Asymptotic Enumeration of Binary Matrices with Bounded Row and Column Weights

Erik Ordentlich, Farzad Parvaresh, Ron M. Roth,

HP Laboratories
HPL-2011-239

Keyword(s):

Asymptotic enumeration; Laplace's method of integration; Majorization; Weight constrained arrays; two-dimensional coding;

Abstract:

Consider the set $\Aset_n$ of all $n \times n$ binary matrices in which the number of 1's in each row and column is at most $n/2$. We show that the redundancy, $n^2 - \log_2 |\Aset_n|$, of this set equals $
ho n - \delta \sqrt{n} + O(\log n)$, for a constant $
ho \approx 1.42515$, and $\delta = \delta(n) \approx 1.46016$ for even n and 0 otherwise.

External Posting Date: December 8, 2011 [Fulltext] Approved for External Publication

Internal Posting Date: December 8, 2011 [Fulltext]

Asymptotic Enumeration of Binary Matrices with Bounded Row and Column Weights*

Erik Ordentlich† Farzad Parvaresh† Ron M. Roth‡

November 30, 2011

Abstract

Consider the set $\mathcal{A}_n$ of all $n \times n$ binary matrices in which the number of 1's in each row and column is at most $n/2$. We show that the redundancy, $n^2 - \log_2 |\mathcal{A}_n|$, of this set equals $\rho n - \delta\sqrt{n} + O(\log n)$, for a constant $\rho \approx 1.42515$, and $\delta = \delta(n) \approx 1.46016$ for even n and 0 otherwise.

Keywords: Asymptotic enumeration, Laplace's method of integration, Majorization, Weight constrained arrays, Two-dimensional coding.

AMS subject classifications: 05A16, 05C30, 60F10, 94A17.

1 Introduction

Let $\mathcal{A}_n$ denote the set of all $n \times n$ binary matrices in which the number of 1's in each row and column is at most $n/2$. The main contribution of this paper is providing an asymptotic expression for the redundancy, $n^2 - \log_2 |\mathcal{A}_n|$, of the set $\mathcal{A}_n$. Specifically, we prove the following theorem; hereafter, $Q(\cdot)$ denotes the cumulative distribution function of the normal distribution $\mathcal{N}(0,1)$, namely, $Q(x) = (1/\sqrt{2\pi}) \int_{-\infty}^{x} e^{-z^2/2}\, dz$. Let

$$x_0 = \text{argmax}_x \left\{ Q(x) e^{-x^2/2} \right\} , \tag{1}$$

*The work of E. Ordentlich and R. M. Roth was supported in part by Grant No. 2008058 from the United-States–Israel Binational Science Foundation. This work was presented in part at the 2011 International Symposium on Information Theory (ISIT), St. Petersburg, Russia.

†Hewlett–Packard Laboratories, 1501 Page Mill Rd., Palo Alto, CA 94304, USA (erik.ordentlich@hp.com, farzad.parvaresh@hp.com).

‡Computer Science Department, Technion, Haifa 32000, Israel. Work was done in part while visiting Hewlett–Packard Laboratories, Palo Alto, CA 94304, USA (ronny@cs.technion.ac.il).

which is not hard to see is a unique (finite) extremum and is positive. Also, define

$$\rho = -2\log_2\bigl(Q(x_0)e^{-x_0^2/2}\bigr) \ (\approx 1.42515) \tag{2}$$

and

$$\delta = \delta(n) = \begin{cases} 0 & \text{for odd } n \\ 2x_0/\ln 2 \quad (\approx 1.46016) & \text{for even } n \end{cases} . \tag{3}$$

Theorem 1. *With ρ and $\delta = \delta(n)$ as in (2) and (3),*

$$|\mathcal{A}_n| = 2^{n^2-\rho n+\delta\sqrt{n}} \cdot n^{O(1)} ,$$

namely, the redundancy of $\mathcal{A}_n$ equals $\rho n - \delta\sqrt{n} + O(\log n)$.

Remark 1. Throughout the paper, the implicit constants in "big-O" notation, e.g., $O(f(n))$, can be taken to be absolute, in the sense that no hidden dependencies on other parameters or on n must be met. The notation $o(1)$ will stand for an expression that goes to 0 as n goes to infinity. □

Our study of the redundancy of $\mathcal{A}_n$ is motivated, in part, by the potential application of coding arbitrary binary sequences into elements of $\mathcal{A}_n$. Such coding schemes, in turn, may be used for limiting parasitic current in next generation memory technologies based on crossbar arrays of resistive devices [1] (see also [2]). Coding schemes into $\mathcal{A}_n$ are presented in [3]; while these schemes have efficient implementation, their redundancy is $2n$.

We mention the related problem of computing the redundancy of the set $\mathcal{S}_n$ which consists of all matrices in $\mathcal{A}_n$ that are also symmetric and have an all-zero main diagonal. This problem was studied in [4] and [5], and the size of $|\mathcal{S}_n|$, when divided by $2^{n(n-1)/2}$, was shown (in [5]) to be asymptotic to $2^{-\rho n/2+\delta(2)\sqrt{n}}$, for even n, and to $2^{-(\rho n+\delta(2)\sqrt{n})/2}$, for odd n, where ρ and $\delta(\cdot)$ are as in (2) and (3). In fact, the results of [4] and [5] apply more generally to sets of symmetric matrices where the number of 1's in each row (and column) is at most a prescribed integer $d = n/2 + O(n^{1/2+\varepsilon})$, and for each such d, the set size was computed therein to within a multiplicative factor that goes to 1 as n goes to infinity.

As it turns out, there is also a close connection between the size of $\mathcal{A}_n$ and the number of stable points of infinite-range spin glass memory, which also can be related to stable points of Hopfield Memory [6]. In [7], the authors consider the following spin-glass model. A spin glass can be seen as a real n-vector $\boldsymbol{\sigma} = (\sigma_1\,\sigma_2\,\ldots\,\sigma_n)$ whose entries are the spins taking on ± 1; the interaction between the spins is represented by a symmetric $n \times n$ matrix $J = (J_{i,j})$, whose entries above the main diagonal are independently identically distributed (i.i.d.) $\mathcal{N}(0,1)$ and the main diagonal is all-zero. Each spin value σ_i changes to a new value σ_i' according to the rule:

$$\sigma_i' = \operatorname{sgn}\Bigl(\sum_{j=1}^{n} J_{i,j}\sigma_j\Bigr) , \quad i = 1, 2, \ldots, n , \tag{4}$$

where $\mathrm{sgn}(\cdot)$ is the sign function. It is shown in [7] that the expected number of the fixed points of (4) (where $\boldsymbol{\sigma}' = \boldsymbol{\sigma}$) is asymptotic to $\eta \cdot 2^{n(1-(\rho/2))}$, where $\eta \approx 1.0505$ and ρ is—again—the very same constant (2). In fact, some parts of our proof of Theorem 1 were inspired by [7].

The rest of this paper is devoted to proving Theorem 1. We split the proof into proving lower and upper bounds on the size of $\mathcal{A}_n$, in Sections 2 and 3, respectively. Section 3 also includes a comparison between the actual size of $\mathcal{A}_n$ and the asymptotic expression of Theorem 1, for small n. The proofs of our bounds make use of a strong result by Canfield *et al.* [8], who gave an asymptotically tight expression for the number of $n \times n$ binary matrices with row sums equaling prescribed integers $s_1, s_2, \ldots, s_n$ and column sums equaling $t_1, t_2, \ldots, t_n$, provided that the values s_i (respectively, t_j) are sufficiently close to each other (in a well-defined sense to be recalled in Theorem 3 below). A key ingredient in the proof of our lower bound consists of estimating the sum of the expressions of [8] over (sufficiently many) values of s_i and t_j that satisfy the conditions of [8] yet do not exceed $n/2$. The proof of our upper bound is based, in part, on controlling the error term incurred to the expression of [8] when the values s_i and t_j are skewed to violate the conditions required in [8]. We give one proof based on the "switching" technique of [5] and sketch another proof based on a majorization inequality that may be of independent interest.

2 Lower bound on the size of $\mathcal{A}_n$

This section contains the proof of the following lower bound.

Theorem 2.

$$|\mathcal{A}_n| \geqslant 2^{n^2-\rho n+\delta\sqrt{n}} \cdot n^{O(1)} \,,$$

where ρ and $\delta = \delta(n)$ are given by (2) and (3).

2.1 Preliminaries

We start by quoting a specialized version of the result of Canfield *et al.* [8]. For non-negative integer vectors $\boldsymbol{s} = (s_1\, s_2\, \ldots\, s_n)$ and $\boldsymbol{t} = (t_1\, t_2\, \ldots\, t_n)$ such that $\sum_{i=1}^n s_i = \sum_{j=1}^n t_j$, let $\mathcal{B}(\boldsymbol{s}, \boldsymbol{t})$ denote the set of all $n \times n$ binary matrices with row sums equal to $\boldsymbol{s}$ and column sums equal to $\boldsymbol{t}$.

Theorem 3. *Given such $\boldsymbol{s}$ and $\boldsymbol{t}$, write $\mu = (1/n)\sum_{i=1}^n s_i$ $\big(= (1/n)\sum_{j=1}^n t_j\big)$, $\lambda = \mu/n$, $A = \frac{1}{2}\lambda(1-\lambda)$, $R = \sum_{i=1}^n (s_i - \mu)^2$, and $C = \sum_{j=1}^n (t_j - \mu)^2$. There exists a sufficiently small*

positive absolute constant ε_0 $(< \frac{1}{2})$ *such that*

$$|\mathcal{B}(\boldsymbol{s},\boldsymbol{t})| = \binom{n^2}{\lambda n^2}^{-1} \prod_{i=1}^{n} \binom{n}{s_i} \prod_{j=1}^{n} \binom{n}{t_j} \times \exp\left\{ -\frac{1}{2}\Big(1 - \frac{R}{2An^2}\Big)\Big(1 - \frac{C}{2An^2}\Big) + O(n^{-\frac{1}{4}}) \right\} , \qquad (5)$$

whenever $\boldsymbol{s}$ *and* $\boldsymbol{t}$ *satisfy the following three conditions for some positive* $\gamma = \gamma(n) = O(n^{\varepsilon_0})$*:*

(i) $|s_i - \mu| \leqslant \gamma\sqrt{n}$ *for all* i*;*

(ii) $|t_j - \mu| \leqslant \gamma\sqrt{n}$ *for all* j*;*

(iii) $\lambda = 1/2 - o(1)$*.*

Remark 2. It can be verified that condition (iii) implies a set of weaker conditions involving λ and A in the original statement of this theorem in [8]. In addition, we note that conditions (i)–(iii) imply that the expression in the argument of $\exp\{\cdot\}$ in (5) equals $O(\gamma^4)$. □

Henceforth in this paper, we will assume that $\gamma = \gamma(n)$ is a positive function that is $O(n^{\varepsilon_0})$. At certain steps of the analysis (in Section 3, as well) we will specialize to γ of the form

$$\gamma_0(n) = \Theta(1) \cdot \sqrt{\ln n} \, , \qquad (6)$$

where $\Theta(1)$ here stands for a term that is bounded from below and from above by sufficiently large absolute constants as $n \to \infty$, to ensure that certain error terms arising in the proofs vanish sufficiently rapidly.

For γ as in (6), we will bound $|\mathcal{A}_n|$ from below by summing $|\mathcal{B}(\boldsymbol{s},\boldsymbol{t})|$ over pairs $(\boldsymbol{s},\boldsymbol{t})$ that satisfy conditions (i)–(iii) of Theorem 3, with the additional requirement that no entry in $\boldsymbol{s}$ or $\boldsymbol{t}$ exceeds $n/2$.

We establish now some notation that will be used throughout the paper. For $\boldsymbol{u} = (u_1\, u_2\, \ldots\, u_n)$ in $\mathbb{R}^n$, let $\|\boldsymbol{u}\|_p$ denote the value $(\sum_{i=1}^n u_i^p)^{1/p}$ (this value may be negative for odd p if $\boldsymbol{u}$ has negative components). We will write $|\boldsymbol{u}|$ for $\|\boldsymbol{u}\|_1$ and $\|\boldsymbol{u}\|$ for $\|\boldsymbol{u}\|_2$.

Denote by $\mathbf{1}$ the all-one vector in $\mathbb{Z}^n$ and let $\Lambda = \Lambda_n$ be the following (shifted) n-dimensional integer lattice:

$$\Lambda = \Lambda_n = \begin{cases} \mathbb{Z}^n + (1/2)\cdot\mathbf{1} & \text{for odd } n \, , \\ \mathbb{Z}^n & \text{for even } n \end{cases} .$$

Define

$$\Delta = \Delta_n = \Lambda_n \cap [0, n/2]^n$$

and

$$\mathrm{T} = \mathrm{T}_n = \Big\{ (\boldsymbol{u},\boldsymbol{v}) \in \Delta \times \Delta \, : \, |\boldsymbol{u}| = |\boldsymbol{v}| \Big\} .$$

Clearly,

$$\mathcal{A}_n = \bigcup_{(\boldsymbol{u},\boldsymbol{v})\in \mathrm{T}} \mathcal{B}\big((n/2)\cdot\mathbf{1}-\boldsymbol{u}, (n/2)\cdot\mathbf{1}-\boldsymbol{v}\big) \ .$$

For $(\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}$, define the values $B(\boldsymbol{u},\boldsymbol{v})$ and $F(\boldsymbol{u})$ by

$$B(\boldsymbol{u},\boldsymbol{v}) = \binom{n^2}{n^2/2+|\boldsymbol{u}|}^{-1} \prod_{i=1}^{n} \binom{n}{n/2+u_i} \prod_{j=1}^{n} \binom{n}{n/2+v_j}$$

and

$$F(\boldsymbol{u}) = \frac{e^{|\boldsymbol{u}|^2/n^2 - 2\|\boldsymbol{u}\|^2/n}}{(2\pi n)^{n/2}} \ .$$

Let

$$\Delta^* = \Delta_n^*(\gamma) = \Lambda_n \cap [0, \gamma\sqrt{n}]^n$$

and

$$\mathrm{T}^* = \mathrm{T}_n^*(\gamma) = \Big\{(\boldsymbol{u},\boldsymbol{v}) \in \Delta^* \times \Delta^* \ : \ |\boldsymbol{u}| = |\boldsymbol{v}|\Big\} \ ,$$

and define the subset $\mathcal{A}_n^* \subseteq \mathcal{A}_n$ by

$$\mathcal{A}_n^* = \mathcal{A}_n^*(\gamma) = \bigcup_{(\boldsymbol{u},\boldsymbol{v})\in \mathrm{T}^*} \mathcal{B}\big((n/2)\cdot\mathbf{1}-\boldsymbol{u}, (n/2)\cdot\mathbf{1}-\boldsymbol{v}\big)$$

(where n is assumed to be sufficiently large so that $\gamma\sqrt{n} \leqslant n/2$).

