mu,l})}\right].$$

From (IV.10) and the triangle inequality, it follows from

$$X\le\sum_{(s,t,\mathcal{L}_U,\mathcal{L}_V)}(1-\rho)^{2jk-|\mathcal{L}_U\cap\mathcal{L}_V|}(1/p)^{2j(k+1)-|\Omega|}|X_{s,t,\mathcal{L}_U,\mathcal{L}V}|$$

where the sum ranges over all strongly admissible quadruplets, and

$$X_{s,t,\mathcal{L}_U,\mathcal{L}_V}:=\sum_{\alpha,\beta}\left[\prod_{i\in[j]}\prod_{\mu=0}^{1}E_{\alpha(s_{i,\mu,k})\beta(t_{i,\mu,k})}\right]\times\left[\prod_{(i,\mu,l)\in\mathcal{L}_U}U_{\alpha(s_{i,\mu,l-1}),\alpha(s_{i,\mu,l})}\right]\times\left[\prod_{(i,\mu,l)\in\mathcal{L}_V}V_{\beta(t_{i,\mu,l-1}),\beta(t_{i,\mu,l})}\right].$$

Remark. A strongly admissible quadruplet can be viewed as the configuration of a "spider" with several additional constraints. First, the spider must visit each of its vertices at least twice (strong admissibility). When $(i,\mu,l)\in[j]\times\{0,1\}\times[k]$ lies out of $\mathcal{L}_U$, then only horizontal rook moves are allowed when reaching (i,μ,l) from $(i,\mu,l-1)$; similarly, when (i,μ,l) lies out of $\mathcal{L}_V$, then only vertical rook moves are allowed from $(i,\mu,l-1)$ to (i,μ,l). In particular, non-rook moves are only allowed inside $\mathcal{L}_U\cap\mathcal{L}_V$; in the notation of the previous section, we have $Q\subset\mathcal{L}_U\cap\mathcal{L}_V$. Note though that while one has the right to execute a non-rook move to $\mathcal{L}_U\cap\mathcal{L}_V$, it is not mandatory; it could still be that $(s_{i,\mu,l-1},t_{i,\mu,l-1})$ shares a common row or column (or even both) with $(s_{i,\mu,l},t_{i,\mu,l})$.

We claim the following fundamental bound on the summand $|X_{s,t,\mathcal{L}_U,\mathcal{L}_V}|$.

Proposition 6.1 (Summand Bound): Let $(s,t,\mathcal{L}_U,\mathcal{L}_V)$ be a strongly admissible quadruplet. Then we have

$$|X_{s,t,\mathcal{L}_U,\mathcal{L}_V}|\le O(j(k+1))^{2j(k+1)}(r_\mu/n)^{2j(k+1)-|\Omega|}n.$$

Assuming this proposition, we have

$$X\le O(j(k+1))^{2j(k+1)}\sum_{(s,t,\mathcal{L}_U,\mathcal{L}_V)}(r_\mu/np)^{2j(k+1)-|\Omega|}n$$

and since $|\Omega|\le j(k+1)$ (by strong admissibility) and $r\le np$, and the number of $(s,t,\mathcal{L}_U,\mathcal{L}_V)$ can be crudely bounded by $O(j(k+1))^{4j(k+1)}$

$$X\le O(j(k+1))^{6j(k+1)}(r_\mu/np)^{j(k+1)}n.$$

This gives (III.27) as desired. The bound on the number of quadruplets follows from the fact that there are at most $(j(k+1))^{4j(k+1)}$ strongly admissible pairs and that the number of $(\mathcal{L}_U,\mathcal{L}_V)$ per pair is at most $3^{2j(k+1)}$.

Remark. It seems clear that the exponent 6 can be lowered by a finer analysis, for instance by using counting bounds such as Lemma 5.2. However, substantial effort seems to be required in order to obtain the optimal exponent of 1 here.

C. Proof of Proposition 6.1

To prove the proposition, it is convenient to generalize it by allowing k to depend on i, μ. More precisely, define a *configuration* $\mathcal{C}=(j,k,J,K,s,t,\mathcal{L}_U,\mathcal{L}_V)$ to be the following set of data.

- An integer $j\ge 1$, and a map $k:[j]\times\{0,1\}\to\{0,1,2,\ldots\}$, generating a set $\Gamma:=\{(i,\mu,l):i\in[j],\mu\in\{0,1\},0\le l\le k(i,\mu)\}$.
- Finite sets J, K, and surjective maps $s:\Gamma\to J$ and $t:\Gamma\to K$ obeying (IV.6).
- Sets $\mathcal{L}_U$, $\mathcal{L}_V$ such that

$$\mathcal{L}_U\cup\mathcal{L}_V:=\Gamma_+:=\{(i,\mu,l)\in\Gamma:l>0\}$$

and such that $s_{i,\mu,l-1}=s_{i,\mu,l}$ whenever $(i,\mu,l)\in\Gamma_+\backslash\mathcal{L}_U$, and $t_{i,\mu,l-1}=t_{i,\mu,l}$ whenever $(i,\mu,l)\in\Gamma_+\backslash\mathcal{L}_V$.

Remark. Note that we do not require configurations to be strongly admissible, although for our application of Proposition 6.1 strong admissibility is required. Similarly, we no longer require that the segments (IV.7) be initial segments. This removal of hypotheses will give us a convenient amount of flexibility in a certain induction argument that we shall perform shortly. One can think of a configuration as describing a "generalized spider" whose legs are allowed to be of unequal length, but for which certain of the segments/certain parts of the segments (indicated by the sets $\mathcal{L}_U$, $\mathcal{L}_V$) are required to be horizontal or vertical. The freedom to extend or shorten the legs of the spider separately will be of importance when we use the identities (VI.1),

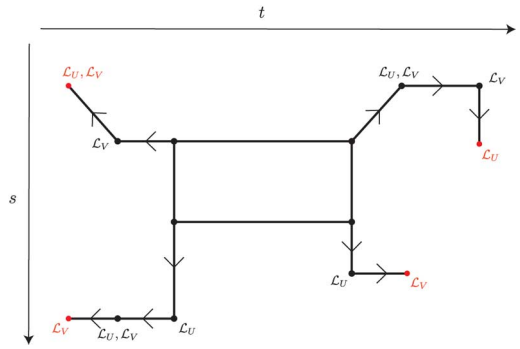

Fig. 4. Generalized spider (note the variable leg lengths). A vertex labeled just by $\mathcal{L}_U$ must have been reached from its predecessor by a vertical rook move, while a vertex labeled just by $\mathcal{L}_V$ must have been reached by a horizontal rook move. Vertices labeled by both $\mathcal{L}_U$ and $\mathcal{L}_V$ *may* be reached from their predecessor by a non-rook move, but they are still allowed to lie on the same row or column as their predecessor, as is the case in the leg on the bottom left of this figure. The sets $\mathcal{L}_U$, $\mathcal{L}_V$ indicate which U and V terms will show up in the expansion (VI.5).

(VI.3), (VI.4) to simplify the expression $X_{s,t,\mathcal{L}_U,\mathcal{L}_V}$, see Fig. 4.

Given a configuration $\mathcal{C}$, define the quantity $X_{\mathcal{C}}$ by the formula

$$X_{\mathcal{C}} := \sum_{\alpha,\beta} \left[\prod_{i\in[j]} \prod_{\mu=0}^{1} E_{\alpha(s(i,\mu,k(i,\mu)))\beta(t(i,\mu,k(i,\mu)))} \right] \cdot \left[\prod_{(i,\mu,l)\in\mathcal{L}_U} U_{\alpha(s(i,\mu,l-1)),\alpha(s(i,\mu,l))} \right] \cdot \left[\prod_{(i,\mu,l)\in\mathcal{L}_V} V_{\beta(t(i,\mu,l-1)),\beta(t(i,\mu,l))} \right] \quad \text{(VI.5)}$$

where $\alpha : J \to [n]$, $\beta : K \to [n]$ range over all injections. To prove Proposition 6.1, it then suffices to show that

$$|X_{\mathcal{C}}| \leq (C_0(1+|J|+|K|))^{|J|+|K|}(r_\mu/n)^{|\Gamma|-|\Omega|}n \quad \text{(VI.6)}$$

for some absolute constant $C_0 > 0$, where

$$\Omega := \{(s(i,\mu,l), t(i,\mu,l)) : (i,\mu,l) \in \Gamma\}$$

since Proposition 6.1 then follows from the special case in which $k(i,\mu) = k$ is constant and (s,t) is strongly admissible, in which case we have

$$|J|+|K| \leq 2|\Omega| \leq |\Gamma| = 2j(k+1)$$

(by strong admissibility).

To prove the claim (VI.6) we will perform strong induction on the quantity $|J|+|K|$; thus, we assume that the claim has already been proven for all configurations with a strictly smaller value of $|J|+|K|$ (this inductive hypothesis can be vacuous for very small values of $|J|+|K|$).[4] Then, for fixed $|J|+|K|$, we perform strong induction on $|\mathcal{L}_U \cap \mathcal{L}_V|$, assuming that the claim has already been proven for all configurations with the same value of $|J|+|K|$ and a strictly smaller value of $|\mathcal{L}_U \cap \mathcal{L}_V|$.

Remark. Roughly speaking, the inductive hypothesis is asserting that the target estimate (VI.6) has already been proven for all generalized spider configurations which are "simpler" than the current configuration, either by using fewer rows and columns, or by using the same number of rows and columns but by having fewer opportunities for non-rook moves.

As we shall shortly see, whenever we invoke the inner induction hypothesis (decreasing $|\mathcal{L}_U \cap \mathcal{L}_V|$, keeping $|J|+|K|$ fixed) we are replacing the expression $X_{\mathcal{C}}$ with another expression $X_{\mathcal{C}'}$ covered by this hypothesis; this causes no degradation in the constant. However, when we invoke the outer induction hypothesis (decreasing $|J|+|K|$), we will be splitting up $X_{\mathcal{C}}$ into about $O(1+|J|+|K|)$ terms $X_{\mathcal{C}'}$, each of which is covered by this hypothesis; this causes a degradation of $O(1+|J|+|K|)$ in the constants and is thus responsible for the loss of $(C_0(1+|J|+|K|))^{|J|+|K|}$ in (VI.6).

