# Gardner formula for Ising perceptron models at small densities

**Erwin Bolthausen** EB@MATH.UZH.CH
*Institute of Mathematics, University of Zurich*

**Shuta Nakajima** SHUTA.NAKAJIMA@UNIBAS.CH
*Department of Mathematics and Computer Science, University of Basel*

**Nike Sun** NSUN@MIT.EDU
*Department of Mathematics, Massachusetts Institute of Technology*

**Changji Xu** CXU@CMSA.FAS.HARVARD.EDU
*Center for Mathematical Sciences and Applications, Harvard University*

**Editors:** Po-Ling Loh and Maxim Raginsky

## Abstract

We consider the Ising perceptron model with $N$ spins and $M = N\alpha$ patterns, with a general activation function $U$ that is bounded above. For $U$ bounded away from zero or $U(x) = \mathbf{1}\{x \geqslant \kappa\}$, it was shown by Talagrand (2000, 2011b) that for small densities $\alpha$, the free energy of the model converges as $N \to \infty$ to the replica symmetric formula conjectured in the physics literature by Krauth and Mézard (1989) (see also Gardner and Derrida, 1988). We give a new proof of this result, which covers the more general class of all functions $U$ that are bounded above and satisfy a certain variance bound. The proof uses the (first and second) moment method conditional on the approximate message passing iterates of the model. In order to deduce our main theorem, we also prove a new concentration result for the perceptron model in the case where $U$ is not bounded away from zero.

**Keywords:** List of keywords

## 1. Introduction

### 1.1. Overview

We study a class of generalized **Ising perceptron** models, defined as follows. Let $\boldsymbol{G} \equiv \boldsymbol{G}_{M\times N}$ be an $M \times N$ matrix with i.i.d. standard gaussian entries. Denote the rows of $\boldsymbol{G}$ as $\mathbf{g}^1, \ldots, \mathbf{g}^M$; each $\mathbf{g}^a$ is an independent standard gaussian vector in $\mathbb{R}^N$. Let $U : \mathbb{R} \to [0, \infty)$ be a bounded measurable function (the **activation function**), and denote $u \equiv \log U : \mathbb{R} \to [-\infty, \infty)$. The associated **Ising perceptron partition function** is

$$\boldsymbol{Z} \equiv \boldsymbol{Z}(\boldsymbol{G}) \equiv \sum_{J} \exp\left\{ \sum_{a\leqslant M} u\left( \frac{(\mathbf{g}^a, J)}{N^{1/2}} \right) \right\}, \tag{1}$$

where the sum goes over $J \in \{-1, +1\}^N$. The $J_i$ are called the **spins**, while the vectors $\mathbf{g}^a$ are called the **patterns**. The random matrix $\boldsymbol{G}$ is also called the **disorder** of the model.

A special case of the above is the **half-space intersection** model defined by the function $U(x) = \mathbf{1}\{x \geqslant \kappa\}$, where $\kappa \in \mathbb{R}$ is a fixed parameter. In this case, the pattern $\mathbf{g}^a \in \mathbb{R}^N$ defines a "half-space"

$H_{\mathbf{g}^a}$, which is the set of $J \in \{-1,+1\}^N$ such that $(\mathbf{g}^a, J)/N^{1/2} \geqslant \kappa$. The partition function (1) is then the cardinality of the intersection of random half-spaces,

$$\boldsymbol{Z} = \left| \bigcap_{a=1}^{M} H_{\mathbf{g}^a} \right| \leqslant 2^N \,. \tag{2}$$

This is connected to a neural network memorization model, which has been much studied following seminal works from the physics literature in the late 1980s (reviewed in §1.2 below).

The model (1) with general $U$ was introduced by Talagrand (2000, 2002). From the mathematical perspective, a motivation for the generalized model is that it may be more tractable to analyze under restrictions on the function $U$ — for instance, results of Talagrand (2000) impose bounds on $u \equiv \log U$ and its derivatives. In the physics language, these restrictions may be viewed as describing subsets of the "high-temperature" regime. On the other hand, from the statistical perspective, another motivation to consider the model (1) with general $U$ is that we may view $u \equiv \log U$ as a loss function. Thus, understanding the behavior of the model (1) may shed insight on the nature of certain high-dimensional loss surfaces.