Next, partition Δ^* into

$$\Delta' = \Big\{\boldsymbol{u} \in \Delta^* \ : \ \|\boldsymbol{u}\|_4^4 \leqslant \gamma^2 n^3\Big\} \quad \text{and} \quad \Delta'' = \Delta^* \setminus \Delta' \ ;$$

we note for future reference that by the Cauchy–Schwarz inequality, for every $\boldsymbol{u} \in \Delta'$ we have

$$\|\boldsymbol{u}\|^2 \leqslant \|\boldsymbol{u}\|_4^2 \sqrt{n} \leqslant \gamma n^2 \tag{7}$$

and

$$|\boldsymbol{u}| \leqslant \|\boldsymbol{u}\|\sqrt{n} \leqslant \gamma^{1/2} n^{3/2} \ . \tag{8}$$

Finally, partition T^* into

$$\mathrm{T}' = (\Delta' \times \Delta') \cap \mathrm{T}^* \quad \text{and} \quad \mathrm{T}'' = \mathrm{T}^* \setminus \mathrm{T}' \ ,$$

and, respectively, partition $\mathcal{A}_n^*$ into

$$\mathcal{A}_n' = \mathcal{A}_n'(\gamma) = \bigcup_{(\boldsymbol{u},\boldsymbol{v})\in \mathrm{T}'} \mathcal{B}\big((n/2)\cdot\mathbf{1}-\boldsymbol{u}, (n/2)\cdot\mathbf{1}-\boldsymbol{v}\big)$$

and

$$\mathcal{A}''_n = \mathcal{A}''_n(\gamma) = \bigcup_{(\boldsymbol{u},\boldsymbol{v})\in \mathrm{T}''} \mathcal{B}\big((n/2)\cdot\mathbf{1}-\boldsymbol{u}, (n/2)\cdot\mathbf{1}-\boldsymbol{v}\big) \ .$$

In the sequel, some error terms in the analysis will be present due to the subset $\mathcal{A}''_n$; therefore, part of the effort in our proof will be put into showing that this "bad" subset is much smaller than $\mathcal{A}^*_n$.

The rest of Section 2 is devoted to proving the next proposition which, in turn, immediately implies Theorem 2.

Proposition 4. *With $\gamma = \gamma_0(n)$ as in (6),*

$$|\mathcal{A}^*_n| = 2^{n^2-\rho n+\delta\sqrt{n}} \cdot n^{O(1)} \ .$$

We prove Proposition 4 in the upcoming subsections, through a sequence of lemmas.

2.2 First set of approximations

We start with the next lemma, which provides an approximation for $B(\boldsymbol{u},\boldsymbol{v})$ in terms of $F(\boldsymbol{u})$ and $F(\boldsymbol{v})$.

Lemma 5. *For every $(\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}^*$,*

$$\frac{B(\boldsymbol{u},\boldsymbol{v})}{2^{n^2+2n}F(\boldsymbol{u})F(\boldsymbol{v})} = \begin{cases} e^{O(\gamma^2)} & \text{if } (\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}' \\ e^{O(\gamma^4)} & \text{if } (\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}'' \end{cases} \ .$$

Proof. We approximate the factorials in $B(\boldsymbol{u},\boldsymbol{v})$ using Stirling's formula [9]:

$$w! = \sqrt{2\pi w}\left(\frac{w}{e}\right)^w e^{\theta/(12w)} \ , \quad \text{where } 1-1/(12w+1) < \theta < 1 \ . \tag{9}$$

After some simplification, we can write $B(\boldsymbol{u},\boldsymbol{v})$ as

$$\begin{aligned} B(\boldsymbol{u},\boldsymbol{v}) \ &= \ \Theta(1)\cdot(2\pi)^{1/2-n}\cdot\frac{(n^2/2-|\boldsymbol{u}|)^{n^2/2-|\boldsymbol{u}|+1/2}\,(n^2/2+|\boldsymbol{u}|)^{n^2/2+|\boldsymbol{u}|+1/2}}{n^{2n^2+1}} \\ &\quad\times\prod_{i=1}^{n}\frac{n^{1/2+n}}{(n/2-u_i)^{n/2-u_i+1/2}(n/2+u_i)^{n/2+u_i+1/2}} \\ &\quad\times\prod_{j=1}^{n}\frac{n^{1/2+n}}{(n/2-v_j)^{n/2-v_j+1/2}(n/2+v_j)^{n/2+v_j+1/2}} \ . \end{aligned} \tag{10}$$

Namely, all of the exponential terms in Stirling's approximation cancel out and the constant factor $\Theta(1)$ $(= (1+o(1))/\sqrt{e})$ collects the error terms $e^{\theta/12w}$, where w is at least $n/2-o(n)$ in all cases for $(\boldsymbol{u},\boldsymbol{v})$ in T^*.

Next, consider the Taylor expansion of $x \mapsto (c+x+1/2)\ln(c+x)$ about $x=0$:

$$\begin{aligned}\Big(c+x+\frac{1}{2}\Big)\ln(c+x) \;&=\; \Big(c+\frac{1}{2}\Big)\ln c + \Big(1+\frac{1}{2c}+\ln c\Big)x \\ &\quad + \Big(-\frac{1}{2c^2}+\frac{1}{c}\Big)\frac{x^2}{2} + \Big(\frac{1}{c^3}-\frac{1}{c^2}\Big)\frac{x^3}{6} \\ &\quad + \Big(-\frac{1}{2(c+\xi)^4}+\frac{1}{3(c+\xi)^3}\Big)\frac{x^4}{4}\,, \end{aligned} \tag{11}$$

where $\xi \in [0,x]$ if $x \geqslant 0$ and $\xi \in [x,0]$ if $x<0$. We can apply this expansion to the various terms of this form appearing in the logarithm of (10) with c equal to either $n^2/2$ or $n/2$. The linear and cubic terms are identical except for sign for the approximations involving the terms $n^2/2 \pm |\boldsymbol{u}|$ and thus cancel out, and the same holds for the terms $n/2 \pm u_i$ and $n/2 \pm v_i$. Concerning the other terms, it can be readily verified that because $u_i, v_j \leqslant \gamma\sqrt{n}$ (and hence $|\boldsymbol{u}| = |\boldsymbol{v}| \leqslant \gamma n^{3/2}$) for $(\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}^*$, the only terms that result in contributions of magnitude greater than $O(\gamma^2)$ are $2|\boldsymbol{u}|^2/n^2 - 2\|\boldsymbol{u}\|^2/n - 2\|\boldsymbol{v}\|^2/n$ and

$$O\Big(|\boldsymbol{u}|^4/n^6 - \|\boldsymbol{u}\|_4^4/n^3 - \|\boldsymbol{v}\|_4^4/n^3\Big)\,.$$

The latter expression is $O(\gamma^4)$ for every $(\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}^*$; furthermore, by the definition of T' and by (8), it is $O(\gamma^2)$ for $(\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}'$. Collecting terms and simplifying completes the proof. □

Lemma 6.

$$|\mathcal{A}_n^*| = \Big(e^{O(\gamma^2)} \cdot 2^{n^2+2n} \cdot \sum_{(\boldsymbol{u},\boldsymbol{v})\in\mathrm{T}^*} F(\boldsymbol{u})F(\boldsymbol{v})\Big) + E_n(\gamma)\,, \tag{12}$$

where

$$-e^{O(\gamma^4)} \cdot |\mathcal{A}_n''| \leqslant E_n(\gamma) \leqslant |\mathcal{A}_n''|\,.$$

Proof. For every $(\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}^*$, the vector pair $(\boldsymbol{s},\boldsymbol{t}) = ((n/2)\cdot\mathbf{1}-\boldsymbol{u}, (n/2)\cdot\mathbf{1}-\boldsymbol{v})$ satisfies conditions (i)–(iii) of Theorem 3 (with $|\boldsymbol{u}| = n^2/2 - n^2\lambda$). Therefore, by that theorem,

$$\frac{\big|\mathcal{B}\big((n/2)\cdot\mathbf{1}-\boldsymbol{u}, (n/2)\cdot\mathbf{1}-\boldsymbol{v}\big)\big|}{B(\boldsymbol{u},\boldsymbol{v})} = \begin{cases} e^{O(\gamma^2)} & \text{if } (\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}' \\ e^{O(\gamma^4)} & \text{if } (\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}'' \end{cases},$$

where we recall that the argument of $\exp\{\cdot\}$ in (5) is $e^{O(\gamma^4)}$ whenever conditions (i)–(iii) are satisfied; furthermore, by (7), that argument is $e^{O(\gamma^2)}$ for $(\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}'$. Hence, by Lemma 5 we get that

$$|\mathcal{A}_n'| = e^{O(\gamma^2)} \cdot 2^{n^2+2n} \cdot \sum_{(\boldsymbol{u},\boldsymbol{v})\in\mathrm{T}'} F(\boldsymbol{u})F(\boldsymbol{v})$$

and

$$|\mathcal{A}_n''| = e^{O(\gamma^4)} \cdot 2^{n^2+2n} \cdot \sum_{(\boldsymbol{u},\boldsymbol{v})\in\mathrm{T}''} F(\boldsymbol{u})F(\boldsymbol{v})\,.$$

The result follows. □

To compute the expression in the right-hand size of (12), we need to do the summation over all vectors $(\boldsymbol{u}, \boldsymbol{v})$ in the set T^*. The next lemma shows that, in fact, we still get a good approximation even if we sum over the larger set $\Delta^* \times \Delta^*$ instead.

Lemma 7.

$$\Big(\sum_{\boldsymbol{u}\in\Delta^*} F(\boldsymbol{u})\Big)^2 \geqslant \sum_{(\boldsymbol{u},\boldsymbol{v})\in\mathrm{T}^*} F(\boldsymbol{u})F(\boldsymbol{v}) \geqslant \frac{1}{\gamma n^{3/2}+1}\Big(\sum_{\boldsymbol{u}\in\Delta^*} F(\boldsymbol{u})\Big)^2 .$$

Proof. The first inequality is obvious. To prove the second inequality, we define for any rational ℓ the sum

$$D(\ell) \stackrel{\text{def}}{=} \sum_{\boldsymbol{u}\in\Delta^* : |\boldsymbol{u}|=\ell} F(\boldsymbol{u}) ,$$

and we denote by $\mathcal{L}$ the set of all values ℓ for which $D(\ell)$ is strictly positive. By the Cauchy–Schwarz inequality,

$$\sum_{\ell\in\mathcal{L}} (D(\ell))^2 \geqslant \frac{1}{|\mathcal{L}|}\Big(\sum_{\ell\in\mathcal{L}} D(\ell)\Big)^2 .$$

The result follows by noting that $|\mathcal{L}| \leqslant \gamma n^{3/2}+1$. □

2.3 Approximating sums by integrals

We now turn to approximating the sum, $\sum_{\boldsymbol{u}\in\Delta^*} F(\boldsymbol{u})$, which appears in Lemma 7.

Let

$$\mathscr{R}^* = \mathscr{R}^*_n(\gamma) = \begin{cases} [0, \gamma\sqrt{n}]^n & \text{for odd } n , \\ [-\frac{1}{2}, \gamma\sqrt{n}]^n & \text{for even } n , \end{cases} \tag{13}$$

where we add hereafter in Section 2 the assumption that γ is such that $\gamma\sqrt{n}$ (respectively, $\gamma\sqrt{n} - \frac{1}{2}$) is an integer for odd (respectively, even) n; note that this assumption can hold also when γ is taken as $\gamma_0(n)$ in (6).

Lemma 8.

$$\sum_{\boldsymbol{u}\in\Delta^*} F(\boldsymbol{u}) = e^{O(\gamma^2)} \int_{\boldsymbol{u}\in\mathscr{R}^*} F(\boldsymbol{u})\, d\boldsymbol{u} .$$

Proof. For any $\boldsymbol{r} \in \mathbb{R}^n$ there are unique vectors $\boldsymbol{u} = \boldsymbol{u}(\boldsymbol{r}) \in \Lambda$ and $\boldsymbol{\omega} = \boldsymbol{\omega}(\boldsymbol{r}) \in [-\frac{1}{2}, \frac{1}{2})^n$ such that $\boldsymbol{r} = \boldsymbol{u} + \boldsymbol{\omega}$. Define $f : \mathbb{R}^n \to \mathbb{R}$ by

$$f(\boldsymbol{r}) = \exp\left\{ \frac{|\boldsymbol{u}|^2}{n^2} - \frac{2\|\boldsymbol{u}\|^2}{n} + \frac{2|\boldsymbol{u}|\cdot|\boldsymbol{\omega}|}{n^2} - \frac{4\langle \boldsymbol{u}, \boldsymbol{\omega}\rangle}{n} \right\} ,$$

where $\langle \cdot, \cdot \rangle$ stands for inner product. Next, we express the integral $\int_{\boldsymbol{r}\in\mathscr{R}^*} f(\boldsymbol{r})\, d\boldsymbol{r}$ in two different ways.