For future reference we observe that we may take $r_\mu \leq n$, as the hypotheses of Theorem 1.1 are vacuous otherwise (m cannot exceed n^2).

To prove (VI.6) we divide into several cases.

1) First Case: An Unguarded Non-Rook Move: Suppose first that $\mathcal{L}_U \cap \mathcal{L}_V$ contains an element (i_0,μ_0,l_0) with the property that

$$(s_{i_0,\mu_0,l_0-1}, t_{i_0,\mu_0,l_0}) \notin \Omega. \quad \text{(VI.7)}$$

Note that this forces the edge from $(s_{i_0,\mu_0,l_0-1}, t_{i_0,\mu_0,l_0-1})$ to $(s_{i_0,\mu_0,l_0}, t_{i_0,\mu_0,l_0})$ to be partially "unguarded" in the sense that one of the opposite vertices of the rectangle that this edge is inscribed in is not visited by the (s,t) pair.

When we have such an unguarded non-rook move, we can "erase" the element (i_0,μ_0,l_0) from $\mathcal{L}_U \cap \mathcal{L}_V$ by replacing $\mathcal{C} = (j,k,J,K,s,t,\mathcal{L}_U,\mathcal{L}_V)$ by the "stretched" variant $\mathcal{C}' = (j',k',J',K',s',t',\mathcal{L}'_U,\mathcal{L}'_V)$, defined as follows.

- $j' := j$, $J' := J$, and $K' := K$.
- $k'(i,\mu) := k(i,\mu)$ for $(i,\mu) \neq (i_0,\mu_0)$, and $k'(i_0,\mu_0) := k(i_0,\mu_0)+1$.
- $\left(s'_{i,\mu,l}, t'_{i,\mu,l}\right) := (s_{i,\mu,l}, t_{i,\mu,l})$ whenever $(i,\mu) \neq (i_0,\mu_0)$, or when $(i,\mu) = (i_0,\mu_0)$ and $l < l_0$.
- $\left(s'_{i,\mu,l}, t'_{i,\mu,l}\right) := (s_{i,\mu,l-1}, t_{i,\mu,l-1})$ whenever $(i,\mu) = (i_0,\mu_0)$ and $l > l_0$.
- $\left(s'_{i_0,\mu_0,l_0}, t'_{i_0,\mu_0,l_0}\right) := (s_{i_0,\mu_0,l_0-1}, t_{i_0,\mu_0,l_0})$.

[4]The principle of strong induction asserts that if $P(n)$ is a property involving a natural number n, and for every natural number n, the statement that $P(m)$ holds for all $m < n$ implies that $P(n)$ holds, then $P(n)$ holds for all n. Unlike the ordinary principle of induction, the principle of strong induction does not require a separate "base case": if $n = 0$, then the claim "$P(m)$ holds for all $m < n$" is vacuously true, and the implication "$P(m)$ holds for all $m < n$ implies that $P(n)$ holds" is equivalent to asserting that $P(0)$ holds. In the current argument, if $|J|+|K|$ is extremely small, what happens in practice is that the cases which would require one to decrease $|J|+|K|$ further cannot occur, and other cases are activated instead, so the (vacuous) induction hypothesis is not actually used.

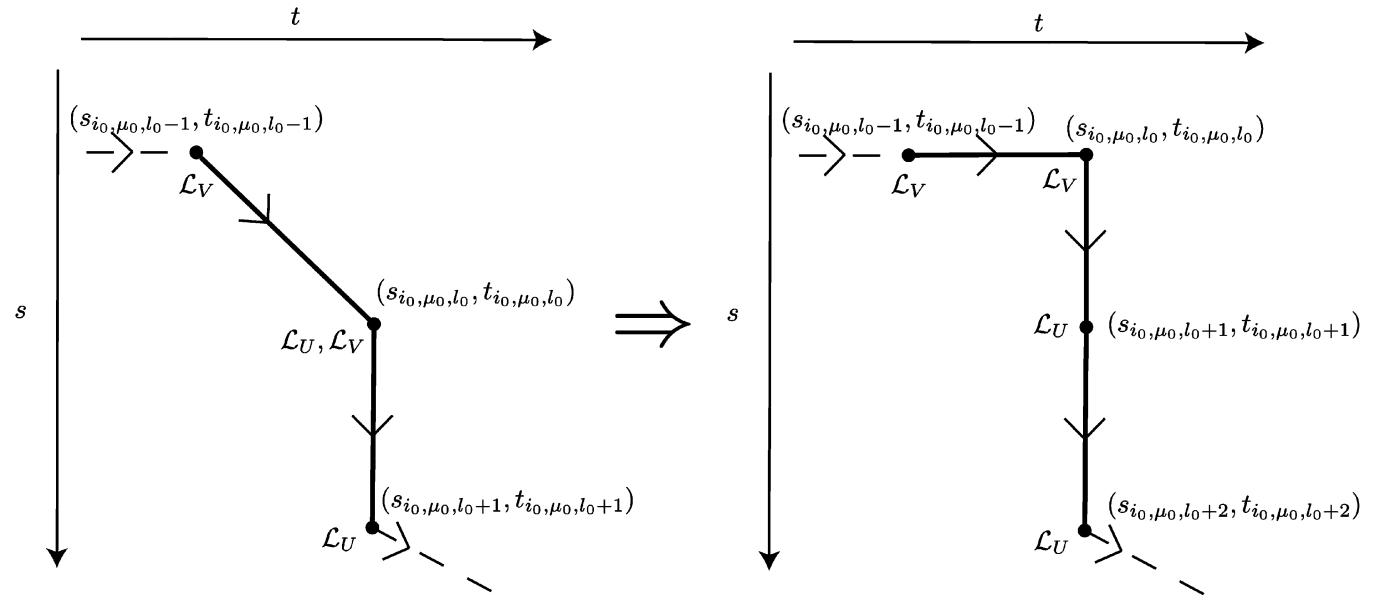

Fig. 5. Fragment of a leg showing how an unguarded non-rook move from $(s_{i_0,\mu_0,l_0-1}, t_{i_0,\mu_0,l_0-1})$ to $(s_{i_0,\mu_0,l_0}, t_{i_0,\mu_0,l_0})$ is converted into two rook moves, thus decreasing $|\mathcal{L}_U \cap \mathcal{L}_V|$ by one. Note that the labels further down the leg have to be incremented by one.

- We have

$$\begin{aligned}\mathcal{L}'_U :=& \{(i,\mu,l) \in \mathcal{L}_U : (i,\mu) \neq (i_0,\mu_0)\} \\ & \cup \{(i_0,\mu_0,l) \in \mathcal{L}_U : l < l_0\} \\ & \cup \{(i_0,\mu_0,l+1) : (i_0,\mu_0,l) \in \mathcal{L}_U \\ & \quad l > l_0 + 1\} \\ & \cup \{(i_0,\mu_0,l_0+1)\} \\ & \qquad \text{and} \\ \mathcal{L}'_V :=& \{(i,\mu,l) \in \mathcal{L}_V : (i,\mu) \neq (i_0,\mu_0)\} \\ & \cup \{(i_0,\mu_0,l) \in \mathcal{L}_V : l < l_0\} \\ & \cup \{(i_0,\mu_0,l+1) : (i_0,\mu_0,l) \in \mathcal{L}_V \\ & \quad l > l_0 + 1\} \\ & \cup \{(i_0,\mu_0,l_0)\}.\end{aligned}$$

All of this is illustrated in Fig. 5.

One can check that $\mathcal{C}'$ is still a configuration, and $X_{\mathcal{C}'}$ is exactly equal to $X_{\mathcal{C}}$; informally what has happened here is that a single "non-rook" move (which contributed both a $U_{a,a'}$ factor and a $V_{b,b'}$ factor to the summand in $X_{\mathcal{C}}$) has been replaced with an equivalent pair of two rook moves (one of which contributes the $U_{a,a'}$ factor, and the other contributes the $V_{b,b'}$ factor). Observe that, $|\Gamma'| = |\Gamma| + 1$ and $|\Omega'| = |\Omega| + 1$ (here we use the nonguarded hypothesis (VI.7)), while $|J'| + |K'| = |J| + |K|$ and $|\mathcal{L}'_U \cap \mathcal{L}'_V| = |\mathcal{L}_U \cap \mathcal{L}_V| - 1$. Thus, in this case, we see that the claim follows from the (second) induction hypothesis. We may thus eliminate this case and assume that

$$(s_{i_0,\mu_0,l_0-1}, t_{i_0,\mu_0,l_0}) \in \Omega \text{ whenever } (i_0,\mu_0,l_0) \in \mathcal{L}_U \cap \mathcal{L}_V. \tag{VI.8}$$

For similar reasons we may assume

$$(s_{i_0,\mu_0,l_0}, t_{i_0,\mu_0,l_0-1}) \in \Omega \text{ whenever } (i_0,\mu_0,l_0) \in \mathcal{L}_U \cap L_V. \tag{VI.9}$$

2) Second Case: A Low Multiplicity Row or Column, No Unguarded Non-Rook Moves: Next, given any $x \in J$, define the *row multiplicity* τ_x to be

$$\begin{aligned}\tau_x :=& |\{(i,\mu,l) \in \mathcal{L}_U : s(i,\mu,l) = x\}| \\ & + |\{(i,\mu,l) \in \mathcal{L}_U : s(i,\mu,l-1) = x\}| \\ & + |\{(i,\mu) \in [j] \times \{0,1\} : s(i,\mu,k(i,\mu)) = x\}|\end{aligned}$$

and similarly for any $y \in K$, define the *column multiplicity* τ^y to be

$$\begin{aligned}\tau^y :=& |\{(i,\mu,l) \in \mathcal{L}_V : t(i,\mu,l) = y\}| \\ & + |\{(i,\mu,l) \in \mathcal{LV} : t(i,\mu,l-1) = y\}| \\ & + |\{(i,\mu) \in [j] \times \{0,1\} : t(i,\mu,k(i,\mu)) = y\}|.\end{aligned}$$

Remark. Informally, τ_x measures the number of times $\alpha(x)$ appears in (VI.5), and similarly for τ^y and $\beta(y)$. Beware that τ_x is not simply counting the number of times the spider visits row $s = x$ since the definition excludes those indices $(i,\mu,l) \in \mathcal{L}_V \cap \mathcal{L}_U$ implying horizontal moves, and similarly, τ^y is not simply counting the number of visits to column $t = y$.