On the one hand, we can write

$$\begin{aligned}\int_{\boldsymbol{r}\in\mathscr{R}^*} f(\boldsymbol{r})\,d\boldsymbol{r} &= \sum_{\boldsymbol{u}\in\Delta^*}\left(\int_{\boldsymbol{\omega}\in[-\frac{1}{2},\frac{1}{2})^n} e^{|\boldsymbol{u}|^2/n^2-2\|\boldsymbol{u}\|^2/n+2|\boldsymbol{u}|\cdot|\boldsymbol{\omega}|/n^2-4\langle\boldsymbol{u},\boldsymbol{\omega}\rangle/n}\,d\boldsymbol{\omega}\right)\\ &= \sum_{\boldsymbol{u}\in\Delta^*}\left(e^{|\boldsymbol{u}|^2/n^2-2\|\boldsymbol{u}\|^2/n}\int_{\boldsymbol{\omega}\in[-\frac{1}{2},\frac{1}{2})^n} e^{2|\boldsymbol{u}|\cdot|\boldsymbol{\omega}|/n^2-4\langle\boldsymbol{u},\boldsymbol{\omega}\rangle/n}\,d\boldsymbol{\omega}\right),\end{aligned}$$

and for every $\boldsymbol{u}\in\Delta^*$,

$$\begin{aligned}\int_{\boldsymbol{\omega}\in[-\frac{1}{2},\frac{1}{2})^n} e^{2|\boldsymbol{u}|\cdot|\boldsymbol{\omega}|/n^2-4\langle\boldsymbol{u},\boldsymbol{\omega}\rangle/n}\,d\boldsymbol{\omega} &= \prod_{i=1}^{n}\Big(\int_{\omega_i=-1/2}^{1/2} e^{(2|\boldsymbol{u}|/n^2-4u_i/n)\omega_i}\,d\omega_i\Big)\\ &= \prod_{i=1}^{n}\frac{\sinh\left(|\boldsymbol{u}|/n^2-2u_i/n\right)}{|\boldsymbol{u}|/n^2-2u_i/n}\,.\end{aligned}$$

For $\boldsymbol{u}\in\Delta^*$, we have $|\boldsymbol{u}|/n^2-2u_i/n=O(\gamma/\sqrt{n})$, so,

$$\prod_{i=1}^{n}\frac{\sinh\left(|\boldsymbol{u}|/n^2-2u_i/n\right)}{|\boldsymbol{u}|/n^2-2u_i/n}=\prod_{i=1}^{n}\Big(1+O\big((|\boldsymbol{u}|/n^2-2u_i/n)^2\big)\Big)=\big(1+O(\gamma^2/n)\big)^n=e^{O(\gamma^2)}\,, \tag{14}$$

and, therefore,

$$\int_{\boldsymbol{r}\in\mathscr{R}^*} f(\boldsymbol{r})\,d\boldsymbol{r}=e^{O(\gamma^2)}\sum_{\boldsymbol{u}\in\Delta^*} e^{|\boldsymbol{u}|^2/n^2-2\|\boldsymbol{u}\|^2/n}\,. \tag{15}$$

On the other hand, we observe that $f(\boldsymbol{r})$ can be written as

$$f(\boldsymbol{r})=\exp\left\{\frac{|\boldsymbol{r}|^2}{n^2}-\frac{2\|\boldsymbol{r}\|^2}{n}-\frac{|\boldsymbol{\omega}|^2}{n^2}+\frac{2\|\boldsymbol{\omega}\|^2}{n}\right\}=\exp\left\{\frac{|\boldsymbol{r}|^2}{n^2}-\frac{2\|\boldsymbol{r}\|^2}{n}+O(1)\right\}\,,$$

which implies that

$$\int_{\boldsymbol{r}\in\mathscr{R}^*} f(\boldsymbol{r})\,d\boldsymbol{r}=\Theta(1)\cdot\int_{\boldsymbol{r}\in\mathscr{R}^*} e^{|\boldsymbol{r}|^2/n^2-2\|\boldsymbol{r}\|^2/n}\,d\boldsymbol{r}\,.$$

Combining the latter equation with (15) completes the proof. □

Let $\boldsymbol{U}$ be an n-dimensional jointly normal random vector with zero mean and with the $n\times n$ covariance matrix

$$\Sigma=\frac{1}{4}\left(nI+\mathbf{1}\cdot\mathbf{1}^t\right)\,. \tag{16}$$

It is easy to verify that $\det(\Sigma)=2^{1-2n}n^n$ and that

$$\Sigma^{-1}=\frac{4}{n}\left(I-\frac{\mathbf{1}\cdot\mathbf{1}^t}{2n}\right)\,,$$

and, so, $-\boldsymbol{u}^t\Sigma^{-1}\boldsymbol{u}/2 = |\boldsymbol{u}|^2/n^2 - 2\|\boldsymbol{u}\|/n$ for every $\boldsymbol{u} \in \mathbb{R}^n$. Hence, for $\mathscr{R}^*$ as defined in (13),

$$\mathsf{Pr}\{\boldsymbol{U} \in \mathscr{R}^*\} = \frac{1}{\sqrt{\det(2\pi\Sigma)}} \int_{\boldsymbol{u}\in\mathscr{R}^*} e^{-\boldsymbol{u}^t\Sigma^{-1}\boldsymbol{u}/2}\, d\boldsymbol{u} = 2^{n-1/2} \int_{\boldsymbol{u}\in\mathscr{R}^*} F(\boldsymbol{u})\, d\boldsymbol{u} \ .$$

It follows from Lemmas 7 and 8 that

$$\sum_{(\boldsymbol{u},\boldsymbol{v})\in \mathrm{T}^*} F(\boldsymbol{u})F(\boldsymbol{v}) = (\gamma n)^{O(1)} \cdot e^{O(\gamma^2)} \cdot 2^{-2n} \cdot \left(\mathsf{Pr}\{\boldsymbol{U} \in \mathscr{R}^*\}\right)^2 \ . \tag{17}$$

Next, we compute estimates of the probability in (17).

Lemma 9. *With x_0, ρ, and $\delta = \delta(n)$ as in (1)–(3) and $\gamma = \gamma_0(n)$ as in (6),*

$$\mathsf{Pr}\{\boldsymbol{U} \in \mathscr{R}^*\} = (1 + o(1)) \cdot \alpha \cdot 2^{-(\rho n - \delta\sqrt{n})/2} \ ,$$

where, for $\beta_0 = 1/\sqrt{2x_0^2 + 1}$,

$$\alpha = \alpha(n) = \begin{cases} \beta_0 & (\approx 0.81320) \quad \textit{for odd } n \\ \beta_0 \cdot e^{(\beta_0^2-1)/2} & (\approx 0.68651) \quad \textit{for even } n \end{cases} \ .$$

Proof. We borrow the idea of [7] of "simulating" the random vector $\boldsymbol{U}$ through an $(n+1)$-dimensional random vector $\boldsymbol{Y} = (Y_0\, Y_1\, Y_2\, \ldots\, Y_n)$ whose entries are i.i.d. $\mathcal{N}(0,1)$. Specifically, let $\boldsymbol{V} = (V_1\, V_2\, \ldots\, V_n)$ be a random vector function of $\boldsymbol{Y}$ defined as follows:

$$V_i = \frac{1}{2}\left(\sqrt{n} \cdot Y_i + Y_0\right) \ , \quad i = 1, 2, \ldots, n \ . \tag{18}$$

Clearly, $\boldsymbol{V}$ is a zero-mean jointly normal vector, and a simple calculation reveals that it has the same covariance matrix Σ as $\boldsymbol{U}$; hence, $\boldsymbol{V}$ and $\boldsymbol{U}$ have precisely the same distribution. Next, we distinguish between odd and even values of n.

Case 1: odd n. Conditioning on $Y_0 = y$, the entries of $\boldsymbol{V}$ become statistically independent and identically distributed, and, so,

$$\mathsf{Pr}\{\boldsymbol{V} \in \mathscr{R}^* \,|\, Y_0 = y\} = \left[Q\left(2\gamma - \frac{y}{\sqrt{n}}\right) - Q\left(\frac{-y}{\sqrt{n}}\right)\right]^n \tag{19}$$

(where $Q(x) = (1/\sqrt{2\pi}) \int_{-\infty}^{x} e^{-z^2/2}\, dz$). Hence,

$$\begin{aligned} \mathsf{Pr}\{\boldsymbol{U} \in \mathscr{R}^*\} &= \mathsf{Pr}\{\boldsymbol{V} \in \mathscr{R}^*\} \\ &= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{-y^2/2} \cdot \mathsf{Pr}\{\boldsymbol{V} \in \mathscr{R}^* \,|\, Y_0 = y\}\, dy \\ &= \sqrt{\frac{n}{2\pi}} \int_{-\infty}^{+\infty} \left[\big(Q(2\gamma - x) - Q(-x)\big) e^{-x^2/2}\right]^n dx \qquad (20) \\ &= \sqrt{\frac{n}{2\pi}} \int_{-\infty}^{+\infty} \left[\big(Q(x) - 1 + Q(2\gamma - x)\big) e^{-x^2/2}\right]^n dx \ , \qquad (21) \end{aligned}$$

where in (20) we have substituted $x = y/\sqrt{n}$, and (21) follows from the fact that $1-Q(x) = Q(-x)$. We proceed by computing lower and upper bounds on (21).

With x_0 as in (1), we can bound (21) from below by limiting the range of integration to $[x_0-c, x_0+c]$ for any finite absolute constant $c > 0$ and obtain the following chain of (in)equalities:

$$\begin{aligned}
\mathsf{Pr}\{\boldsymbol{U} \in \mathscr{R}^*\} &\geqslant \sqrt{\frac{n}{2\pi}} \int_{x_0-c}^{x_0+c} \Big[\big(Q(x) - 1 + Q(2\gamma - x)\big)e^{-x^2/2}\Big]^n dx \\
&\geqslant \sqrt{\frac{n}{2\pi}} \int_{x_0-c}^{x_0+c} \Big[Q(x)e^{-x^2/2}\big(1 - e^{-\Omega(\gamma^2)}\big)\Big]^n dx \qquad (22)\\
&= (1+o(1)) \cdot \sqrt{\frac{n}{2\pi}} \int_{x_0-c}^{x_0+c} \Big[Q(x)e^{-x^2/2}\Big]^n dx \qquad (23)\\
&= (1+o(1)) \cdot \beta_0 \cdot \Big[Q(x_0)e^{-x_0^2/2}\Big]^n \qquad (24)\\
&= (1+o(1)) \cdot \beta_0 \cdot 2^{-\rho n/2}\,; \qquad (25)
\end{aligned}$$

Eq. (22) follows from the well known upper bound (see, e.g., [10, Lemma VII.1.2])

$$1 - Q(z) \leqslant e^{-z^2/2}/(z\sqrt{2\pi})\,, \qquad (26)$$

for $z \geqslant 0$, applied to $1 - Q(2\gamma - x)$; Eq. (23) follows from our choice of $\gamma = \gamma_0(n)$ as in (6), where $\Theta(1)$ therein is taken sufficiently large for this step to hold; Eq. (24) follows from Laplace's method of integration (see e.g., [11, Theorem 8.17]), as in an analogous step in [7], where the second derivative of $x \mapsto x^2/2 - \ln Q(x)$ at $x = x_0$ can be verified to be $2x_0^2 + 1 = 1/\beta_0^2$; and, finally, (25) follows from the definition of ρ in (2).

To obtain an upper bound on $\mathsf{Pr}\{\boldsymbol{U} \in \mathscr{R}^*\}$ (for odd n), we simply drop the (non-positive) term $-1 + Q(2\gamma - x)$ from (21) and then apply Laplace's method of integration:

$$\begin{aligned}
\mathsf{Pr}\{\boldsymbol{U} \in \mathscr{R}^*\} &\leqslant \sqrt{\frac{n}{2\pi}} \int_{-\infty}^{+\infty} \Big[Q(x)e^{-x^2/2}\Big]^n dx \\
&= (1+o(1)) \cdot \beta_0 \cdot \Big[Q(x_0)e^{-x_0^2/2}\Big]^n \\
&= (1+o(1)) \cdot \beta_0 \cdot 2^{-\rho n/2}\,.
\end{aligned}$$

This completes the proof of the lemma for odd n.

Case 2: even n. The counterpart of (19) in this case takes the form

$$\mathsf{Pr}\{\boldsymbol{V} \in \mathscr{R}^* \,|\, Y_0 = y\} = \left[Q\left(2\gamma - \frac{y}{\sqrt{n}}\right) - Q\left(\frac{-1-y}{\sqrt{n}}\right)\right]^n\,,$$

which readily implies the following counterpart of (21):

$$\mathsf{Pr}\{\boldsymbol{U} \in \mathscr{R}^*\} = \sqrt{\frac{n}{2\pi}} \int_{-\infty}^{+\infty} \Big[e^{-x^2/2}\big(Q(x + 1/\sqrt{n}) - 1 + Q(2\gamma - x)\big)\Big]^n dx\,. \qquad (27)$$

Next, we shift the integration variable by an additive $1/\sqrt{n}$ and limit the integration range (as before) to $[x_0-c, x_0+c]$; this yields

$$\begin{aligned}\mathsf{Pr}\{\boldsymbol{U} \in \mathscr{R}^*\} &\geqslant \sqrt{\frac{n}{2\pi}} \int_{x_0-c}^{x_0+c} \Big[e^{-(x-1/\sqrt{n})^2/2}\big(Q(x) - 1 + Q(2\gamma + 1/\sqrt{n} - x)\big)\Big]^n dx \\ &= (1+o(1)) \cdot \sqrt{\frac{n}{2\pi e}} \int_{x_0-c}^{x_0+c} e^{\sqrt{n}\,x} \left[e^{-x^2/2} Q(x)\right]^n dx\ . \end{aligned} \tag{28}$$

We now invoke an extended form of Laplace's method of integration [12, Theorem 1] for the asymptotic behavior of the integral in (28):

$$\begin{aligned}\mathsf{Pr}\{\boldsymbol{U} \in \mathscr{R}^*\} &\geqslant \frac{1+o(1)}{\sqrt{2\pi e}} \left(\int_{-\infty}^{+\infty} e^{-z^2/(2\beta_0^2)+z}\, dz\right) \cdot e^{\sqrt{n}\,x_0} \left[e^{-x_0^2/2} Q(x_0)\right]^n \\ &= (1+o(1)) \cdot \beta_0 \cdot e^{(\beta_0^2-1)/2} \cdot 2^{-(\rho n - \delta\sqrt{n})/2}\ . \end{aligned} \tag{29}$$

Finally, to show that the expression in (29) is also an upper bound on $\mathsf{Pr}\{\boldsymbol{U} \in \mathscr{R}^*\}$, we drop the term $-1 + Q(2\gamma - x)$ from (27) and then apply the extended Laplace's method of integration. □

2.4 Bounding the effect of the bad subset

Proposition 4 will be proved by combining Lemma 6 with (17) and Lemma 9. Yet, in order to achieve this, we need to show that the additive term $E_n(\gamma)$ in (12) is negligible. We do this with the help of the following lemma.