By surjectivity we know that τ_x, τ^y are strictly positive for each $x \in J$, $y \in K$. We also observe that τ_x, τ^y must be even. To see this, write

$$\begin{aligned}\tau_x = & \sum_{(i,\mu,l) \in \mathcal{L}_U} \left(1_{s(i,\mu,l)=x} + 1_{s(i,\mu,l-1)=x}\right) \\ & + \sum_{(i,\mu) \in [j] \times \{0,1\}} 1_{s(i,\mu,k(i,\mu))=x}.\end{aligned}$$

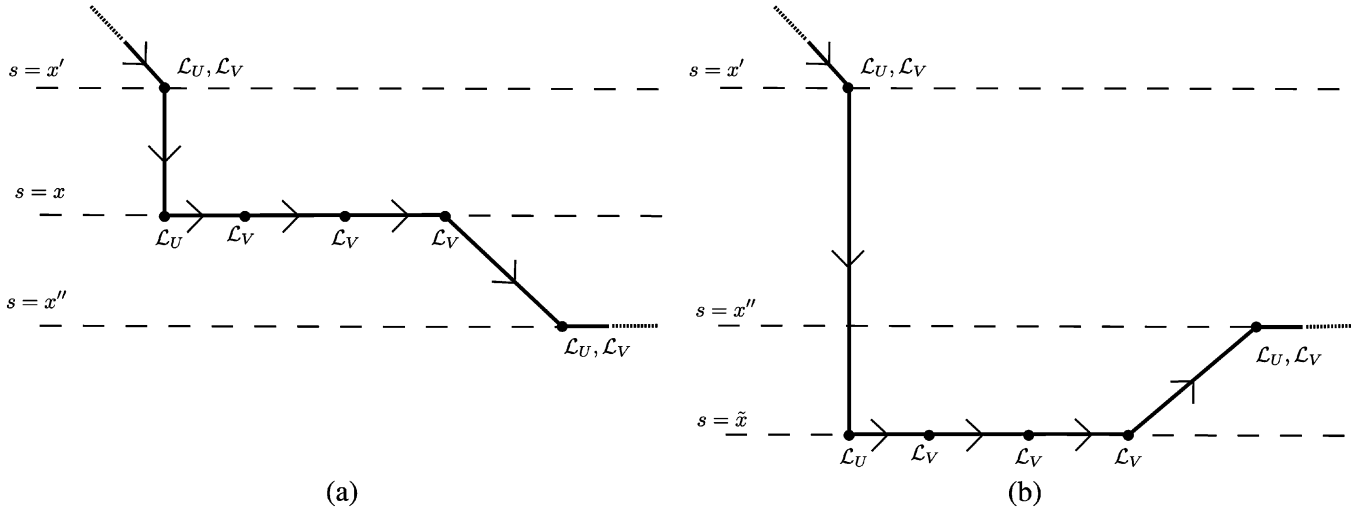

Fig. 6. In (a), a multiplicity 2 row is shown. After using the identity (VI.1), the contribution of this configuration is replaced with a number of terms one of which is shown in (b), in which the x row is deleted and replaced with another existing row $\tilde{x}$.

Now observe that if $(i,\mu,l) \in \Gamma_+ \backslash \mathcal{L}_U$, then $1_{s(i,\mu,l)=x} = 1_{s(i,\mu,l-1)=x}$. Thus, we have

$$\tau_x \bmod 2 = \sum_{(i,\mu,l)\in\Gamma_+} \left(1_{s(i,\mu,l)=x} + 1_{s(i,\mu,l-1)=x}\right) + \sum_{i,\mu\in[j]\times\{0,1\}} 1_{s(i,\mu,k(i,\mu))=x} \bmod 2$$

but we can telescope this to

$$\tau_x \bmod 2 = \sum_{i,\mu\in[j]\times\{0,1\}} 1_{s(i,\mu,0)=x} \bmod 2$$

and the right-hand side vanishes by (IV.6), showing that τ_x is even, and similarly τ^y is even.

In this subsection, we dispose of the case of a low-multiplicity row, or more precisely when $\tau_x = 2$ for some $x \in J$. By symmetry, the argument will also dispose of the case of a low-multiplicity column, when $\tau^y = 2$ for some $y \in K$.

Suppose that $\tau_x = 2$ for some $x \in J$. We first remark that this implies that there does not exist $(i,\mu,l) \in \mathcal{L}_U$ with $s(i,\mu,l) = s(i,\mu,l-1) = x$. We argue by contradiction and define $l^\star$ to be the first integer larger than l for which $(i,\mu,l^\star) \in \mathcal{L}_U$. First, suppose that $l^\star$ does not exist (which, for instance, happens when $l = k(i,\mu)$). Then in this case it is not hard to see that $s(i,\mu,k(i,\mu)) = x$ since for $(i,\mu,l') \notin \mathcal{L}_U$, we have $s(i,\mu,l') = s(i,\mu,l'-1)$. In this case, τ_x exceeds 2. Else, $l^\star$ does exist but then $s(i,\mu,l^\star - 1) = x$ since $s(i,\mu,l') = s(i,\mu,l'-1)$ for $l < l' < l^\star$. Again, τ_x exceeds 2 and this is a contradiction. Thus, if $(i,\mu,l) \in \mathcal{L}_U$ and $s(i,\mu,l) = x$, then $s(i,\mu,l-1) \neq x$, and similarly if $(i,\mu,l) \in \mathcal{L}_U$ and $s(i,\mu,l-1) = x$, then $s(i,\mu,l) \neq x$.

Now let us look at the terms in (VI.5) which involve $\alpha(x)$. Since $\tau_x = 2$, there are only two such terms, and each of the terms are either of the form $U_{\alpha(x),\alpha(x')}$ or $E_{\alpha(x),\beta(y)}$ for some $y \in K$ or $x' \in J\backslash\{x\}$. We now have to divide into three subcases.

Subcase 1: (VI.5) Contains Two Terms $U_{\alpha(x),\alpha(x')}$, $U_{\alpha(x),\alpha(x'')}$: Fig. 6(a) for a typical configuration in which this is the case.

The idea is to use the identity (VI.1) to "delete" the row x, thus reducing $|J| + |K|$ and allowing us to use an induction hypothesis. Accordingly, let us define $\tilde{J} := J\backslash\{x\}$, and let $\tilde{\alpha} : \tilde{J} \to [n]$ be the restriction of α to $\tilde{J}$. We also write $a := \alpha(x)$ for the deleted row a.

We now isolate the two terms $U_{\alpha(x),\alpha(x')}$, $U_{\alpha(x),\alpha(x'')}$ from the rest of (VI.5), expressing this sum as

$$\sum_{\tilde{\alpha},\beta} \cdots \left[\sum_{a\in[n]\backslash\tilde{\alpha}(\tilde{J})} U_{a,\tilde{\alpha}(x')} U_{a,\tilde{\alpha}(x'')}\right]$$

where the $\ldots$ denotes the product of all the terms in (VI.5) other than $U_{\alpha(x),\alpha(x')}$ and $U_{\alpha(x),\alpha(x'')}$, but with α replaced by $\tilde{\alpha}$, and $\tilde{\alpha}$, β ranging over injections from $\tilde{J}$ and K to $[n]$, respectively.

From (VI.1), we have

$$\sum_{a\in[n]} U_{a,\tilde{\alpha}(x')} U_{a,\tilde{\alpha}(x'')} = (1-2\rho)\, U_{\tilde{\alpha}(x'),\tilde{\alpha}(x'')} + \rho\,(1-\rho)\, 1_{x'=x''}$$

and thus

$$\sum_{a\in[n]\backslash\tilde{\alpha}(\tilde{J})} U_{a,\tilde{\alpha}(x')} U_{a,\tilde{\alpha}(x'')} = (1-2\rho)\, U_{\tilde{\alpha}(x'),\tilde{\alpha}(x'')} + \rho\,(1-\rho)\, 1_{x'=x''} - \sum_{\tilde{x}\in\tilde{J}} U_{\tilde{\alpha}(\tilde{x}),\tilde{\alpha}(x')} U_{\tilde{\alpha}(\tilde{x}),\tilde{\alpha}(x'')}. \quad \text{(VI.10)}$$

Consider the contribution of one of the final terms $U_{\tilde{\alpha}(\tilde{x}),\tilde{\alpha}(x')} U_{\tilde{\alpha}(\tilde{x}),\tilde{\alpha}(x'')}$ of (VI.10). This contribution is equal to $X_{\mathcal{C}'}$, where $\mathcal{C}'$ is formed from $\mathcal{C}$ by replacing J with $\tilde{J}$, and replacing every occurrence of x in the range of α with $\tilde{x}$, but leaving all other components of $\mathcal{C}$ unchanged (see Fig. 6(b)). Observe that $|\Gamma'| = |\Gamma|$, $|\Omega'| \leq |\Omega|$, $|J'| + |K'| < |J| + |K|$, so the contribution of these terms is acceptable by the (first) induction hypothesis (for C_0 large enough).

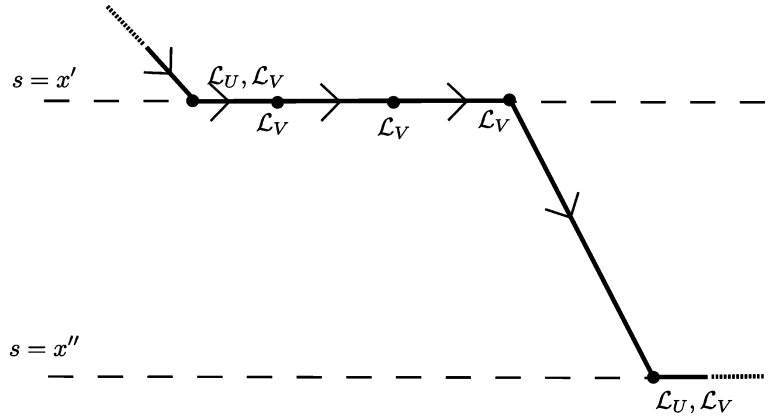

Fig. 7. Another term arising from the configuration in Fig. 6(a), in which two U factors have been collapsed into one. Note the reduction in length of the configuration by one.