Lemma 10.

$$|\mathcal{A}_n''| < 2^{n^2+1} \Big[e^{-1}(1 + 2/\gamma^2)\Big]^n\ .$$

Proof. Let Υ^{r} denote the union of all sets $\mathcal{B}\big((n/2)\cdot\mathbf{1}-\boldsymbol{u}, (n/2)\cdot\mathbf{1}-\boldsymbol{v}\big)$, where $(\boldsymbol{u}, \boldsymbol{v})$ ranges over

$$\Big\{(\boldsymbol{u}, \boldsymbol{v}) \in \Delta'' \times \Delta^* \,:\, |\boldsymbol{u}| = |\boldsymbol{v}|\Big\}\ .$$

Similarly, let Υ^{c} be the respective set where rows and columns switch rolls. It is easy to see that $\mathcal{A}_n'' = \Upsilon^{\mathrm{r}} \cup \Upsilon^{\mathrm{c}}$ and, so, $|\mathcal{A}_n''| \leqslant 2|\Upsilon^{\mathrm{r}}|$. We show that $|\Upsilon^{\mathrm{r}}| < 2^{n^2}\,[e^{-1}(1 + 2/\gamma^2)]^n$.

Let $(X_{i,j})_{i,j=1}^n$ be n^2 i.i.d. Bernoulli-1/2 random variables taking on $\{0, 1\}$, and let $\boldsymbol{S} = (S_1\ S_2\ \ldots\ S_n)$ be the random vector whose entries are $S_i = n/2 - \sum_{j=1}^n X_{i,j}$. We have

$$|\Upsilon^{\mathrm{r}}| \leqslant 2^{n^2} \cdot \mathsf{Pr}\Big\{\boldsymbol{S} \in \Delta''\Big\} \tag{30}$$

(the right-hand side of (30) counts matrices with no constraints on the columns).

We use the Chernoff bound to bound $\mathsf{Pr}\{\boldsymbol{S} \in \Delta''\}$ from above:

$$\begin{aligned}
\mathsf{Pr}\Big\{\boldsymbol{S} \in \Delta''\Big\} &= \mathsf{Pr}\Big\{\|\boldsymbol{S}\|_4^4 > \gamma^2 n^3 \text{ and } \boldsymbol{S} \in \Delta^*\Big\} \\
&\overset{\tau>0}{\leqslant} \mathsf{E}\Big\{e^{\tau \sum_i (S_i^4 - \gamma^2 n^2)} \prod_{i=1}^{n} \mathbb{1}\big(0 \leqslant S_i \leqslant \gamma\sqrt{n}\big)\Big\} \\
&= \left[e^{-\tau\gamma^2 n^2} \mathsf{E}\Big\{e^{\tau S_1^4} \mathbb{1}\big(0 \leqslant S_1 \leqslant \gamma\sqrt{n}\big)\Big\}\right]^n , \qquad (31)
\end{aligned}$$

where $\mathbb{1}(\cdot)$ stands for the indicator function. We continue analyzing the inner expectation in (31):

$$\begin{aligned}
\mathsf{E}\Big\{e^{\tau S_1^4} \mathbb{1}\big(0 \leqslant S_1 \leqslant \gamma\sqrt{n}\big)\Big\} &= \int_0^\infty \mathsf{Pr}\Big\{e^{\tau S_1^4} \mathbb{1}\big(0 \leqslant S_1 \leqslant \gamma\sqrt{n}\big) \geqslant x\Big\}\, dx \\
&= \int_0^\infty \mathsf{Pr}\Big\{S_1^4 \geqslant (\ln x)/\tau \text{ and } 0 \leqslant S_1 \leqslant \gamma\sqrt{n}\Big\}\, dx \\
&\leqslant 1 + \int_1^\infty \mathsf{Pr}\Big\{\gamma\sqrt{n} \geqslant S_1 \geqslant \sqrt[4]{(\ln x)/\tau}\Big\}\, dx \\
&= 1 + 4\tau \int_0^\infty \mathsf{Pr}\Big\{\gamma\sqrt{n} \geqslant S_1 \geqslant y\Big\} e^{\tau y^4} y^3\, dy \\
&= 1 + 4\tau \int_0^{\gamma\sqrt{n}} \mathsf{Pr}\Big\{\gamma\sqrt{n} \geqslant S_1 \geqslant y\Big\} e^{\tau y^4} y^3\, dy \\
&\leqslant 1 + 4\tau \int_0^{\gamma\sqrt{n}} e^{-2y^2/n + \tau y^4} y^3\, dy , \qquad (32)
\end{aligned}$$

where (32) follows from Hoeffding's inequality [14]:

$$\mathsf{Pr}\Big\{\gamma\sqrt{n} \geqslant S_1 \geqslant y\Big\} \leqslant \mathsf{Pr}\Big\{S_1 \geqslant y\Big\} \leqslant e^{-2y^2/n} .$$

Next, we compute the integral in (32) for $\tau = \gamma^{-2} n^{-2}$. For $0 \leqslant y \leqslant \gamma\sqrt{n}$ we then have

$$e^{-2y^2/n + \tau y^4} \leqslant e^{-y^2/n} .$$

Hence, the integral is bounded from above by

$$\begin{aligned}
\int_0^{\gamma\sqrt{n}} e^{-2y^2/n + \tau y^4} y^3\, dy &\leqslant \int_0^{\gamma\sqrt{n}} e^{-y^2/n} y^3\, dy \\
&= -(n/2) \cdot e^{-y^2/n} y^2 \,\Big|_0^{\gamma\sqrt{n}} + n \int_0^{\gamma\sqrt{n}} e^{-y^2/n} y\, dy \\
&< n^2/2 .
\end{aligned}$$

Plugging the latter into (32) and computing (31) for $\tau = \gamma^{-2}n^{-2}$ yields

$$\mathsf{Pr}\Big\{\boldsymbol{S} \in \Delta''\Big\} < \Big[e^{-\tau\gamma^2 n^2}(1+2n^2\tau)\Big]^n = \Big[e^{-1}(1+2/\gamma^2)\Big]^n \,. \tag{33}$$

The proof is completed by combining (33) with (30). □

Proof of Proposition 4. By combining Lemma 9 with (17) we conclude that, with $\gamma = \gamma_0(n)$ as in (6), the main term in the right-hand side of (12) equals $2^{-\rho n+\delta\sqrt{n}} \cdot n^{O(1)}$. As for the remaining term, $E_n(\gamma)$, since $e > 2^\rho$, it follows from Lemma 10 that

$$|E_n(\gamma)| \leqslant e^{O(\gamma^4)} \cdot |\mathcal{A}''_n| < 2^{n^2} e^{-n+o(n)} = o(1) \cdot 2^{n^2} 2^{-\rho n} \,,$$

namely, this term is negligible compared to the main term in (12). □

3 Upper bound on the size of $\mathcal{A}_n$

In this section, we prove the following upper bound.

Theorem 11.

$$|\mathcal{A}_n| \leqslant 2^{n^2-\rho n+\delta\sqrt{n}} \cdot n^{O(1)} \,,$$

where ρ and $\delta = \delta(n)$ are given by (2) and (3).

The problem with applying the method of the previous section to, in this case, bounding from above the summation of $|\mathcal{B}(\boldsymbol{s},\boldsymbol{t})|$ over the set of integer valued row–column sums $(\boldsymbol{s},\boldsymbol{t}) \in [0,n/2]^n \times [0,n/2]^n$ satisfying $|\boldsymbol{s}| = |\boldsymbol{t}|$ is that we must now account for $(\boldsymbol{s},\boldsymbol{t})$ that are too "skewed" and do not satisfy conditions (i)–(iii) of Theorem 3. We give two proofs of Theorem 11 that address this issue in two different ways. The first proof uses the switching technique of [5] to show that the summation of $|\mathcal{B}(\boldsymbol{s},\boldsymbol{t})|$ over those $(\boldsymbol{s},\boldsymbol{t})$ that are too skewed is negligible compared to the summation over $(\boldsymbol{s},\boldsymbol{t})$ that are not skewed (i.e., satisfy conditions (i)–(iii) of Theorem 3). The second proof, which we only sketch, is based on a new upper bound (c.f., Lemma 18 below) on $|\mathcal{B}(\boldsymbol{s},\boldsymbol{t})|$ for skewed $(\boldsymbol{s},\boldsymbol{t})$ in terms of $|\mathcal{B}(\boldsymbol{s}',\boldsymbol{t}')|$ for non-skewed $(\boldsymbol{s}',\boldsymbol{t}')$ that are *majorized* (see [13] and the discussion below) by $(\boldsymbol{s},\boldsymbol{t})$. This upper bound may be of independent interest.

3.1 Switching technique proof

In this subsection we prove the next proposition; Theorem 11 will then follow from Proposition 4.

Proposition 12. *With $\gamma = \gamma_0(n)$ as in (6),*

$$|\mathcal{A}_n| = (1 + o(1)) \cdot |\mathcal{A}_n^*| \, .$$

The proof of Proposition 12 makes use of the following definitions and lemmas.

Let

$$\Delta^\circ = \Delta_n^\circ(\gamma) = \Big\{ \boldsymbol{u} \in \Delta \, : \, |\boldsymbol{u}| \leqslant \gamma n^{3/2}/8 \Big\}$$

and

$$\mathrm{T}^\circ = (\Delta^\circ \times \Delta^\circ) \cap \mathrm{T} \, ,$$

and define the ("good") subset $\mathcal{A}_n^\circ \subseteq \mathcal{A}_n$ by

$$\mathcal{A}_n^\circ = \bigcup_{(\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}^\circ} \mathcal{B}\big((n/2)\cdot\mathbf{1} - \boldsymbol{u}, (n/2)\cdot\mathbf{1} - \boldsymbol{v}\big) \, .$$

We then have the following lemma, which implies that for sufficiently large γ, the subset $\mathcal{A}_n^\circ$ contains all but a negligible fraction of $\mathcal{A}_n$.

Lemma 13.

$$|\mathcal{A}_n \setminus \mathcal{A}_n^\circ| \leqslant 2^{n^2 - \Omega(\gamma^2 n)} \, .$$

Proof. Clearly, $\mathcal{A}_n \setminus \mathcal{A}_n^\circ$ is contained in the set of $n \times n$ binary matrices with fewer than $n^2/2 - \gamma n^{3/2}/8$ total number of 1's. The fraction of such matrices of the total number of $n \times n$ binary matrices corresponds to the probability

$$\mathsf{Pr}\bigg\{ \sum_{i,j=1}^{n} X_{i,j} \leqslant \frac{n^2}{2} - \frac{1}{8}\,\gamma n^{3/2} \bigg\} \, ,$$

where $(X_{i,j})_{i,j=1}^n$ are n^2 i.i.d. Bernoulli-1/2 random variables taking on $\{0, 1\}$. By Hoeffding's inequality [14], this probability is at most $\exp\{-\Omega(\gamma^2 n)\}$. □

Next, we shall use the switching technique of McKay, Wanless, and Wormald [5] to prove Lemma 15 below, which states that all but a negligible portion of the elements of $\mathcal{A}^\circ$ are, in fact, elements of $\mathcal{A}_n^*$. To this end, we will need the following intermediate result (Lemma 14). For integers $s \in [0, n^2/2]$, $d \in [0, n/2]$, and $\ell \in [1, n]$, let

$$\Delta(s, d, \ell) = \Big\{ \boldsymbol{u} \in \Delta \, : \, |\boldsymbol{u}| = n^2/2 - s, \; u_\ell = n/2 - d \Big\}$$

and

$$\mathcal{A}(s, d, \ell) = \bigcup_{(\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T} \,:\, \boldsymbol{u} \in \Delta(s,d,\ell)} \mathcal{B}\big((n/2)\cdot\mathbf{1} - \boldsymbol{u}, (n/2)\cdot\mathbf{1} - \boldsymbol{v}\big) \, .$$

Thus, $\mathcal{A}(s, d, \ell)$ is the set of constraint satisfying arrays in which the ℓ-th row sum is precisely d and in which the total number of 1's is s.

Lemma 14. *For $0 < d < 2s/n$,*

$$\frac{|\mathcal{A}(s,d{-}1,\ell)|}{|\mathcal{A}(s,d,\ell)|} \leqslant \frac{n^2/2 - s + dn/2}{s - (d{-}1)n/2} \leqslant \frac{n - 2s/n + d}{2s/n - d} \; . \tag{34}$$

Proof. Consider a bipartite graph with left and right vertices corresponding respectively to the elements of $\mathcal{A}(s,d{-}1,\ell)$ and $\mathcal{A}(s,d,\ell)$. A pair of vertices $(a,b) \in \mathcal{A}(s,d{-}1,\ell) \times \mathcal{A}(s,d,\ell)$ will have an edge if and only if the matrix b can be obtained from $a = (a_{i,j})$ by switching the values of $a_{\ell,j}$ and $a_{i,j}$ for some j and $i \neq \ell$. Notice that this implies that $a_{\ell,j} = 0$ and $a_{i,j} = 1$. Let $\deg(v)$ denote the degree of a vertex v in this graph. For $a \in \mathcal{A}(s,d{-}1,\ell)$ we have

$$\deg(a) \geqslant s - (d{-}1)n/2 \; , \tag{35}$$

where the lower bound is a lower bound on the number of 1's in a belonging to the same column as a 0 in the ℓ-th row, as these are precisely the 1's that can be switched with a 0 in the manner above, with each such switch giving rise to a distinct $b \in \mathcal{A}(s,d,\ell)$. The lower bound on the number of these 1's is obtained by subtracting from the total number of 1's, the maximum number of 1's that could occur in the remaining columns.