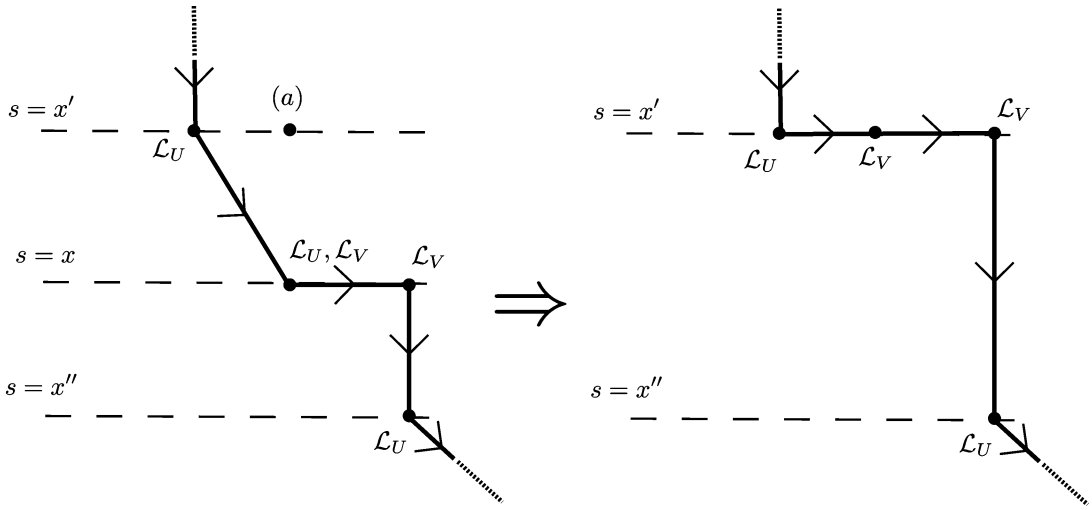

Fig. 8. Another collapse of two U factors into one. This time, the presence of the $\mathcal{L}_V$ label means that the length of the configuration remains unchanged; but the guarded nature of the collapsed non-rook move [evidenced here by the point (a)] ensures that the support Ω of the configuration shrinks by at least one instead.

Next, we consider the contribution of the term $U_{\tilde{\alpha}(x'),\tilde{\alpha}(x'')}$ of (VI.10). This contribution is equal to $X_{\mathcal{C}''}$, where $\mathcal{C}''$ is formed from $\mathcal{C}$ by replacing J with $\tilde{J}$, replacing every occurrence of x in the range of α with x', and also deleting the one element (i_0, μ_0, l_0) in $\mathcal{L}_U$ from Γ_+ (relabeling the remaining triples (i_0, μ_0, l) for $l_0 < l \leq k(i_0, \mu_0)$ by decrementing l by 1) that gave rise to $U_{\alpha(x),\alpha(x')}$, unless this element (i_0, μ_0, l_0) also lies in $\mathcal{L}_V$, in which case one removes (i_0, μ_0, l_0) from $\mathcal{L}_U$ but leaves it in $\mathcal{L}_V$ (and does not relabel any further triples) (see Fig. 7 for an example of the former case, and Fig. 8 for the latter case). One observes that $|\Gamma''| \geq |\Gamma| - 1$, $|\Omega''| \leq |\Omega| - 1$ (here we use (VI.8), (VI.9)), $|J''| + |K''| < |J| + |K|$, and so this term also is controlled by the (first) induction hypothesis (for C_0 large enough).

Finally, we consider the contribution of the term $\rho 1_{x'=x''}$ of (VI.10), which of course is only nontrivial when $x' = x''$. This contribution is equal to $\rho X_{\mathcal{C}'''}$, where $\mathcal{C}'''$ is formed from $\mathcal{C}$ by deleting x from J, replacing every occurrence of x in the range of α with $x' = x''$, and also deleting the two elements (i_0, μ_0, l_0), (i_1, μ_1, l_1) of $\mathcal{L}_U$ from Γ_+ that gave rise to the factors $U_{\alpha(x),\alpha(x')}$, $U_{\alpha(x),\alpha(x'')}$ in (VI.5), unless these elements also lie in $\mathcal{L}_V$, in which case one deletes them just from $\mathcal{L}_U$ but leaves them in $\mathcal{L}_V$ and Γ_+; one also decrements the labels of any subsequent (i_0, μ_0, l), (i_1, μ_1, l) accordingly (see Fig. 9). One observes that $|\Gamma'''| - |\Omega'''| \geq |\Gamma| - |\Omega| - 1$, $|J'''| + |K'''| < |J| + |K|$, and so this term also is controlled by the induction hypothesis [note we need to use the additional ρ factor (which is less than r_μ/n) in order to make up for a possible decrease in $|\Gamma| - |\Omega|$ by 1].

This deals with the case when there are two U terms involving $\alpha(x)$.

Subcase 2: (VI.5) Contains a Term $U_{\alpha(x),\alpha(x')}$ and a Term $E_{\alpha(x),\beta(y)}$: A typical case here is depicted in Fig. 10.

The strategy here is similar to Subcase 1, except that one uses (VI.3) instead of (VI.1). Letting $\tilde{J}$, $\tilde{\alpha}$, a be as before, we can express (VI.5) as

$$\sum_{\tilde{\alpha},\beta} \cdots \left[\sum_{a \in [n] \backslash \tilde{\alpha}(\tilde{J})} U_{a,\tilde{\alpha}(x')} E_{a,\beta(y)} \right]$$

where the $\ldots$ denotes the product of all the terms in (VI.5) other than $U_{\alpha(x),\alpha(x')}$ and $E_{\alpha(x),\beta(y)}$, but with α replaced by $\tilde{\alpha}$, and $\tilde{\alpha}$, β ranging over injections from $\tilde{J}$ and K to $[n]$, respectively.

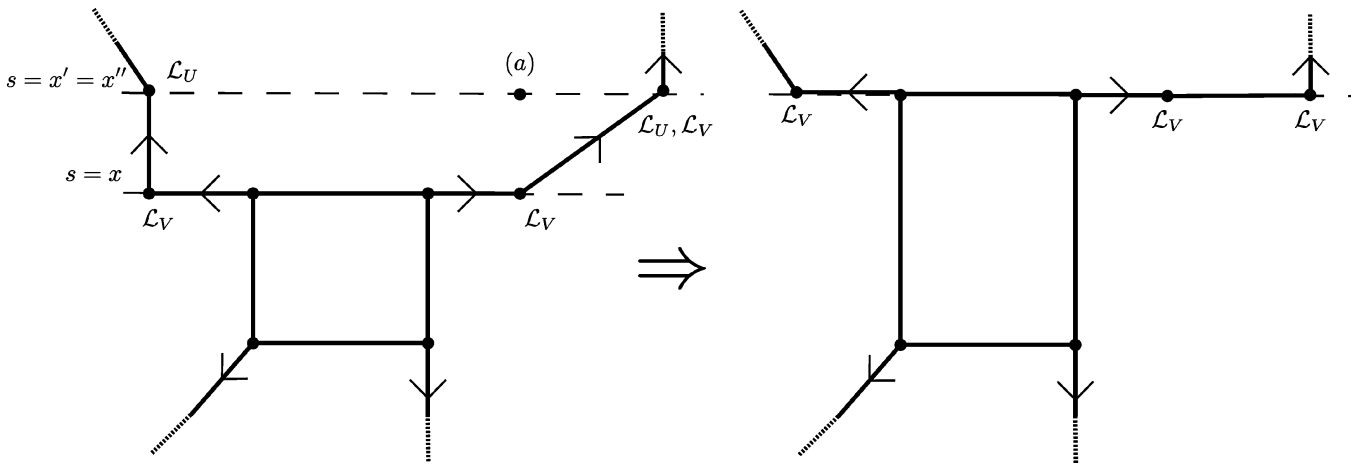

Fig. 9. Collapse of two U factors (with identical indices) to a $\rho 1_{x'=x''}$ factor. The point marked (a) indicates the guarded nature of the non-rook move on the right. Note that $|\Gamma| - |\Omega|$ can decrease by at most 1 (and will often stay constant or even increase).

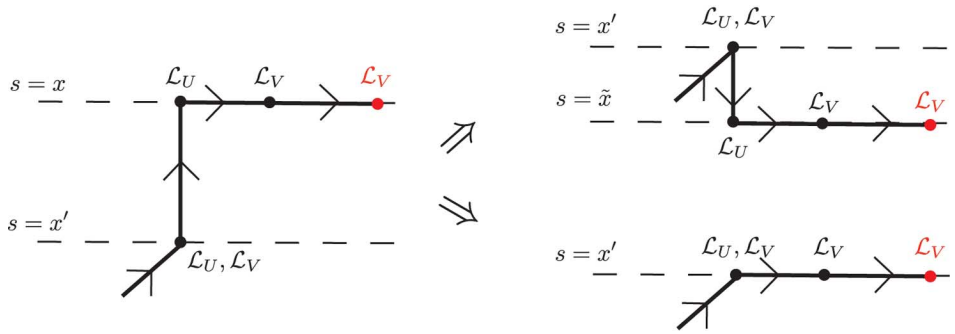

Fig. 10. Configuration involving a U and E factor on the left. After applying (VI.3), one gets some terms associated to configuations such as those in the upper right, in which the x row has been deleted and replaced with another existing row $\tilde{x}$, plus a term coming from a configuration in the lower right, in which the UE terms have been collapsed to a single E term.

From (VI.3), we have

$$\sum_{a\in[n]} U_{a,\tilde{\alpha}(x')} E_{a,\beta(y)} = (1-\rho)\, E_{\tilde{\alpha}(x'),\beta(y)}$$

and hence

$$\sum_{a\in[n]\setminus\tilde{\alpha}(\tilde{J})} U_{a,\tilde{\alpha}(x')} E_{a,\beta(y)} = (1-\rho)\, E_{\tilde{\alpha}(x'),\beta(y)} - \sum_{\tilde{x}\in\tilde{J}} U_{\tilde{\alpha}(\tilde{j}),\tilde{\alpha}(x')} E_{\tilde{\alpha}(\tilde{j}),\beta(y)}. \quad \text{(VI.11)}$$

The contribution of the final terms in (VI.11) are treated in exactly the same way as the final terms in (VI.10), and the main term $E_{\tilde{\alpha}(x'),\beta(y)}$ is treated in exactly the same way as the term $U_{\tilde{\alpha}(x'),\tilde{\alpha}(x'')}$ in (VI.10) This concludes the treatment of the case when there is one U term and one E term involving $\alpha(x)$.