Similarly for $b \in \mathcal{A}(s,d,\ell)$ we have

$$\deg(b) \leqslant n^2 - s - (n-d)(n/2) = n^2/2 - s + dn/2 \; , \tag{36}$$

where the upper bound is an upper bound on the number of 0's in b belonging to the same column as a 1 in the ℓ-th row, as only these 0's could have been switched with a 1 in the manner above. In this case, some of these switches would have been impossible since the originating array would violate the constraint, but we can still count these for an upper bound on the degree. The upper bound on the number of 0's is obtained by subtracting from the total number of 0's, the fewest 0's that could occur in the remaining columns.

We then have

$$\begin{aligned} |\mathcal{A}(s,d{-}1,\ell)|\,(s - (d{-}1)n/2) &\leqslant \sum_{a \in \mathcal{A}(s,d-1,\ell)} \deg(a) && (37) \\ &= \sum_{b \in \mathcal{A}(s,d,\ell)} \deg(b) \\ &\leqslant |\mathcal{A}(s,d,\ell)|\,(n^2/2 - s + dn/2) \; , && (38) \end{aligned}$$

where (37) and (38), respectively, follow from (35) and (36). A simple manipulation establishes (34). □

Lemma 15. *With $\gamma = \gamma_0(n)$ as in (6),*

$$\frac{|\mathcal{A}_n^\circ \setminus \mathcal{A}_n^*|}{|\mathcal{A}_n^\circ|} = o(1) \; .$$

Proof. Notice that the bound (34) is decreasing in s and increasing in d. Thus, if we set

$$s_1 = \lceil n^2/2 - \gamma n^{3/2}/8 \rceil \quad \text{and} \quad d_1 = \lfloor n/2 - \gamma\sqrt{n}/2 \rfloor \,,$$

it will follow that

$$\begin{aligned} \frac{|\mathcal{A}(s,d-1,\ell)|}{|\mathcal{A}(s,d,\ell)|} &\leqslant \frac{n/2-\gamma\sqrt{n}/4}{n/2+\gamma\sqrt{n}/4} \\ &= 1-\gamma/\sqrt{n}+O(\gamma^2/n) \end{aligned} \tag{39}$$

will hold for all $s \geqslant s_1$ and $d \leqslant d_1$, where (39) is the bound evaluated for $s = s_1$ and $d = d_1$, after simplification. In particular, for $d \leqslant d_2 = \lfloor n/2 - \gamma\sqrt{n} \rfloor$, $s \geqslant s_1$, and sufficiently large n, it follows that

$$\frac{|\mathcal{A}(s,d,\ell)|}{|\mathcal{A}_n^\circ|} \leqslant \frac{|\mathcal{A}(s,d,\ell)|}{|\mathcal{A}(s,d_1,\ell)|} \tag{40}$$

$$\leqslant \big(1-\gamma/\sqrt{n}+O(\gamma^2/n)\big)^{d_1-d_2} \tag{41}$$

$$\leqslant e^{-\Omega(\gamma^2)} = n^{-\Omega(1)} \,, \tag{42}$$

where Eq. (40) follows from the fact that $\mathcal{A}(s,d_1,\ell) \subseteq \mathcal{A}_n^\circ$ for $s \geqslant s_1$; Eq. (41) follows from writing the ratio as a product of one-step ratios and the bound (39) for the first $d_1 - d_2$ ratios (and a bound of 1 for the remaining ratios); and (42) follows from our choice of $\gamma = \gamma_0(n)$ as in (6). We complete the proof by bounding $|\mathcal{A}_n^\circ \setminus \mathcal{A}_n^*|/|\mathcal{A}_n^\circ|$ from above by a union bound involving $|\mathcal{A}(s,d,\ell)|/|\mathcal{A}_n^\circ|$ over $s \geqslant s_1$, $d \leqslant d_2$, and rows and columns ℓ (the above assumed ℓ corresponded to a row index, but the analysis applies almost verbatim to columns). The resulting bound can, in turn, be bounded from above by multiplying the bound (42) by a polynomial factor in n. This final bound will be $o(1)$ when the term $\Theta(1)$ in (6) is bounded from below by a sufficiently large constant. □

Proof of Proposition 12. Combining Lemmas 13 and 15 yields

$$\begin{aligned} \frac{|\mathcal{A}_n^*|}{|\mathcal{A}_n|} &= \frac{|\mathcal{A}_n^*|}{|\mathcal{A}_n^\circ|}\frac{|\mathcal{A}_n^\circ|}{|\mathcal{A}_n|} \\ &\geqslant \frac{|\mathcal{A}_n^*|}{|\mathcal{A}_n^\circ|}\big(1-2^{-\Omega(n)}\big) \qquad (43) \\ &\geqslant \frac{|\mathcal{A}_n^* \cap \mathcal{A}_n^\circ|}{|\mathcal{A}_n^\circ|}\big(1-2^{-\Omega(n)}\big) \\ &\geqslant 1-o(1) \,, \qquad (44) \end{aligned}$$

or that $|\mathcal{A}_n| \leqslant (1+o(1)) \cdot |\mathcal{A}_n^*|$, where (43) follows from Lemma 13, Theorem 2, and the fact that $\rho < 2$, while (44) follows from Lemma 15. □

3.2 Majorization proof

This second proof was outlined in the preliminary conference version of this paper [15], wherein we obtained a less precise characterization of the redundancy than given in the present Theorem 1. Here, we sketch how this proof can be adapted to establish the stronger result here and also present a full proof, which was omitted in [15], of the key majorization bound.

This proof of Theorem 11 is based on an upper bound on the ratio $|\mathcal{B}(\boldsymbol{s},\boldsymbol{t})|/|\mathcal{B}(\boldsymbol{s}',\boldsymbol{t}')|$ when $\boldsymbol{s}$ and $\boldsymbol{t}$ respectively majorize $\boldsymbol{s}'$ and $\boldsymbol{t}'$. Given any $(\boldsymbol{s},\boldsymbol{t}) \in [0,n/2]^n \times [0,n/2]^n$, we then find a suitable *anchor point* $(\boldsymbol{s}',\boldsymbol{t}')$ (in the set of row–column sums satisfying conditions (i)–(iii) in Theorem 3) which is also majorized by $(\boldsymbol{s},\boldsymbol{t})$. We then obtain an upper bound on $|\mathcal{B}(\boldsymbol{s},\boldsymbol{t})|$ by combining the ratio bound with the expression for $|\mathcal{B}(\boldsymbol{s}',\boldsymbol{t}')|$ from Theorem 3. After a series of approximations along the lines of Section 2, we arrive at a bound that corresponds to the expected value of a certain product under the same jointly normal distribution as in Section 2 and is analyzed similarly. The key aspects of this proof are a (re)definition of a "good" subset $\mathcal{A}_n^\circ$, the majorization upper bound, and an analytically tractable, yet sufficiently tight choice for the anchor point mapping.

For this proof, we need to redefine

$$\Delta^\circ = \Delta_n^\circ(\gamma) = \left\{ \boldsymbol{u} \in \Delta \,:\, \|\boldsymbol{u}\|^2 \leqslant \gamma n^2 \quad \text{and} \quad \max_i u_i < n/2 \text{ for all } i \right\} .$$

Also, define T° and $\mathcal{A}_n^\circ$ as in Section 3.1, but in terms of the redefined Δ°. We then have the following analog of Lemma 13, proved in Appendix A.

Lemma 16. *For γ sufficiently large,*

$$|\mathcal{A}_n \setminus \mathcal{A}_n^\circ| \leqslant 2^{n^2-2n+o(n)} .$$

The bounding of $|\mathcal{A}_n^\circ|$ for this proof of Theorem 11 shall require using the majorization upper bound and the anchor point technique mentioned above. We begin with the following lemma, whose proof is in Appendix B.

Lemma 17. *For any integer vectors $\boldsymbol{s},\boldsymbol{t} \in [0,n/2]^n$ with $|\boldsymbol{s}| = |\boldsymbol{t}|$, if $s_i{-}1 \geqslant s_j{+}1$ (where we assume w.l.o.g. that $j > i$) then, for $\boldsymbol{s}' = (s'_k)_{k=1}^n = (s_1 \,\ldots\, s_i{-}1 \,\ldots\, s_j{+}1 \,\ldots\, s_n)$:*

$$\frac{|\mathcal{B}(\boldsymbol{s},\boldsymbol{t})|}{|\mathcal{B}(\boldsymbol{s}',\boldsymbol{t})|} \leqslant \frac{s'_j}{s_i} \quad \textit{and} \quad \frac{|\mathcal{B}(\boldsymbol{t},\boldsymbol{s})|}{|\mathcal{B}(\boldsymbol{t},\boldsymbol{s}')|} \leqslant \frac{s'_j}{s_i} . \tag{45}$$

Given two vectors $\boldsymbol{x},\boldsymbol{x}' \in \mathbb{R}^n$, we say that $\boldsymbol{x}$ *majorizes* $\boldsymbol{x}'$ and write $\boldsymbol{x} \succeq \boldsymbol{x}'$, if and only if $|\boldsymbol{x}| = |\boldsymbol{x}'|$ and $\sum_{i=1}^k \tilde{x}_i \geqslant \sum_{i=1}^k \tilde{x}'_i$ for each k, where $\tilde{\boldsymbol{x}}$ denotes $\boldsymbol{x}$ with entries reordered from largest to smallest (i.e., $\tilde{x}_1 \geqslant \tilde{x}_2 \geqslant \ldots$) and similarly for $\tilde{\boldsymbol{x}}'$.

Lemma 18. *For any integer vectors $\boldsymbol{s}, \boldsymbol{t}, \boldsymbol{s}', \boldsymbol{t}' \in [0, n/2]^n$ such that $|\boldsymbol{s}| = |\boldsymbol{t}|$, $\boldsymbol{s} \succeq \boldsymbol{s}'$, and $\boldsymbol{t} \succeq \boldsymbol{t}'$,*

$$\frac{|\mathcal{B}(\boldsymbol{s}, \boldsymbol{t})|}{|\mathcal{B}(\boldsymbol{s}', \boldsymbol{t}')|} \leqslant \frac{\prod_{i=1}^n s_i'! \prod_{i=1}^n t_i'!}{\prod_{i=1}^n s_i! \prod_{i=1}^n t_i!} \,. \tag{46}$$

Proof. Since $\mathcal{B}(\boldsymbol{s}, \boldsymbol{t})$ remains the same even if we permute the entries of $\boldsymbol{s}$ or of $\boldsymbol{t}$, we assume hereafter in the proof that the entries in each of the vectors $\boldsymbol{s}$, $\boldsymbol{t}$, $\boldsymbol{s}'$, and $\boldsymbol{t}'$ are sorted from largest to smallest. A well known consequence of majorization is that $\boldsymbol{s}$ can be obtained from $\boldsymbol{s}'$ by a finite sequence of transformations in which s_i' is increased by 1 and s_j' is decreased by 1 for some pair of indexes $i < j$. Applying Lemma 17 for each such transformation results in

$$\frac{|\mathcal{B}(\boldsymbol{s}, \boldsymbol{t})|}{|\mathcal{B}(\boldsymbol{s}', \boldsymbol{t}')|} \leqslant \frac{\prod_{i:s_i<s_i'} \prod_{k=s_i+1}^{s_i'} k}{\prod_{i:s_i>s_i'} \prod_{k=s_i'+1}^{s_i} k} \cdot \frac{\prod_{i:t_i<t_i'} \prod_{k=t_i+1}^{t_i'} k}{\prod_{i:t_i>t_i'} \prod_{k=t_i'+1}^{t_i} k} \,, \tag{47}$$

with each *net* increment or decrement of an entry respectively contributing a factor in the numerator or denominator of (47). The expression (46) is obtained by rewriting the products appearing in (47) as ratios of factorials, simplifying, and suitably permuting the resulting factorials. □

Given $(\boldsymbol{u}, \boldsymbol{v}) \in \mathrm{T}^\circ$, let $(\boldsymbol{u}', \boldsymbol{v}') \in \mathrm{T}$ be such that $(\boldsymbol{s}', \boldsymbol{t}') = \big((n/2)\cdot\mathbf{1}-\boldsymbol{u}', (n/2)\cdot\mathbf{1}-\boldsymbol{v}'\big)$ satisfies conditions (i)–(ii) of Theorem 3 and both $\boldsymbol{u} \succeq \boldsymbol{u}'$ and $\boldsymbol{v} \succeq \boldsymbol{v}'$. In particular, $|\boldsymbol{u}'|$ and $|\boldsymbol{v}'|$ are both equal to $|\boldsymbol{u}|$ $(= |\boldsymbol{v}|)$, which, in turn, is bounded from above (using the Cauchy–Schwarz inequality) by $\|\boldsymbol{u}\|\sqrt{n} \leqslant \gamma^{1/2} n^{3/2} = o(n^2)$; hence, $(\boldsymbol{s}', \boldsymbol{t}')$ also satisfies condition (iii) of Theorem 3. Furthermore, by the Schur convexity of power sums (see [13]) we have $\|\boldsymbol{u}'\|^2 \leqslant \|\boldsymbol{u}\|^2 \leqslant \gamma n^2$ and $\|\boldsymbol{v}'\|^2 \leqslant \|\boldsymbol{v}\|^2 \leqslant \gamma n^2$ (and so $(\boldsymbol{u}', \boldsymbol{v}') \in \Delta^\circ$). It follows from Theorem 3 that

$$|\mathcal{B}(\boldsymbol{s}', \boldsymbol{t}')| = \big|\mathcal{B}\big((n/2)\cdot\mathbf{1}-\boldsymbol{u}', (n/2)\cdot\mathbf{1}-\boldsymbol{v}'\big)\big| = e^{O(\gamma^2)} \cdot B(\boldsymbol{u}', \boldsymbol{v}')$$

which, with Lemma 18, yields

$$\big|\mathcal{B}\big((n/2)\cdot\mathbf{1}-\boldsymbol{u}, (n/2)\cdot\mathbf{1}-\boldsymbol{v}\big)\big| \leqslant e^{O(\gamma^2)} \cdot B(\boldsymbol{u}', \boldsymbol{v}') \cdot \frac{\prod_{i=1}^n (n/2 - u_i')! \prod_{i=1}^n (n/2 - v_i')!}{\prod_{i=1}^n (n/2 - u_i)! \prod_{i=1}^n (n/2 - v_i)!} \,.$$

We conclude that, with $(\boldsymbol{u}, \boldsymbol{v})$ and $(\boldsymbol{u}', \boldsymbol{v}')$ as above,

$$\begin{aligned} |\mathcal{B}\left((n/2)\cdot\mathbf{1}-\boldsymbol{u}, (n/2)\cdot\mathbf{1}-\boldsymbol{v}\right)| \;\leqslant\; & e^{O(\gamma^2)} \cdot \binom{n^2}{n^2/2 + |\boldsymbol{u}|}^{-1} \\ & \times \prod_{j=1}^n \frac{n!}{(n/2 + u_j')!(n/2 - u_j)!} \prod_{k=1}^n \frac{n!}{(n/2 + v_k')!(n/2 - v_k)!} \,. \end{aligned} \tag{48}$$

The following counterpart of (the combination of) Lemmas 6 and 7 can then be proved.