Subcase 3: (VI.5) Contains Two Terms $E_{\alpha(x),\beta(y)}$, $E_{\alpha(x),\beta(y')}$: A typical case here is depicted in 11. The strategy here is similar to that in the previous two subcases, but now one uses (VI.4) rather than (VI.1). The combinatorics of the situation are, however, slightly different.

By considering the path from $E_{\alpha(x),\beta(y)}$ to $E_{\alpha(x),\beta(y')}$ along the spider, we see (from the hypothesis $\tau_x = 2$) that this path must be completely horizontal (with no elements of $\mathcal{L}_U$ present), and the two legs of the spider that give rise to $E_{\alpha(x),\beta(y)}$, $E_{\alpha(x),\beta(y')}$ at their tips must be adjacent, with their bases connected by a horizontal line segment. In other words, up to interchange of y and y', and cyclic permutation of the $[j]$ indices, we may assume that

$$(x,y) = (s(1,1,k(i,1)), t(1,1,k(i,1)))$$
$$(x,y') = (s(2,0,k(2,0)), t(2,0,k(2,0)))$$

with

$$s(1,1,l) = s(2,0,l') = x$$

for all $0 \le l \le k(1,1)$ and $0 \le l' \le k(2,0)$, where the index 2 is understood to be identified with 1 in the degenerate case $j = 1$. Also, $\mathcal{L}_U$ cannot contain any triple of the form $(1,1,l)$ for $l \in [k(1,1)]$ or $(2,0,l')$ for $l' \in [k(2,0)]$ (and so all these triples lie in $\mathcal{L}_V$ instead).

For technical reasons we need to deal with the degenerate case $j = 1$ separately. In this case, s is identically equal to x, and so (VI.5) simplifies to

$$\sum_{\beta} \left[\sum_{a\in[n]} E_{a,\beta(y)} E_{a,\beta(y')} \right] \prod_{\mu=0}^{1} \prod_{l=0}^{k(1,\mu)} V_{\beta(t(i,\mu,l-1)),\beta(t(i,\mu,l))}.$$

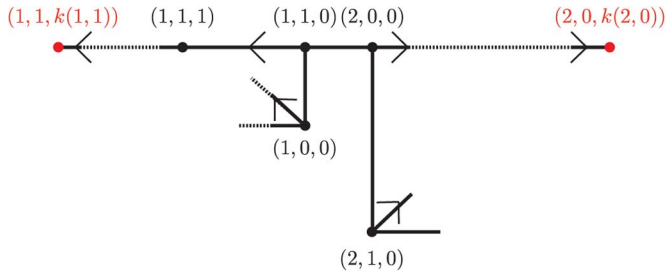

Fig. 11. Multiplicity 2 row with two Es, which are necessarily at the ends of two adjacent legs of the spider. Here, we use (i,μ,l) as shorthand for $(s_{i,\mu,l}, t_{i,\mu,l})$.

In the extreme degenerate case when $k(1,0) = k(1,1) = 0$, the sum is just $\sum_{a,b\in[n]} E_{ab}^2 = r$, which is acceptable, so we may assume that $k(1,0)+k(1,1) > 0$. We may assume that the column multiplicity $\tau^{\tilde{y}} \geq 4$ for every $\tilde{y} \in K$, since otherwise we could use (the reflected form of) one of the previous two subcases to conclude (VI.6) from the induction hypothesis (note when $y = y'$, it is not possible for τ^y to equal 2 since $k(1,0) + k(1,1) > 0$).

Using (VI.4) followed by (I.8a) we have

$$\left|\sum_{a\in[n]} E_{a,\beta(y)}E_{a,\beta(y')}\right| \lesssim \sqrt{r_\mu}/n + 1_{y=y'}r/n \lesssim r_\mu/n$$

and so by (I.8b), we can bound

$$|X_{\mathcal{C}}| \lesssim \sum_{\beta}(r_\mu/n)\left(\sqrt{r_\mu}/n\right)^{k(1,0)+k(1,1)}.$$

The number of possible β is at most $n^{|K|}$, so to establish (VI.6) in this case it suffices to show that

$$n^{|K|}(r_\mu/n)\left(\sqrt{r_\mu}/n\right)^{k(1,0)+k(1,1)} \lesssim (r_\mu/n)^{|\Gamma|-|\Omega|}n.$$

Observe that in this degenerate case $j = 1$, we have $|\Omega| = |K|$ and $|\Gamma| = k(1,0)+k(1,1)+2$. One then checks that the claim is true when $r_\mu = 1$, so it suffices to check that the other extreme case $r_\mu = n$, i.e.,

$$|K| - \frac{1}{2}(k(1,0)+k(1,1)) \leq 1$$

but as $\tau^y \geq 4$ for all y, every element in K must be visited at least twice (in other words $k(1,0)+k(1,1) \geq 2|K|$), and the claim follows.

Now we deal with the nondegenerate case $j > 1$. Letting $\tilde{J}$, $\tilde{\alpha}$, a be as in previous subcases, we can express (VI.5) as

$$\sum_{\tilde{\alpha},\beta}\cdots\left[\sum_{a\in[n]\setminus\tilde{\alpha}(\tilde{J})} E_{a,\beta(y)}E_{a,\beta(y')}\right] \qquad \text{(VI.12)}$$

where the $\ldots$ denotes the product of all the terms in (VI.5) other than $E_{\alpha(x),\beta(y)}$ and $E_{\alpha(x),\beta(y')}$, but with α replaced by $\tilde{\alpha}$, and $\tilde{\alpha}$, β ranging over injections from $\tilde{J}$ and K to $[n]$ respectively.

From (VI.4), we have

$$\sum_{a\in[n]} E_{a,\beta(y)}E_{a,\beta(y')} = V_{\beta(y),\beta(y')} + \rho 1_{y=y'}$$

and hence

$$\sum_{a\in[n]\setminus\tilde{\alpha}(\tilde{J})} E_{a,\beta(y)}E_{a,\beta(y')} = V_{\beta(y),\beta(y')} + \rho 1_{y=y'} - \sum_{\tilde{x}\in\tilde{J}} E_{\tilde{\alpha}(\tilde{x}),\beta(y)}E_{\tilde{\alpha}(\tilde{x}),\beta(y')}. \qquad \text{(VI.13)}$$

The final terms are treated here in exactly the same way as the final terms in (VI.10) or (VI.11). Now we consider the main term $V_{\beta(y),\beta(y')}$. The contribution of this term will be of the form $X_{\mathcal{C}'}$, where the configuration $\mathcal{C}'$ is formed from $\mathcal{C}$ by "detaching" the two legs $(i,\mu) = (1,1),(2,0)$ from the spider, "gluing them together" at the tips using the $V_{\beta(y),\beta(y')}$ term, and then "inserting" those two legs into the base of the $(i,\mu) = (1,0)$ leg. To explain this procedure more formally, observe that the $\ldots$ term in (VI.12) can be expanded further (isolating out the terms coming from $(i,\mu) = (1,1),(2,0)$) as

$$\left[\prod_{l=1}^{k(2,0)} V_{\beta(t(2,0,l-1)),\beta(t(2,0,l))}\right] \cdot \left[\prod_{l=k(1,1)}^{1} V_{\beta(s(1,1,l-1)),\beta(s(1,1,l))}\right]\cdots$$

where the $\ldots$ now denotes all the terms that do not come from $(i,\mu) = (1,1)$ or $(i,\mu) = (2,0)$, and we have reversed the order of the second product for reasons that will be clearer later. Recalling that $y = t(1,1,k(1,1))$ and $y' = t(2,0,k(2,0))$, we see that the contribution of the first term of (VI.13) to (VI.12) is now of the form

$$\sum_{\tilde{\alpha},\beta}\left[\prod_{l=1}^{k(2,0)} V_{\beta(t(2,0,l-1)),\beta(t(2,0,l))}\right] \cdot V_{\beta(t(2,0,k(2,0))),\beta(t(1,1,k(1,1)))} \cdot \left[\prod_{l=k(1,1)}^{1} V_{\beta(s(1,1,l-1)),\beta(s(1,1,l))}\right]\cdots.$$

bBut this expression is simply $X_{\mathcal{C}'}$, where the configuration $\mathcal{C}'$ is formed from $\mathcal{C}$ in the following fashion.

- j' is equal to $j-1$, J' is equal to $\tilde{J}$, and K' is equal to K.
- $k'(1,0) := k(2,0)+1+k(1,1)+k(1,0)$, and $k'(i,\mu) := k(i+1,\mu)$ for $(i,\mu) \neq (1,0)$.
- The path $\{(s'(1,0,l),t'(1,0,l)) : l = 0,\ldots,k'(1,0)\}$ is formed by concatenating the path $\{(s(1,0,0),t(2,0,l)) : l = 0,\ldots,k(2,0)\}$, with an edge from $(s(1,0,0),t(2,0,k(2,0)))$ to $(s(1,0,0),t(1,1,k(1,1)))$, with the path $\{(s(1,0,0),t(1,1,l)) : l = k(1,1),\ldots,0\}$, with the path $\{(s(1,0,l),t(1,0,l)) : l = 0,\ldots,k(1,0)\}$.

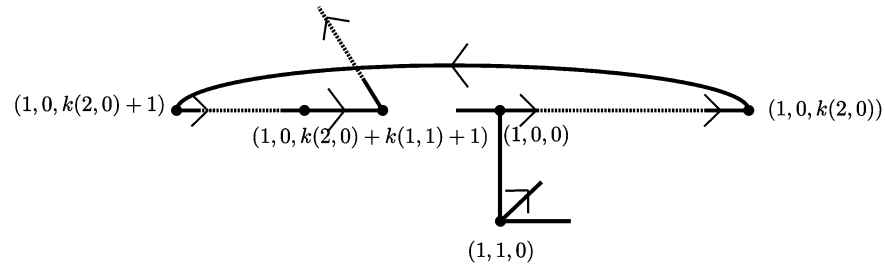

Fig. 12. Configuation from Fig. 11 after collapsing the two E's to a V, which is represented by a long curved line rather than a straight line for clarity. Note the substantial relabeling of vertices.