Lemma 19.

$$|\mathcal{A}_n^\circ| \leqslant e^{O(\gamma^2)} \cdot 2^{n^2+2n} \cdot \left(\sum_{\boldsymbol{u} \in \Delta^\circ} F(\boldsymbol{u}) \cdot e^{(\|\boldsymbol{u}\|^2 - \|\boldsymbol{u}'\|^2)/n} \right)^2 , \tag{49}$$

where each $\boldsymbol{u}'$ is (an anchor point which is) an image of $\boldsymbol{u}$ under a prescribed mapping $\Delta^\circ \to \Delta^\circ$ such that $\boldsymbol{u}'$ satisfies conditions (i)–(ii) of Theorem 3 and is majorized by $\boldsymbol{u}$.

Proof sketch. As in the proof of Lemma 5, for $\boldsymbol{u}, \boldsymbol{v} \in \Delta^\circ$, we approximate the factorials in (48) using (9) and the Taylor expansion (11). We then eliminate terms via a combination of the properties of the set Δ°, majorization, the Schur convexity of power sums [13], and the dropping of terms with negative contributions to the exponent (to obtain an upper bound); more details on these steps can be found in Appendix C. This results in the following counterpart of Lemma 6:

$$|\mathcal{A}_n^\circ| \leqslant e^{O(\gamma^2)} \cdot 2^{n^2+2n} \cdot \sum_{(\boldsymbol{u},\boldsymbol{v}) \in \mathrm{T}^\circ} \left(F(\boldsymbol{u}) \cdot e^{(\|\boldsymbol{u}\|^2 - \|\boldsymbol{u}'\|^2)/n} \right) \left(F(\boldsymbol{v}) \cdot e^{(\|\boldsymbol{v}\|^2 - \|\boldsymbol{v}'\|^2)/n} \right) .$$

The squared summation in (49) is obtained by summing over the product set $\Delta^\circ \times \Delta^\circ$ containing T°. □

We now specify a good choice for the anchor point $\boldsymbol{u}'$ for a given $\boldsymbol{u} \in \Delta^\circ$, through the following simple algorithm. We start by initializing $\boldsymbol{u}'$ to $\boldsymbol{u}$; then, we update $\boldsymbol{u}'$ by iterating the following pair of operations as long as $(\max_j u'_j) - (\min_j u'_j) > \gamma\sqrt{n}$: subtract 1 from a largest entry in $\boldsymbol{u}'$, and then add 1 to a smallest entry in $\boldsymbol{u}'$. It is obvious that the resulting $\boldsymbol{u}'$ will satisfy conditions (i)–(ii) of Theorem 3 since the difference between the largest and smallest entries is at most $\gamma\sqrt{n}$. Also, by design, $\boldsymbol{u} \succeq \boldsymbol{u}'$. Moreover, it is not hard to see that

$$u'_j \geqslant \min(u_j, \gamma\sqrt{n}) \tag{50}$$

(assuming here that $\gamma\sqrt{n}$ is an integer).

Letting

$$\mathscr{R} = \mathscr{R}_n = \begin{cases} [0, n/2]^n & \text{for odd } n \\ [-1/2, n/2]^n & \text{for even } n \end{cases}$$

and paralleling Section 2, the following integral bound can be proved.

Lemma 20.

$$|\mathcal{A}_n^\circ| \leqslant e^{O(\gamma^2)} \cdot 2^{n^2+2n} \cdot \left(\int_{\boldsymbol{u} \in \mathscr{R}} F(\boldsymbol{u}) \cdot e^{-(1/n)\sum_j \min(0, \gamma^2 n - u_j^2)} \, d\boldsymbol{u} \right)^2 . \tag{51}$$

Proof sketch. We incorporate the above specification for the anchor point $\boldsymbol{u}'$ and the lower bound (50) into (49), resulting in an upper bound. By regrouping terms of the resulting exponent in the summand we obtain the exponent of the integrand in (51). The summation

is then replaced by an integration over the set of unit cubes containing points in Δ°, and the error in the integration relative to the summation can be bounded using the technique of Lemma 8 and the properties of Δ° to control higher order error terms in the Taylor expansions of $\sinh(\cdot)$; specifically, we first rewrite (14) as

$$\begin{aligned}\prod_{i=1}^{n} \frac{\sinh\left(|\boldsymbol{u}|/n^2 - 2u_i/n\right)}{|\boldsymbol{u}|/n^2 - 2u_i/n} &= \prod_{i=1}^{n}\Big(1 + O\big((|\boldsymbol{u}|/n^2 - 2u_i/n)^2\big)\Big) \\ &\leqslant \Big(1 + (1/n)\sum_{i=1}^{n} O\big((|\boldsymbol{u}|/n^2 - 2u_i/n)^2\big)\Big)^n \\ &= \Big(1 + O\big(|\boldsymbol{u}|^2/n^4 + \|\boldsymbol{u}\|^2/n^3\big)\Big)^n \\ &= \big(1 + O(\gamma^2/n)\big)^n = e^{O(\gamma^2)} ,\end{aligned}$$

where the second step follows from the inequality of arithmetic and geometric means; then, we replace the instances of u_i in the above steps by $u_i + (u_i/2)\mathbb{1}(u_i \geqslant \gamma\sqrt{n})$. The domain of integration can then be enlarged to obtain (51). □

The integral in (51) is equivalent to the expectation

$$\mathcal{P} = \mathcal{P}_n(\gamma) = \mathsf{E}\left\{e^{-(1/n)\sum_j \min(0,\gamma^2 n - U_j^2)}\mathbb{1}(\boldsymbol{U} \in \mathscr{R})\right\} ,$$

where $\boldsymbol{U} = (U_1\, U_2\, \ldots\, U_n)$ is the jointly normal vector with zero mean and covariance matrix Σ defined in (16). We can analyze this expectation by using the equivalent representation $\boldsymbol{V}$ of $\boldsymbol{U}$ given by (18) and the resulting conditional independence of the V_i's given Y_0. This yields, for odd n,

$$\begin{aligned}\mathcal{P} &= \mathsf{E}\left\{\prod_{j=1}^{n} \mathsf{E}\big\{e^{-(1/n)\min(0,\gamma^2 n - V_j^2)}\mathbb{1}(V_j \in [0, n/2]) \;\big|\; Y_0\big\}\right\} \\ &= \mathsf{E}\left\{\Big[\mathsf{E}\big\{e^{-(1/n)\min(0,\gamma^2 n - V_1^2)}\mathbb{1}(V_1 \in [0, n/2]) \;\big|\; Y_0\big\}\Big]^n\right\} , \qquad (52)\end{aligned}$$

and for even n,

$$\mathcal{P} = \mathsf{E}\left\{\Big[\mathsf{E}\big\{e^{-(1/n)\min(0,\gamma^2 n - V_1^2)}\mathbb{1}(V_1 \in [-1/2, n/2]) \;\big|\; Y_0\big\}\Big]^n\right\} .$$

For odd n, Eq. (52) can be expressed as

$$\mathcal{P} = \int_{-\infty}^{+\infty} \frac{e^{-y^2/2}}{\sqrt{2\pi}}\left[Q\left(2\gamma - \frac{y}{\sqrt{n}}\right) - Q\left(\frac{-y}{\sqrt{n}}\right) + \int_{\gamma\sqrt{n}}^{n/2} e^{-\gamma^2 + v^2/n}\frac{2e^{-2(v-y/2)^2/n}}{\sqrt{2\pi n}}\,dv\right]^n dy , \quad (53)$$

and we show in Appendix D that (53) simplifies to

$$\mathcal{P} = \sqrt{\frac{n}{2\pi}} \int_{-\infty}^{+\infty} \Big[e^{-x^2/2} \big(Q(x) - 1 + Q(2\gamma - x) + \varphi(x, n) \big) \Big]^n dx \ , \tag{54}$$

where in this last expression we have defined

$$\varphi(x, n) = \varphi(x, n, \gamma) = \sqrt{2}\, e^{-\gamma^2 + x^2/2} \Big(Q\big(\sqrt{n/2} - \sqrt{2}\, x \big) - Q\big(\sqrt{2}(\gamma - x) \big) \Big) \ . \tag{55}$$

The expression analogous to (54) for even n is

$$\mathcal{P} = \sqrt{\frac{n}{2\pi}} \int_{-\infty}^{+\infty} \Big[e^{-x^2/2} \big(Q(x + 1/\sqrt{n}) - 1 + Q(2\gamma - x) + \varphi(x, n) \big) \Big]^n dx \ . \tag{56}$$

Notice that the only difference between (54) and (56) and the corresponding integrals (21) and (27) from the lower bound analysis is the presence of the term $\varphi(x, n)$. In Appendix D, we show that even with this new term, (54) and (56) behave like $(1 + o(1)) \cdot \alpha \cdot 2^{-(\rho n - \delta\sqrt{n})/2}$, where α is as defined in Lemma 9 and $\gamma = \gamma_0(n)$ as in (6). Noting that $\rho < 2$, Theorem 11 then follows from Lemmas 16 and 20.

3.3 Numerical comparison

In Table 1, we present the exact redundancy of $\mathcal{A}_n$ (up to the displayed decimal precision), computed recursively, for $n = 1, 2, \ldots, 15$ (in the two leftmost sub-columns), along with the ratio

$$|\mathcal{A}_n| / 2^{n^2 - \rho n + \delta\sqrt{n}} \tag{57}$$

for this range of n (two rightmost sub-columns), where the denominator of (57) was obtained in Theorem 1 for the asymptotic behavior of $|\mathcal{A}_n|$, without the the polynomial factor $n^{O(1)}$. In the computations, we used the numerical values $\rho = 1.425148088$, and $\delta = 0$ for odd n and $\delta = 1.460164546$ for even n. As can be seen, the values for the ratio appear to be converging from above (respectively, from below) for odd n (respectively, for even n), indicating that the polynomial factor can likely be improved.

References

[1] E. Ordentlich, G. M. Ribeiro, R. M. Roth, G. Seroussi, and P. O. Vontobel, "Coding for limiting current in memristor crossbar memories," *2nd Annual Non-Volatile Memories Workshop*, UCSD, La Jolla, CA, Mar. 2011. Presentation slides are accessible at: `http://nvmw.ucsd.edu/2011/`.

n	Redundancy		Ratio	
1	1.000000		1.342710	
2		1.192645		0.754016
3	3.912537		1.286015	
4		3.157846		0.769726
5	6.785406		1.266050	
6		5.328775		0.782116
7	9.645269		1.257682	
8		7.609241		0.791123
9	12.500576		1.253322	
10		9.959640		0.797964
11	15.353959		1.250643	
12		12.359454		0.803386
13	18.206349		1.248829	
14		14.796522		0.807825
15	21.058160		1.247518	

Table 1: Exact redundancy of $\mathcal{A}_n$ and ratio of exact value of $|\mathcal{A}_n|$ to asymptotic expression for small n.

[2] D. B. Strukov and R. S. Williams, "Four-dimensional address topology for circuits with stacked multilayer crossbar arrays," *Proc. Nat'l. Acad. Sci.*, 106 (2009), 20155–20158.

[3] E. Ordentlich and R. M. Roth, "Low complexity two-dimensional weight constrained codes," *Proc. 2011 IEEE Intl. Symp. Inform. Theory (ISIT 2011)*, St. Petersburg, Russia (Aug. 2011), 149–153, and submitted to *IEEE Trans. Inform. Theory* (Sep. 2011).

[4] O. Riordan and A. Selby, "The maximum degree of a random graph," *Comb. Probab. Comput.*, 9 (2000), 549–572.

[5] B. D. McKay, I. M. Wanless, and N. C. Wormald, "Asymptotic enumeration of graphs with a given bound on the maximum degree," *Comb. Probab. Comput.*, 11 (2002), 373–392.

[6] J. J. Hopfield, "Neural networks and physical systems with emergent collective computational abilities," *Proc. Nat'l. Acad. Sci.*, 79 (1982), 2554–2558.