- For any $(i,\mu) \neq (i,0)$, the path $\{(s'(i,\mu,l),t'(i,\mu,l)) : l = 0,\dots k'(i,\mu)\}$ is equal to the path $\{(s(i,\mu,l),t(i+1,\mu,l)) : l = 0,\dots,k(i+1,\mu)\}$.
- We have

$$\begin{aligned}\mathcal{L}'_U :=& \{(1,0,k(2,0)+1+k(1,1)+l) : (1,0,l) \in \mathcal{L}_U\} \\ & \cup \{(i,\mu,l) : (i+1,\mu,l) \in \mathcal{L}_U\} \\ & \text{and} \\ \mathcal{L}'_V :=& \{(1,0,k(2,0)+1+k(1,1)+l) : (1,0,l) \in \mathcal{L}_V\} \\ & \cup \{(i,\mu,l) : (i+1,\mu,l) \in \mathcal{L}_V\} \\ & \cup \{(1,0,1),\dots,(1,0,k(2,0)+1+k(1,1))\}.\end{aligned}$$

This construction is represented in Fig. 12.

One can check that this is indeed a configuration. One has $|J'|+|K'| < |J|+|K|$, $|\Gamma'| = |\Gamma|-1$, and $|\Omega'| \leq |\Omega|-1$, and so this contribution to (VI.6) is acceptable from the (first) induction hypothesis.

This handles the contribution of the $V_{\beta(y),\beta(y')}$ term. The $\rho 1_{y=y'}$ term is treated similarly, except that there is no edge between the points $(s(1,0,0),t(2,0,k(2,0)))$ and $(s(1,0,0),t(1,1,k(1,1)))$ (which are now equal, since $y = y'$). This reduces the analogue of $|\Gamma'|$ to $|\Gamma| - 2$, but the additional factor of ρ (which is at most r_μ/n) compensates for this. We omit the details. This concludes the treatment of the third subcase.

3) Third Case: High Multiplicity Rows and Columns: After eliminating all of the previous cases, we may now may assume (since τ_x is even) that

$$\tau_x \geq 4 \text{ for all } x \in J \tag{VI.14}$$

and similarly we may assume that

$$\tau^y \geq 4 \text{ for all } y \in K. \tag{VI.15}$$

We have now made the maximum use we can of the cancellation identities (VI.1), (VI.3), (VI.4), and have no further use for them. Instead, we shall now place absolute values everywhere and estimate $X_{\mathcal{C}}$ using (I.9), (I.8a), (I.8b), obtaining the bound

$$|X_{\mathcal{C}}| \leq n^{|J|+|K|} O\left(\sqrt{r_\mu}/n\right)^{|\Gamma|+|\mathcal{L}_U \cap \mathcal{L}_V|}.$$

Comparing this with (VI.6), we see that it will suffice (by taking C_0 large enough) to show that

$$n^{|J|+|K|}\left(\sqrt{r_\mu}/n\right)^{|\Gamma|+|\mathcal{L}U \cap \mathcal{L}_V|} \leq (r_\mu/n)^{|\Gamma|-|\Omega|} n.$$

Using the extreme cases $r_\mu = 1$ and $r_\mu = n$ as test cases, we see that our task is to show that

$$|J|+|K| \leq |\mathcal{L}_U \cap \mathcal{L}_V| + |\Omega| + 1 \tag{VI.16}$$

and

$$|J|+|K| \leq \frac{1}{2}(|\Gamma| + |\mathcal{L}U \cap \mathcal{L}_V|) + 1. \tag{VI.17}$$

The first inequality (VI.16) is proven by Lemma 5.1 because $Q \subset \mathcal{L}_U \cap \mathcal{L}_V$, and thus $|Q| \leq |\mathcal{L}_U \cap \mathcal{L}_V|$. The second is a consequence of the double counting identity

$$4(|J|+|K|) \leq \sum_{x \in J} \tau_x + \sum_{y \in K} \tau^y = 2|\Gamma| + 2|\mathcal{L}_U \cap \mathcal{L}_V|$$

where the inequality follows from (VI.14)–(VI.15) (and we don't even need the $+1$ in this case).

VII. Discussion

Interestingly, there is an emerging literature on the development of efficient algorithms for solving the nuclear-norm minimization problem (I.3) [6], [18]. For instance, in [6], the authors show that the singular-value thresholding algorithm can solve certain problem instances in which the matrix has close to a billion unknown entries in a matter of minutes on a personal computer. Hence, the near-optimal sampling results introduced in this paper are practical and, therefore, should be of consequence to practitioners interested in recovering low-rank matrices from just a few entries.

To be broadly applicable, however, the matrix completion problem needs to be robust vis a vis noise. That is, if one is given a few entries of a low-rank matrix contaminated with a small amount of noise, one would like to be able to guess the missing entries, perhaps not exactly, but accurately. We actually believe that the methods and results developed in this paper are amenable to the study of "the noisy matrix completion problem" and hope to report on our progress in a later paper.

Appendix

1) Equivalence Between the Uniform and Bernoulli Models:

2) Lower Bounds: For the sake of completeness, we explain how Theorem 1.7 implies nearly identical results for the uniform model. We have established the lower bound by showing that there are two fixed matrices $M \neq M'$ for which $\mathcal{P}_\Omega(M) = \mathcal{P}_\Omega(M')$ with probability greater than δ unless m

obeys the bound (I.20). Suppose that Ω is sampled according to the Bernoulli model with $p' \geq m/n^2$ and let F be the event $\{\mathcal{P}_\Omega(M) = \mathcal{P}_\Omega(M')\}$. Then

$$\begin{aligned}\mathbb{P}(F) &= \sum_{k=0}^{n^2} \mathbb{P}(F \,|\, |\Omega| = k)\mathbb{P}(|\Omega| = k) \\ &\leq \sum_{k=0}^{m-1} \mathbb{P}(|\Omega| = k) + \sum_{k=m}^{n^2} \mathbb{P}(F||\Omega| = k)\mathbb{P}(|\Omega| = k) \\ &\leq \mathbb{P}(|\Omega| < m) + \mathbb{P}(F \,|\, |\Omega| = m)\end{aligned}$$

where we have used the fact that for $k \geq m$, $\mathbb{P}(F \,|\, |\Omega| = m) \geq \mathbb{P}(F \,|\, |\Omega| = k)$. The conditional distribution of Ω given its cardinality is uniform and, therefore

$$\mathbb{P}_{\mathrm{Unif}(m)}(F) \geq \mathbb{P}_{\mathrm{Ber}(p')}(F) - \mathbb{P}_{\mathrm{Ber}(p')}(|\Omega| < m)$$

in which $\mathbb{P}_{\mathrm{Unif}(m)}$ and $\mathbb{P}_{\mathrm{Ber}(p')}$ are probabilities calculated under the uniform and Bernoulli models. If we choose $p' = 2m/n^2$, we have that $\mathbb{P}_{\mathrm{Ber}(p')}(|\Omega| < m) \leq \delta/2$ provided δ is not ridiculously small. Thus, if $\mathbb{P}_{\mathrm{Ber}(p')}(F) \geq \delta$, we have

$$\mathbb{P}_{\mathrm{Unif}(m)}(F) \geq \delta/2.$$

In short, we get a lower bound for the uniform model by applying the bound for the Bernoulli model with a value of $p = 2m^2/n$ and a probability of failure equal to 2δ.

3) Upper Bounds: We prove the claim stated at the onset of Section III which states that the probability of failure under the uniform model is at most twice that under the Bernoulli model. Let F be the event that the recovery via (I.3) is not exact. With our earlier notations

$$\begin{aligned}\mathbb{P}_{\mathrm{Ber}(p)}(F) &= \sum_{k=0}^{n^2} \mathbb{P}_{\mathrm{Ber}(p)}(F \,|\, |\Omega| = k)\mathbb{P}_{\mathrm{Ber}(p)}(|\Omega| = k) \\ &\geq \sum_{k=0}^{m} \mathbb{P}_{\mathrm{Ber}(p)}(F \,|\, |\Omega| = k)\mathbb{P}_{\mathrm{Ber}(p)}(|\Omega| = k) \\ &\geq \mathbb{P}_{\mathrm{Ber}(p)}(F \,|\, |\Omega| = m) \sum_{k=0}^{m} \mathbb{P}_{\mathrm{Ber}(p)}(|\Omega| = k) \\ &\geq \frac{1}{2}\mathbb{P}_{\mathrm{Unif}(m)}(F)\end{aligned}$$

where we have used $\mathbb{P}_{\mathrm{Ber}(p)}(F \,|\, |\Omega| = k) \geq \mathbb{P}_{\mathrm{Ber}(p)}(F \,|\, |\Omega| = m)$ for $k \leq m$ (the probability of failure is nonincreasing in the size of the observed set), and $\mathbb{P}_{\mathrm{Ber}(p)}(|\Omega| \leq m) \geq 1/2$.

A. Proof of Lemma 3.3

In this section, we will make frequent use of (III.3) and of the similar identity

$$\mathcal{Q}_T^2 = (1 - 2\rho')\mathcal{Q}_T + \rho'(1 - \rho')\mathcal{I} \tag{VIII.1}$$

which is obtained by squaring both sides of (III.17) together with $\mathcal{P}_T^2 = \mathcal{P}_T$. We begin with two lemmas.

Lemma 8.1: For each $k \geq 0$, we have

$$\begin{aligned}&(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega \\ &\quad= \sum_{j=0}^{k} \alpha_j^{(k)}(\mathcal{Q}_\Omega\mathcal{Q}_T)^j\mathcal{Q}_\Omega + \sum_{j=0}^{k-1} \beta_j^{(k)}(\mathcal{Q}_\Omega\mathcal{Q}_T)^j \\ &\qquad+ \sum_{j=0}^{k-2} \gamma_j^{(k)}\mathcal{Q}_T(\mathcal{Q}_\Omega\mathcal{Q}_T)^j\mathcal{Q}_\Omega \\ &\qquad+ \sum_{j=0}^{k-3} \delta_j^{(k)}\mathcal{Q}_T(\mathcal{Q}_\Omega\mathcal{Q}_T)^j\end{aligned} \tag{VIII.2}$$

where starting from $\alpha_0^{(0)} = 1$, the sequences $\{\alpha^{(k)}\}$, $\{\beta^{(k)}\}$, $\{\gamma^{(k)}\}$, and $\{\delta^{(k)}\}$ are inductively defined via

$$\begin{aligned}\alpha_j^{(k+1)} &= \left[\alpha_{j-1}^{(k)} + (1-\rho')\gamma_{j-1}^{(k)}\right] \\ &\quad+ \frac{\rho'(1-2p)}{p}\left[\alpha_j^{(k)} + (1-\rho')\gamma_j^{(k)}\right] \\ &\quad+ 1_{j=0}\rho'\left[\beta_0^{(k)} + (1-\rho')\delta_0^{(k)}\right] \\ \beta_j^{(k+1)} &= \left[\beta_{j-1}^{(k)} + (1-\rho')\delta_{j-1}^{(k)}\right] \\ &\quad+ \frac{\rho'(1-2p)}{p}\left[\beta_j^{(k)} + (1-\rho')\delta_j^{(k)}\right]1_{j>0} \\ &\quad+ 1_{j=0}\rho'\frac{1-p}{p}\left[\alpha_0^{(k)} + (1-\rho')\gamma_0^{(k)}\right]\end{aligned}$$

and

$$\begin{aligned}\gamma_j^{(k+1)} &= \frac{\rho'(1-p)}{p}\left[\alpha_{j+1}^{(k)} + (1-\rho')\gamma_{j+1}^{(k)}\right] \\ \delta_j^{(k+1)} &= \frac{\rho'(1-p)}{p}\left[\beta_{j+1}^{(k)} + (1-\rho')\delta_{j+1}^{(k)}\right].\end{aligned}$$

In the above recurrence relations, we adopt the convention that $\alpha_j^{(k)} = 0$ whenever j is not in the range specified by (VIII.2), and similarly for $\beta_j^{(k)}$, $\gamma_j^{(k)}$ and $\delta_j^{(k)}$.

Proof: The proof operates by induction. The claim for $k = 0$ is straightforward. To compute the coefficient sequences of $(\mathcal{Q}_\Omega\mathcal{P}_T)^{k+1}\mathcal{Q}_\Omega$ from those of $(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega$, use the identity $\mathcal{P}_T = \mathcal{Q}_T + \rho'\mathcal{I}$ to decompose $(\mathcal{Q}_\Omega\mathcal{P}_T)^{k+1}\mathcal{Q}_\Omega$ as follows:

$$(\mathcal{Q}_\Omega\mathcal{P}_T)^{k+1}\mathcal{Q}_\Omega = \mathcal{Q}_\Omega\mathcal{Q}_T(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega + \rho'\mathcal{Q}_\Omega(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega.$$

Then expanding $(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega$ as in (VIII.2), and using the two identities

$$\begin{aligned}&\mathcal{Q}_\Omega(\mathcal{Q}_\Omega\mathcal{Q}_T)^j\mathcal{Q}_\Omega \\ &\quad= \begin{cases} \frac{1-2p}{p}\mathcal{Q}_\Omega + \frac{(1-p)}{p}\mathcal{I}, & j = 0 \\ \frac{1-2p}{p}(\mathcal{Q}_\Omega\mathcal{Q}_T)^j\mathcal{Q}_\Omega + \frac{(1-p)}{p}\mathcal{Q}_T(\mathcal{Q}_\Omega\mathcal{Q}_T)^{j-1}\mathcal{Q}_\Omega, & j > 0 \end{cases}\end{aligned}$$

and

$$\begin{aligned}&\mathcal{Q}_\Omega(\mathcal{Q}_\Omega\mathcal{Q}_T)^j \\ &\quad= \begin{cases} \mathcal{Q}_\Omega, & j = 0 \\ \frac{1-2p}{p}(\mathcal{Q}_\Omega\mathcal{Q}_T)^j + \frac{(1-p)}{p}\mathcal{Q}_T(\mathcal{Q}_\Omega\mathcal{Q}_T)^{j-1} & j > 0 \end{cases}\end{aligned}$$

which both follow from (III.13), gives the desired recurrence relation. The calculation is rather straightforward and omitted. ■

We note that the recurrence relations give $\alpha_k^{(k)} = 1$ for all $k \geq 0$

$$\beta_{k-1}^{(k)} = \beta_{k-2}^{(k-1)} = \cdots = \beta_0^{(1)} = \frac{\rho'(1-p)}{p}$$

for all $k \geq 1$, and

$$\gamma_{k-2}^{(k)} = \frac{\rho'(1-p)}{p}\alpha_{k-1}^{(k-1)} = \frac{\rho'(1-p)}{p},$$
$$\delta_{k-3}^{(k)} = \frac{\rho'(1-p)}{p}\beta_{k-2}^{(k-1)} = \left(\frac{\rho'(1-p)}{p}\right)^2$$

for all $k \geq 2$ and $k \geq 3$, respectively.

Lemma 8.2: Put $\lambda = \rho'/p$ and observe that by assumption (I.22), $\lambda < 1$. Then for all $j, k \geq 0$, we have

$$\max\left(\left|\alpha_j^{(k)}\right|, \left|\beta_j^{(k)}\right|, \left|\gamma_j^{(k)}\right|, \left|\delta_j^{(k)}\right|\right) \leq \lambda^{\lceil \frac{k-j}{2} \rceil} 4^k. \quad \text{(VIII.3)}$$

Proof: We prove the lemma by induction on k. The claim is true for $k = 0$. Suppose it is true up to k, we then use the recurrence relations given by Lemma 8.1 to establish the claim up to $k+1$. In details, since $|1-\rho'| < 1$, $\rho' < \lambda$ and $|1-2p| < 1$, the recurrence relation for $\alpha^{(k+1)}$ gives

$$\begin{aligned}\left|\alpha_j^{(k+1)}\right| &\leq \left|\alpha_{j-1}^{(k)}\right| + \left|\gamma_{j-1}^{(k)}\right| + \lambda\left[\left|\alpha_j^{(k)}\right| + \left|\gamma_j^{(k)}\right|\right] \\ &\quad + 1_{j=0}\lambda\left[\left|\beta_0^{(k)}\right| + \left|\delta_0^{(k)}\right|\right] \\ &\leq 2\,\lambda^{\lceil \frac{k+1-j}{2} \rceil} 4^k 1_{j>0} + 2\lambda^{\lceil \frac{k-j}{2} \rceil + 1} 4^k \\ &\quad + 2\lambda^{\lceil \frac{k}{2} \rceil + 1} 4^k 1_{j=0} \\ &\leq 2\,\lambda^{\lceil \frac{k+1-j}{2} \rceil} 4^k 1_{j>0} + 2\,\lambda^{\lceil \frac{k+1-j}{2} \rceil} 4^k \\ &\quad + 2\,\lambda^{\lceil \frac{k+1}{2} \rceil} 4^k 1_{j=0} \\ &\leq \lambda^{\lceil \frac{k+1-j}{2} \rceil} 4^{k+1}\end{aligned}$$

which proves the claim for the sequence $\{\alpha^{(k)}\}$. We bound $\left|\beta_j^{(k+1)}\right|$ in exactly the same way and omit the details. Now the recurrence relation for $\gamma^{(k+1)}$ gives

$$\begin{aligned}\left|\gamma_j^{(k+1)}\right| &\leq \lambda\left[\left|\alpha_{j+1}^{(k)}\right| + \left|\gamma_{j+1}^{(k)}\right|\right] \\ &\leq 2\lambda^{\lceil \frac{k-j-1}{2} \rceil + 1} 4^k \\ &\leq 4^{k+1}\lambda^{\lceil \frac{k+1-j}{2} \rceil}\end{aligned}$$

which proves the claim for the sequence $\{\gamma^{(k)}\}$. The quantity $|\delta_j^{(k+1)}|$ is bounded in exactly the same way, which concludes the proof of the lemma. ■

We are now well positioned to prove Lemma 3.3 and begin by recording a useful fact. Since for any X, $\|\mathcal{P}_{T^\perp}(X)\| \leq \|X\|$, and

$$\mathcal{Q}_T = \mathcal{P}_T - \rho'\mathcal{I} = (\mathcal{I} - \mathcal{P}_{T^\perp}) - \rho'\mathcal{I} = (1-\rho')\mathcal{I} - \mathcal{P}_{T^\perp}$$

the triangular inequality gives that for all X

$$\|\mathcal{Q}_T(X)\| \leq 2\|X\|. \quad \text{(VIII.4)}$$

Now

$$\begin{aligned}&\left\|(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E)\right\| \\ &\quad \leq \sum_{j=0}^{k}\left|\alpha_j^{(k)}\right|\left\|(\mathcal{Q}_\Omega\mathcal{Q}_T)^j\mathcal{Q}_\Omega(E)\right\| \\ &\qquad + \sum_{j=0}^{k-1}\left|\beta_j^{(k)}\right|\left\|(\mathcal{Q}_\Omega\mathcal{Q}_T)^j(E)\right\| \\ &\qquad + \sum_{j=0}^{k-2}\left|\gamma_j^{(k)}\right|\left\|\mathcal{Q}_T(\mathcal{Q}_\Omega\mathcal{Q}_T)^j\mathcal{Q}_\Omega(E)\right\| \\ &\qquad + \sum_{j=0}^{k-3}\left|\delta_j^{(k)}\right|\left\|\mathcal{Q}_T(\mathcal{Q}_\Omega\mathcal{Q}_T)^j(E)\right\|\end{aligned}$$

and it follows from (VIII.4) that

$$\begin{aligned}&\left\|(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E)\right\| \\ &\quad \leq \sum_{j=0}^{k}\left(\left|\alpha_j^{(k)}\right| + 2\left|\gamma_j^{(k)}\right|\right)\left\|(\mathcal{Q}_\Omega\mathcal{Q}_T)^j\mathcal{Q}_\Omega(E)\right\| \\ &\qquad + \sum_{j=0}^{k-1}\left(\left|\beta_j^{(k)}\right| + 2\left|\delta_j^{(k)}\right|\right)\left\|(\mathcal{Q}_\Omega\mathcal{Q}_T)^j(E)\right\|.\end{aligned}$$