[7] E. C. Posner and R. J. McEliece, "The number of stable points of an infinite-range spin glass memory," Jet Propulsion Laboratory, Telecommunications and Data Acquisition Progress Report, Vol. 42–83 (July–Sep. 1985), 209–215.

[8] E. R. Canfield, C. Greenhill, and B. D. McKay, "Asymptotic enumeration of dense 0–1 matrices with specified line sums," *J. Comb. Theory, Series A*, 115 (2008), 32–66.

[9] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables* National Bureau of Standards, Applied Mathematics Series 55, 2002.

[10] W. Feller, *An Introduction to Probability Theory and Its Applications*, Vol. 1, 3rd Ed., Wiley Series in Probability and Mathematical Statistics, Wiley, New York, 1968.

[11] W. Szpankowski, *Average Case Analysis of Algorithms on Sequences*, Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley, New York, 2001.

[12] R. N. Pedersen, "Laplace's method for two parameters," *Pacific J. Math.*, 2 (1965), 585–596.

[13] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications*, Vol. 143 of *Mathematics in Science and Engineering*, Academic Press, London, 1979.

[14] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Amer. Stat. Assoc. J.* (Mar. 1963), 13–30.

[15] E. Ordentlich, F. Parvaresh, and R. M. Roth, "Asymptotic enumeration of binary matrices with bounded row and column weights," *Proc. 2011 IEEE Intl. Symp. Inform. Theory (ISIT 2011)*, St. Petersburg, Russia (Aug. 2011), 154–158.

A Proof of Lemma 16

Proof. Consider the following sets of $n \times n$ binary matrices $a = (a_{i,j})_{i,j=1}^n \in \{0,1\}^{n\times n}$:

$$\begin{aligned}
\Upsilon^{\mathrm{r}} &= \left\{ a \,:\, \sum_i \Big(n/2 - \sum_j a_{i,j} \Big)^2 > \gamma n^2 \right\} , \\
\Upsilon^{\mathrm{c}} &= \left\{ a \,:\, \sum_j \Big(n/2 - \sum_i a_{i,j} \Big)^2 > \gamma n^2 \right\} , \\
\Upsilon^{\mathrm{r}}_h &= \left\{ a \,:\, \sum_j a_{h,j} = 0 \right\} , \quad h = 1, 2, \ldots, n \, , \\
\Upsilon^{\mathrm{c}}_h &= \left\{ a \,:\, \sum_i a_{i,h} = 0 \right\} , \quad h = 1, 2, \ldots, n \, .
\end{aligned}$$

Clearly,

$$\mathcal{A}_n \setminus \mathcal{A}_n^\circ \subseteq \Upsilon^{\mathrm{r}} \cup \Upsilon^{\mathrm{c}} \cup \left(\bigcup_{h=1}^n \Upsilon^{\mathrm{r}}_h \right) \cup \left(\bigcup_{h=1}^n \Upsilon^{\mathrm{c}}_h \right)$$

and, hence, by row–column symmetry,

$$|\mathcal{A}_n \setminus \mathcal{A}_n^\circ| \leqslant 2 \Big(|\Upsilon^{\mathrm{r}}| + \sum_{h=1}^n |\Upsilon^{\mathrm{r}}_h| \Big) \, . \tag{58}$$

Similarly to (30), we can write

$$|\Upsilon^{\mathrm{r}}| = 2^{n^2} \cdot \mathsf{Pr}\Big\{ \|\boldsymbol{S}\|^2 > \gamma n^2 \Big\} \, ,$$

where $\boldsymbol{S} = (S_i)_{i=1}^n$ is as in the proof of Lemma 10. Following the steps of the latter proof, we bound this probability using the Chernoff bound:

$$\mathsf{Pr}\Big\{ \|\boldsymbol{S}\|^2 > \gamma n^2 \Big\} \leqslant \mathsf{E}\Big\{ e^{(1/n)\sum_i (S_i^2 - \gamma n)} \Big\} = \Big[e^{-\gamma} \mathsf{E}\big\{ e^{S_1^2/n} \big\} \Big]^n \, , \tag{59}$$

and

$$\begin{aligned}
\mathsf{E}\big\{ e^{S_1^2/n} \big\} &= \int_0^\infty \mathsf{Pr}\big\{ e^{S_1^2/n} \geqslant x \big\} \, dx \\
&= \int_0^\infty \mathsf{Pr}\big\{ S_1^2 \geqslant n \ln x \big\} \, dx \\
&= 1 + \int_1^\infty \mathsf{Pr}\big\{ S_1 \geqslant \sqrt{n \ln x} \big\} \, dx \\
&\leqslant 1 + \int_1^\infty \frac{dx}{x^2} = 2 \, ,
\end{aligned}$$

where the fourth step follows from Hoeffding's inequality [14]. Incorporating the result into (59) yields, for sufficiently large γ,

$$|\Upsilon^{\mathrm{r}}| \leqslant 2^{n^2} \left[2e^{-\gamma}\right]^n < 2^{n^2-2n+o(n)} \,. \tag{60}$$

As for the sets Υ^{r}_h, it is easy to see that

$$|\Upsilon^{\mathrm{r}}_h| = \left[\sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{j}\right]^{n-1}$$

and, since the summation in the brackets is $2^{n-1+o(1)}$,

$$|\Upsilon^{\mathrm{r}}_h| = 2^{(n-1)^2+n\cdot o(1)} = 2^{n^2-2n+o(n)} \,. \tag{61}$$

The lemma then follows from (58), (60), (61), and Lemma 13. □

B Proof of Lemma 17

Proof. Note that the rightmost inequality of (45) follows from the one on the left by transposition, so we focus on proving the left one. Assume without loss of generality that $i = 1$ and $j = 2$. For $\boldsymbol{w}_1 (= (w_{1,1}\, w_{1,2}\, \ldots\, w_{1,n})), \boldsymbol{w}_2 \in \{0,1\}^n$ with $|\boldsymbol{w}_1| = s_1$ and $|\boldsymbol{w}_2| = s_2$ let $\mathcal{B}(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{s}, \boldsymbol{t})$ denote the set of all matrices in $\mathcal{B}(\boldsymbol{s}, \boldsymbol{t})$ whose first and second rows equal $\boldsymbol{w}_1$ and $\boldsymbol{w}_2$, respectively.

For $\mathcal{J}_1, \mathcal{J}_2 \subseteq \{1, 2, \ldots, n\}$ with $\mathcal{J}_1 \cap \mathcal{J}_2 = \emptyset$ and $v_1 \geqslant v_2$ let

$$\mathcal{W}(v_1, v_2, \mathcal{J}_1, \mathcal{J}_2) = \Big\{(\boldsymbol{w}_1, \boldsymbol{w}_2) \in \{0,1\}^n \times \{0,1\}^n \,:\, |\boldsymbol{w}_1| = v_1 \,,\ |\boldsymbol{w}_2| = v_2 \,,$$
$$w_{1,k} + w_{2,k} = 1 \Leftrightarrow k \in \mathcal{J}_1 \,,\ \text{and}\ w_{1,k} \cdot w_{2,k} = 1 \Leftrightarrow k \in \mathcal{J}_2\Big\} \,.$$

In other words, $\mathcal{J}_1$ is the set of positions where precisely one of either $\boldsymbol{w}_1$ or $\boldsymbol{w}_2$ is 1, and $\mathcal{J}_2$ is the set of positions where both of them are 1.

Note that with $n \geqslant v_1 \geqslant v_2 \geqslant 0$ and $v_1 + v_2 \leqslant n$ fixed, $\mathcal{W}(v_1, v_2, \mathcal{J}_1, \mathcal{J}_2)$ will be non-empty if and only if $|\mathcal{J}_2|$ satisfies $|\mathcal{J}_2| \leqslant v_2$ and $v_1 + v_2 - 2|\mathcal{J}_2| = |\mathcal{J}_1|$. Assuming $\mathcal{W}(v_1, v_2, \mathcal{J}_1, \mathcal{J}_2)$ is indeed not empty, it is then easy to see that

$$|\mathcal{W}(v_1, v_2, \mathcal{J}_1, \mathcal{J}_2)| = \binom{|\mathcal{J}_1|}{v_1 - |\mathcal{J}_2|} = \binom{|\mathcal{J}_1|}{v_2 - |\mathcal{J}_2|} = \binom{v_1 + v_2 - 2|\mathcal{J}_2|}{v_1 - |\mathcal{J}_2|} \,. \tag{62}$$

Namely, one can choose the positions where just $\boldsymbol{w}_1$ is 1, and this, given $\mathcal{J}_1$, also determines the positions where $\boldsymbol{w}_2$ is 1. The positions where both are 1 are determined by $\mathcal{J}_2$.

Next we observe that if $n > s_1{-}1 \geqslant s_2{+}1 > 0$ such that $s_1 + s_2 \leqslant n$, and $\mathcal{J}_1$ and $\mathcal{J}_2$ are such that $\mathcal{W}(s_1, s_2, \mathcal{J}_1, \mathcal{J}_2)$ and $\mathcal{W}(s_1{-}1, s_2{+}1, \mathcal{J}_1, \mathcal{J}_2)$ are both non-empty, then $|\mathcal{B}(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{s}, \boldsymbol{t})|$ is independent of $(\boldsymbol{w}_1, \boldsymbol{w}_2) \in \mathcal{W}(s_1, s_2, \mathcal{J}_1, \mathcal{J}_2)$ and $|\mathcal{B}(\boldsymbol{w}_1', \boldsymbol{w}_2', \boldsymbol{s}', \boldsymbol{t})|$ is independent of $(\boldsymbol{w}_1', \boldsymbol{w}_2') \in \mathcal{W}(s_1{-}1, s_2{+}1, \mathcal{J}_1, \mathcal{J}_2)$; in addition,

$$|\mathcal{B}(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{s}, \boldsymbol{t})| = |\mathcal{B}(\boldsymbol{w}_1', \boldsymbol{w}_2', \boldsymbol{s}', \boldsymbol{t})| \stackrel{\text{def}}{=} \psi(\mathcal{J}_1, \mathcal{J}_2) \tag{63}$$

for any $(\boldsymbol{w}_1, \boldsymbol{w}_2) \in \mathcal{W}(s_1, s_2, \mathcal{J}_1, \mathcal{J}_2)$ and any $(\boldsymbol{w}_1', \boldsymbol{w}_2') \in \mathcal{W}(s_1{-}1, s_2{+}1, \mathcal{J}_1, \mathcal{J}_2)$, where, in defining $\psi(\mathcal{J}_1, \mathcal{J}_2)$, we are suppressing the dependence on $s_3, s_4, \ldots, s_n$ and $\boldsymbol{t}$. The above hold because all $(\boldsymbol{w}_1, \boldsymbol{w}_2) \in \mathcal{W}(s_1, s_2, \mathcal{J}_1, \mathcal{J}_2)$ and all $(\boldsymbol{w}_1', \boldsymbol{w}_2') \in \mathcal{W}(s_1{-}1, s_2{+}1, \mathcal{J}_1, \mathcal{J}_2)$ have the same column sums when viewed as $2 \times n$ matrices, by virtue of their consistency with $\mathcal{J}_1$ and $\mathcal{J}_2$. These partial column sums, in turn, fully determine which $(n{-}2) \times n$ extensions will yield matrices with overall column sums corresponding to $\boldsymbol{t}$ (and remaining row sums $s_3, s_4, \ldots, s_n$).

Next, we express the sizes of $\mathcal{B}(\boldsymbol{s}, \boldsymbol{t})$ and $\mathcal{B}(\boldsymbol{s}', \boldsymbol{t})$ as summations of $|\mathcal{B}(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{s}, \boldsymbol{t})|$ over consistent choices of $|\mathcal{J}_2|, \mathcal{J}_1, \mathcal{J}_2, \boldsymbol{w}_1, \boldsymbol{w}_2$ as follows:

$$|\mathcal{B}(\boldsymbol{s}, \boldsymbol{t})| = \sum_{r=0}^{s_2} \sum_{(\mathcal{J}_1, \mathcal{J}_2)} \sum_{\substack{(\boldsymbol{w}_1, \boldsymbol{w}_2) \in \\ \mathcal{W}(s_1, s_2, \mathcal{J}_1, \mathcal{J}_2)}} |\mathcal{B}(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{s}, \boldsymbol{t})| \tag{64}$$

and

$$|\mathcal{B}(\boldsymbol{s}', \boldsymbol{t})| = \sum_{r=0}^{s_2+1} \sum_{(\mathcal{J}_1, \mathcal{J}_2)} \sum_{\substack{(\boldsymbol{w}_1, \boldsymbol{w}_2) \in \\ \mathcal{W}(s_1-1, s_2+1, \mathcal{J}_1, \mathcal{J}_2)}} |\mathcal{B}(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{s}', \boldsymbol{t})| \,, \tag{65}$$

where the middle summations in (64)–(65) are taken over all pairs $(\mathcal{J}_1, \mathcal{J}_2)$ such that $\mathcal{J}_1 \cap \mathcal{J}_2 = \emptyset$, $|\mathcal{J}_2| = r$, and $|\mathcal{J}_1| = s_1 + s_2 - 2r$. Notice that in (64) the outer summation extends only up to s_2 as compared to (65) which extends up to $s_2 + 1$. Combining (62) and (63) we can rewrite the innermost summations as

$$\sum_{(\boldsymbol{w}_1, \boldsymbol{w}_2) \in \mathcal{W}(s_1, s_2, \mathcal{J}_1, \mathcal{J}_2)} |\mathcal{B}(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{s}, \boldsymbol{t})| = \binom{s_1{+}s_2{-}2r}{s_1{-}r} \psi(\mathcal{J}_1, \mathcal{J}_2)$$

and

$$\sum_{(\boldsymbol{w}_1, \boldsymbol{w}_2) \in \mathcal{W}(s_1-1, s_2+1, \mathcal{J}_1, \mathcal{J}_2)} |\mathcal{B}(\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{s}', \boldsymbol{t})| = \binom{s_1{+}s_2{-}2r}{s_1{-}1{-}r} \psi(\mathcal{J}_1, \mathcal{J}_2) \,.$$

Incorporating these into (64) and (65) and bounding (65) from below by limiting the upper limit of the outer summation to s_2 shows that

$$\begin{aligned} \frac{|\mathcal{B}(\boldsymbol{s}, \boldsymbol{t})|}{|\mathcal{B}(\boldsymbol{s}', \boldsymbol{t})|} &\leqslant \frac{\sum_{r=0}^{s_2} \sum_{(\mathcal{J}_1, \mathcal{J}_2)} \binom{s_1+s_2-2r}{s_1-r} \psi(\mathcal{J}_1, \mathcal{J}_2)}{\sum_{r=0}^{s_2} \sum_{(\mathcal{J}_1, \mathcal{J}_2)} \binom{s_1+s_2-2r}{s_1-1-r} \psi(\mathcal{J}_1, \mathcal{J}_2)} \\ &\leqslant \max_{0 \leqslant r \leqslant s_2} \frac{\binom{s_1+s_2-2r}{s_1-r}}{\binom{s_1+s_2-2r}{s_1-1-r}} \,, \end{aligned} \tag{66}$$

where (66) follows from the inequality

$$\frac{\sum_{k=1}^{L} p_k}{\sum_{k=1}^{L} q_k} \leqslant \max_{1 \leqslant k \leqslant L} \frac{p_k}{q_k}$$

which is valid for $p_k, q_k \geqslant 0$. Hence, from (66),

$$\begin{aligned} \frac{|\mathcal{B}(\boldsymbol{s}, \boldsymbol{t})|}{|\mathcal{B}(\boldsymbol{s}', \boldsymbol{t})|} &\leqslant \max_{0 \leqslant r \leqslant s_2} \frac{1/((s_2 - r)!(s_1 - r)!)}{1/((s_2 + 1 - r)!(s_1 - 1 - r)!)} \\ &= \max_{0 \leqslant r \leqslant s_2} \frac{s_2 + 1 - r}{s_1 - r} \qquad (67) \\ &= \frac{s_2 + 1}{s_1} = \frac{s_2'}{s_1}\,, \qquad (68) \end{aligned}$$

where (68) follows from the fact that the maximum in (67) occurs at $r = 0$ which, in turn, follows from the fact that $s_2 + 1 < s_1$. This completes the proof. □

C Handling higher order error terms in Lemma 19

Referring to the proof sketch of Lemma 19, we first note that the Stirling approximation error factor $e^{\theta/12w}$ is handled as in the proof of Lemma 5 for the factorials involving n^2, n, and $|\boldsymbol{u}|$, where for the latter this is justified by the fact that $|\boldsymbol{u}| \leqslant \gamma^{1/2} n^{3/2}$ for every $\boldsymbol{u} \in \Delta^\circ$. As for the other factorials involving u_j, u_j', v_k, and v_k', appearing in the denominator, the error factor, which is greater than one, can be dropped to get an upper bound. Note that the error factor is always finite since the entries in each element of Δ° are strictly less than $n/2$, and since $\boldsymbol{u}'$ and $\boldsymbol{v}'$ are chosen to satisfy conditions (i)–(ii) of Theorem 3. The linear terms in the Taylor expansion (11) applied to the logarithm of (48) cancel, as in the proof of Lemma 5, since, by the majorization relationship, $|\boldsymbol{u}| = |\boldsymbol{u}'|$ and $|\boldsymbol{v}| = |\boldsymbol{v}'|$. As for the higher order terms, note that the terms involving u_j, u_j', v_k, v_k' derive from the denominator of (48) and hence appear with a global sign change relative to their counterparts involving $|\boldsymbol{u}|$. For these terms, we have

$$+ \frac{\|\boldsymbol{u}\|^2}{n^2} + \frac{\|\boldsymbol{u}'\|^2}{n^2} \qquad (69)$$

$$- \frac{\|\boldsymbol{u}\|^2}{n} - \frac{\|\boldsymbol{u}'\|^2}{n} \qquad (70)$$

$$+ \left(\frac{4}{3n^3} - \frac{2}{3n^2}\right)\left(\|\boldsymbol{u}\|_3^3 - \|\boldsymbol{u}'\|_3^3\right) \qquad (71)$$

$$+ \sum_{j=1}^{n} \frac{-2(n - 2\xi_j - 3)}{3(n - 2\xi_j)^4} u_j^4 \qquad (72)$$

$$+\sum_{j=1}^{n}\frac{-2(n+2\xi_j'-3)}{3(n+2\xi_j')^4}{u_j'}^4\,, \tag{73}$$

where each ξ_j (respectively, ξ_j') is between zero and u_j (respectively, u_j'). For $n>3$ the terms (71) and (73) can be dropped because they are negative (notice that by Schur convexity, $\|\boldsymbol{u}\|_3^3 \geqslant \|\boldsymbol{u}'\|_3^3$) and dropping only increases the bound. The terms (69) are $O(\gamma)$ by definition of Δ° (note that $\|\boldsymbol{u}\|^2 \geqslant \|\boldsymbol{u}'\|^2$, again by Schur convexity). For n large, we show that (72) is negative and can be dropped. We consider two cases. First, if u_j is smaller than $n/2-1$ then $\xi_j < n/2-1$ and the respective term in the sum (72) is therefore negative when $n>3$. For the case that $u_j = n/2-1$, the term $(n/2-u_j+1/2)\ln(n/2-u_j)$ is zero; so, the respective term in the sum (72), when added to the other terms in the Taylor expansion (11), should become zero. The remaining terms of that expansion when $u_j = n/2-1$ sum up to

$$\frac{n}{6}+\frac{17}{12}+\frac{3}{2}\ln\Big(\frac{2}{n}\Big)-O\Big(\frac{1}{n}\Big)\,,$$

which is positive for sufficiently large n. We conclude that the respective error term in (72) in this case is negative. We are then left only with the terms (70). Clearly, we can apply identical reasoning to the higher order terms involving $(v_k)_k$ and $(v_k')_k$.

D Analysis of $\mathcal{P}$ and resulting integrals

We present here more details of the analysis of $\mathcal{P}$ given by (52). We shall focus on the case of odd n. The analysis for even n is similar. We start from (53) and write

$$\begin{aligned}
\mathcal{P} &= \int_{-\infty}^{+\infty}\frac{e^{-y^2/2}}{\sqrt{2\pi}}\left[Q\Big(2\gamma-\frac{y}{\sqrt{n}}\Big)-Q\Big(\frac{-y}{\sqrt{n}}\Big)+\int_{\gamma\sqrt{n}}^{n/2}\sqrt{2}\,e^{-\gamma^2+y^2/(2n)}\frac{e^{-(v-y)^2/n}}{\sqrt{2\pi(n/2)}}\,dv\right]^n dy\\
&= \int_{-\infty}^{+\infty}\frac{e^{-y^2/2}}{\sqrt{2\pi}}\left[Q\Big(2\gamma-\frac{y}{\sqrt{n}}\Big)-Q\Big(\frac{-y}{\sqrt{n}}\Big)\right.\\
&\qquad\left.+\sqrt{2}\,e^{-\gamma^2+y^2/(2n)}\Big(Q\Big(\sqrt{n/2}-\frac{y}{\sqrt{n/2}}\Big)-Q\Big(\sqrt{2}\,\gamma-\frac{y}{\sqrt{n/2}}\Big)\Big)\right]^n dy\,.
\end{aligned}$$

Substituting $x=y/\sqrt{n}$ and recalling the definition of $\varphi(x,n)$ in (55), we obtain

$$\begin{aligned}
\mathcal{P} &= \sqrt{\frac{n}{2\pi}}\int_{-\infty}^{+\infty}e^{-nx^2/2}\Big[Q(2\gamma-x)-Q(-x)+\varphi(x,n)\Big]^n dx\\
&= \sqrt{\frac{n}{2\pi}}\int_{-\infty}^{+\infty}\Big[e^{-x^2/2}\big(Q(x)-1+Q(2\gamma-1)+\varphi(x,n)\big)\Big]^n dx\,,
\end{aligned}$$

thereby establishing (54). We thus conclude that

$$\mathcal{P}\leqslant\sqrt{\frac{n}{2\pi}}\int_{-\infty}^{+\infty}\Big[e^{-x^2/2}\big(Q(x)+\varphi(x,n)\big)\Big]^n dx\,. \tag{74}$$

Next, we show that, for $\gamma = \gamma_0(n)$ as in (6), the right-hand side of (74) equals $(1 + o(1)) \cdot \alpha \cdot 2^{-\rho n/2}$, where α is as defined in Lemma 9. Let x_0 be as defined in (1). We express the integral in (74) as the sum of integrals over the four intervals $I_0 = [-\infty, x_0 - c)$, $I_1 = [x_0 - c, x_0 + c)$, $I_2 = [x_0 + c, 2\sqrt{n})$, and $I_3 = [2\sqrt{n}, \infty]$, for a sufficiently large absolute constant c (to be determined below) and sufficiently large n. Let $\mathcal{I}_0$, $\mathcal{I}_1$, $\mathcal{I}_2$, and $\mathcal{I}_3$ denote the respective integrals. We shall bound these four integrals by applying respective bounds on $\varphi(x, n)$ in each interval.

In I_0,

$$\begin{aligned}
\varphi(x,n) &\leqslant \sqrt{2}\, e^{-\gamma^2 + x^2/2}\Big(1 - Q\big(\sqrt{2}(\gamma - x)\big)\Big) \\
&\leqslant \sqrt{2}\, e^{-\gamma^2 + x^2/2} \frac{e^{-(\gamma - x)^2}}{\sqrt{2}(\gamma - x)\sqrt{2\pi}} \\
&\leqslant c' \,,
\end{aligned}$$

for any absolute constant $c' > 0$, all $x \in I_0$, and sufficiently large n, where the second step follows from the tail bound (26). Therefore, for $\mathcal{I}_0$, we have

$$\begin{aligned}
\mathcal{I}_0 &\leqslant \sqrt{\frac{n}{2\pi}} \int_{-\infty}^{x_0 - c} \Big[e^{-x^2/2}(1 + c')\Big]^n dx \\
&= (1 + c')^n \Big(1 - Q\big(\sqrt{n}(c - x_0)\big)\Big) \\
&= O\big(1/\sqrt{n}\big) \cdot \Big[e^{-(c - x_0)^2/2}(1 + c')\Big]^n \,, \qquad (75)
\end{aligned}$$

where in the last step we have used again the tail bound (26).

The integral $\mathcal{I}_3$ is treated similarly: in this case,

$$\begin{aligned}
\varphi(x,n) &\leqslant \sqrt{2}\, e^{-\gamma^2 + x^2/2}\Big(1 - Q\big(\sqrt{2}\, x - \sqrt{n/2}\big)\Big) \\
&\leqslant \sqrt{2}\, e^{-\gamma^2 + x^2/2} \frac{e^{-(x - \sqrt{n}/2)^2}}{(\sqrt{2}\, x - \sqrt{n/2})\sqrt{2\pi}} \\
&\leqslant c' \,,
\end{aligned}$$

for any absolute constant $c' > 0$, all $x \in I_3$, and sufficiently large n. The corresponding integral then satisfies

$$\mathcal{I}_3 \leqslant \sqrt{\frac{n}{2\pi}} \int_{2\sqrt{n}}^{+\infty} \Big[e^{-x^2/2}(1 + c')\Big]^n dx = (1 + c')^n \big(1 - Q(2n)\big) = e^{-\Omega(n^2)} \,. \qquad (76)$$

In the case of $\mathcal{I}_1$ and $\mathcal{I}_2$,

$$\varphi(x,n) \leqslant \sqrt{2}\, e^{-\gamma^2 + x^2/2} \,, \qquad (77)$$

for all $x \in I_1 \cup I_2$ and sufficiently large n. Therefore,

$$\mathcal{I}_2 \leqslant \sqrt{\frac{n}{2\pi}} \int_{x_0+c}^{2\sqrt{n}} \left[e^{-x^2/2} + \sqrt{2}\, e^{-\gamma^2} \right]^n dx \leqslant O(n) \cdot \left[2e^{-(x_0+c)^2/2} \right]^n , \tag{78}$$

for γ sufficiently large, and

$$\begin{aligned}
\mathcal{I}_1 &\leqslant \sqrt{\frac{n}{2\pi}} \int_{x_0-c}^{x_0+c} \left[e^{-x^2/2} Q(x) + \sqrt{2}\, e^{-\gamma^2} \right]^n dx \\
&= \sqrt{\frac{n}{2\pi}} \int_{x_0-c}^{x_0+c} \left[e^{-x^2/2} Q(x) \big(1 + O(e^{-\gamma^2}) \big) \right]^n dx \\
&\leqslant (1+o(1)) \cdot \sqrt{\frac{n}{2\pi}} \int_{x_0-c}^{x_0+c} \left[e^{-x^2/2} Q(x) \right]^n dx \\
&= (1+o(1)) \cdot \alpha \cdot 2^{-\rho n/2} ,
\end{aligned}$$

by Laplace's method, where the penultimate step follows by our the choice of $\gamma = \gamma_0(n)$ as in (6), with $\Theta(1)$ therein is taken sufficiently large.

We see from (75), (76), and (78) that c can be chosen so that $\mathcal{I}_j = o(\mathcal{I}_1)$ for $j = 0, 2, 3$, from which it follows that

$$\mathcal{P} \leqslant \sum_j \mathcal{I}_j = (1+o(1)) \cdot \mathcal{I}_1 = (1+o(1)) \cdot \alpha \cdot 2^{-\rho n/2} .$$

The case of even n is handled similarly, except that in this case, the counterpart of $\mathcal{I}_1$ can be shown, via the bound (77) on $\varphi(x, n)$ and the extended Laplace's method of [12], to satisfy

$$\mathcal{I}_1 \leqslant (1+o(1)) \cdot \alpha \cdot 2^{-\rho n/2 + x_0 \sqrt{n}/\ln 2} ,$$

in analogy to the corresponding integral (27) from the lower bound analysis.