For $j = 0$, we have $\left\|(\mathcal{Q}_\Omega\mathcal{Q}_T)^j(E)\right\| = \|E\| = 1$ while for $j > 0$

$$\begin{aligned}\left\|(\mathcal{Q}_\Omega\mathcal{Q}_T)^j(E)\right\| &= \left\|(\mathcal{Q}_\Omega\mathcal{Q}_T)^{j-1}\mathcal{Q}_\Omega\mathcal{Q}_T(E)\right\| \\ &= (1-\rho')\left\|(\mathcal{Q}_\Omega\mathcal{Q}_T)^{j-1}\mathcal{Q}_\Omega(E)\right\|\end{aligned}$$

since $\mathcal{Q}_T(E) = (1-\rho')(E)$. By using the size estimates given by Lemma 8.2 on the coefficients, we have

$$\begin{aligned}&\frac{1}{3}\left\|(\mathcal{Q}_\Omega\mathcal{P}_T)^k\mathcal{Q}_\Omega(E)\right\| \\ &\quad \leq \frac{1}{3}\sigma^{\frac{k+1}{2}} + 4^k\sum_{j=0}^{k-1}\lambda^{\lceil \frac{k-j}{2} \rceil}\sigma^{\frac{j+1}{2}} + 4^k\sum_{j=0}^{k-1}\lambda^{\lceil \frac{k-j}{2} \rceil}\sigma^{\frac{j}{2}} \\ &\quad \leq \frac{1}{3}\sigma^{\frac{k+1}{2}} + 4^k\sigma^{\frac{k+1}{2}}\sum_{j=0}^{k-1}\lambda^{\lceil \frac{k-j}{2} \rceil}\sigma^{-\frac{k-j}{2}} \\ &\qquad + 4^k\sigma^{\frac{k}{2}}\sum_{j=0}^{k-1}\lambda^{\lceil \frac{k-j}{2} \rceil}\sigma^{-\frac{k-j}{2}} \\ &\quad \leq \frac{1}{3}\sigma^{\frac{k+1}{2}} + 4^k\left(\sigma^{\frac{k+1}{2}} + \sigma^{\frac{k}{2}}\right)\sum_{j=0}^{k-1}\lambda^{\lceil \frac{k-j}{2} \rceil}\sigma^{-\frac{k-j}{2}}.\end{aligned}$$

Now

$$\sum_{j=0}^{k-1}\lambda^{\lceil \frac{k-j}{2} \rceil}\sigma^{-\frac{k-j}{2}} \leq \left(\frac{\lambda}{\sqrt{\sigma}} + \frac{\lambda}{\sigma}\right)\frac{1}{1-\frac{\lambda}{\sigma}} \leq \frac{2}{3}\sqrt{\sigma}$$

where the last inequality holds provided that $4\lambda \leq \sigma^{3/2}$. The conclusion is

$$\left\|(\mathcal{Q}_\Omega \mathcal{P}_T)^k \mathcal{Q}_\Omega(E)\right\| \leq (1+4^{k+1})\sigma^{\frac{k+1}{2}}$$

which is what we needed to establish.

ACKNOWLEDGMENT

E. J. Candès would like to thank X. Li and C. Sabatti for helpful conversations related to this project. The authors would also like to thank S. Gandy and the anonymous referees for a very careful reading and for suggesting corrections.

REFERENCES

[1] J. Abernethy, F. Bach, T. Evgeniou, and J.-P. Vert, Low-Rank Matrix Factorization With Attributes, Ecole des Mines de Paris, 2006, Tech. Rep. N24/06/MM.

[2] Y. Amit, M. Fink, N. Srebro, and S. Ullman, "Uncovering shared structures in multiclass classification," presented at the 24h Int. Conf. Machine Learning, 2007.

[3] A. Argyriou, T. Evgeniou, and M. Pontil, "Multi-task feature learning," *Neural Inf. Process. Syst.*, 2007.

[4] A. Barvinok, "A course in convexity," in *Graduate Studies in Mathematics*. Providence, RI: AMS, 2002, vol. 54.

[5] P. Biswas, T.-C. Lian, T.-C. Wang, and Y. Ye, "Semidefinite programming based algorithms for sensor network localization," *ACM Trans. Sens. Netw.*, vol. 2, no. 2, pp. 188–220, 2006.

[6] J.-F. Cai, E. J. Candès, and Z. Shen, A Singular Value Thresholding Algorithm for Matrix Completion Tech. Rep., 2008 [Online]. Available: http://arxiv.org/abs/0810.3286

[7] E. J. Candès and B. Recht, "Exact matrix completion via convex optimization," *Found. Comput. Math.*, 2008, to be published.

[8] E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.

[9] P. Chen and D. Suter, "Recovering the missing components in a large noisy low-rank matrix: Application to SFM source," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 26, no. 8, pp. 1051–1063, Aug. 2004.

[10] V. H. de la Peña and S. J. Montgomery-Smith, "Decoupling inequalities for the tail probabilities of multivariate U-statistics," *Ann. Prob.*, vol. 23, no. 2, pp. 806–816, 1995.

[11] M. Fazel, H. Hindi, and S. Boyd, "Log-det heuristic for matrix rank minimization with applications to Hankel and Euclidean distance matrices," presented at the Amer. Control Conf., Jun. 2003.

[12] D. Goldberg, D. Nichols, B. M. Oki, and D. Terry, "Using collaborative filtering to weave an information tapestry," *Commun. ACM*, vol. 35, pp. 61–70, 1992.

[13] R. Keshavan, A. Montanari, and S. Oh, Matrix Completion From a Few Entries Tech. Rep., 2009.

[14] R. Keshavan, S. Oh, and A. Montanari, "Matrix completion from a few entries," presented at the ISIT, 2009, arXiv:0901.3150.

[15] M. Ledoux, *The Concentration of Measure Phenomenon*. Providence, RI: AMS, 2001.

[16] A. S. Lewis, "The mathematics of eigenvalue optimization," *Math. Programm. B*, vol. 97, no. 1–2, pp. 155–176, 2003.

[17] F. Lust-Picquard, "Inégalités de Khintchine dans $C_p(1 < p < \infty)$," *Comptes Rendus Acad. Sci. Paris, Série I*, vol. 303, no. 7, pp. 289–292, 1986.

[18] S. Ma, D. Goldfarb, and L. Chen, Fixed Point and Bregman Iterative Methods for Matrix Rank Minimization Tech. Rep., 2008.

[19] C. McDiarmid, "Centering sequences with bounded differences," *Combin. Probab. Comput.*, vol. 6, no. 1, pp. 79–86, 1997.

[20] M. Mesbahi and G. P. Papavassilopoulos, "On the rank minimization problem over a positive semidefinite linear matrix inequality," *IEEE Trans. Autom. Control*, vol. 42, pp. 239–243, 1997.

[21] B. Recht, M. Fazel, and P. Parrilo, "Guaranteed minimum rank solutions of matrix equations via nuclear norm minimization," *SIAM Rev.*, 2007, submitted for publication.

[22] A. Singer, "A remark on global positioning from local distances," *Proc. Nat. Acad. Sci. USA*, vol. 105, no. 28, pp. 9507–9511, 2008.

[23] A. Singer and M. Cucuringu, *Uniqueness of Low-Rank Matrix Completion by Rigidity Theory*, 2009, submitted for publication.

[24] C. Tomasi and T. Kanade, "Shape and motion from image streams under orthography: A factorization method," *Int. J. Comput. Vis.*, vol. 9, no. 2, pp. 137–154, 1992.

[25] G. A. Watson, "Characterization of the subdifferential of some matrix norms," *Linear Algebra Appl.*, vol. 170, pp. 33–45, 1992.

[26] C.-C. Weng, "Matrix completion for sensor networks," Personal Communication, 2009.

[27] E. Wigner, "Characteristic vectors of bordered matrices with infinite dimensions," *Ann. Math.*, no. 62, pp. 548–564, 1955.

Emmanuel J. Candès (A'10) received the B.Sc. degree from the Ecole Polytechnique, France, in 1993, and the Ph.D. degree in statistics from Stanford University, Stanford, CA, in 1998.

He is the Ronald and Maxine Linde Professor of Applied and Computational Mathematics at the California Institute of Technology, Pasadena, and a Professor of statistics and mathematics at Stanford University. His research interests are in computational harmonic analysis, multiscale analysis, approximation theory, statistical estimation, and detection with applications to the imaging sciences, signal processing, scientific computing, and inverse problems. Other topics of interest include mathematical optimization and information theory.

Dr. Candès received the Third Popov Prize in Approximation Theory and was selected as an Alfred P. Sloan Research Fellow in 2001. He received the DOE Young Investigator Award in 2002. He coauthored a paper that won the Best Paper Award of the European Association for Signal, Speech, and Image Processing (EURASIP) in 2003. In 2005, he was awarded the James H. Wilkinson Prize in Numerical Analysis and Scientific Computing by the Society for Industrial and Applied Mathematics (SIAM). In 2006, he won the U.S. National Science Foundation's Alan T. Waterman Award. In 2008, he received the 2008 Information Theory Society Paper Award. He has given plenary and keynote addresses at major international conferences, including plenary and keynote talks at the 2007 International Congress of Industrial and Applied Mathematics in 2007, the 2007 IEEE International Conference on Image Processing, and the Courant Lectures at New York University.

Terence Tao received the B.Sc. (Hons.) and M.Sc. degrees in mathematics from Flinders University, Adelaide, Australia, in 1991 and 1992, respectively, and the Ph.D. degree in mathematics from Princeton University, Princeton, NJ, in 1996.

From 1996 to present, he was first a Hedrick Assistant Professor, then full Professor at the University of California, Los Angeles. He has also held shorter positions at the University of New South Wales, Australian National University, and at the Clay Mathematical Institute. His research interests include harmonic analysis (both pure and applied), partial differential equations, number theory, combinatorics (both enumerative and analytical), and representation theory.

Dr. Tao received the Salem prize in 2000 for work in harmonic analysis; the Bocher prize in 2002 for work in partial differential equations; the Clay Research Award in 2003 for work in harmonic analysis, partial differential equations, and combinatorics; and the Levi L. Conant Award in 2004 for mathematical exposition. He is currently supported by a grant from the Packard foundation. He was awarded the Fields Medal in 2006. He received the U.S. National Science Foundation's Alan T. Waterman Award in 2008. He is a member of the U.S. National Academy of Sciences and a member of the American Academy of Arts and Sciences.