In this paper we focus on the problem of understanding the **free energy** of the perceptron model (1), i.e., the first-order asymptotic behavior of the partition function $\boldsymbol{Z}$. We develop a method to compute the asymptotic free energy of (1) with $M = \alpha N$ for small $\alpha$, and $N \to \infty$. The small $\alpha$ requirement amounts to a high-temperature condition, which is less restrictive than in previous results (because there are fewer conditions on $U$), but still does not identify the full high-temperature regime for any given $U$.

Before stating our main result, we lay out our assumptions on $U$. Note that if $U$ is scaled by any factor $c$, then the partition function (1) is simply scaled by $c^M$. Therefore, since we assume $U$ is bounded, we may as well assume that $U$ maps into $[0,1]$. More precisely, we impose:

**Assumption 1** *The function $U$ is a measurable mapping from $\mathbb{R}$ into $[0,1]$. Moreover, with $\mathbb{E}_\xi$ denoting expectation over the law of a standard gaussian random variable $\xi$, we have*

$$\mathbb{E}_\xi[\xi U(\xi)] = \int zU(z)\,\varphi(z)\,dz \neq 0\,, \tag{3}$$

*where $\varphi$ denotes the standard gaussian density.*

See Remark 1.2 below for more discussion on the above assumption; in particular, we will explain that the condition (3) only rules out an easier case of the problem. We also impose:

**Assumption 2** *Writing $\mathbb{E}_{\xi,\xi'}$ for expectation over i.i.d. standard gaussians $\xi, \xi'$, the quantity*

$$K_{2,\wr}(U) \equiv \max\left\{1, \sup\left\{\frac{\mathbb{E}_{\xi,\xi'}[(\xi-\xi')^2 U(x+c\xi)U(x+c\xi')]}{\mathbb{E}_{\xi,\xi'}[U(x+c\xi)U(x+c\xi')]} : x \in \mathbb{R}, \frac{2}{5} \leqslant c \leqslant \frac{7}{3}\right\}\right\}.$$

*is finite. This assumption implies that the quantity*

$$K_2(U) \equiv \max\left\{1, \sup\left\{\frac{\mathbb{E}_{\xi,\xi'}[(\xi-\xi')^2 U(x+c\xi)U(x+c\xi')]}{\mathbb{E}_{\xi,\xi'}[U(x+c\xi)U(x+c\xi')]} : x \in \mathbb{R}, \frac{1}{2} \leqslant c \leqslant 2\right\}\right\}$$

*is also finite, and indeed $K_2(U) \leqslant K_{2,\wr}(U)$. (The bound on $K_{2,\wr}(U)$ further ensures that $K_2(U_\eta)$ is bounded, where $U_\eta$ is a smoothed approximation of $U$; see Lemma B.9.)*[1]

[1] Assumption 2 is the "certain variance bound" mentioned in the abstract of this paper: $K_2(U)$ and $K_{2,\wr}(U)$ refer to variances of certain measures $\mu_{x,c}$ on the real line, which are essentially gaussian measures reweighted by translates of $U$ — see Definition B.1.

Discussion of Assumption 2 is also deferred to Remark 1.2. We now state our main result:

**Theorem 1.1 (main theorem)** *If the function $U$ satisfies Assumptions 1 and 2, then there exists a positive constant $\alpha_\wr(U) > 0$ such that, if $\boldsymbol{G}$ is an $M \times N$ matrix with i.i.d. standard gaussian entries and $M/N \to \alpha$ with $0 \leqslant \alpha \leqslant \alpha_\wr(U)$, then for the (generalized) Ising perceptron model (1) the following limit holds in probability:*

$$\lim_{N\to\infty} \frac{1}{N} \log \boldsymbol{Z}(\boldsymbol{G}) = \mathrm{RS}(\alpha; U)\,, \tag{4}$$

*where $\mathrm{RS}(\alpha; U)$ is an exact expression known as the "replica symmetric free energy" of the model, defined by (12) and (29) below. Moreover, we can take $\alpha_\wr(U)$ explicitly as in (31) below.*

For $U$ bounded uniformly away from zero, as well as for the half-space intersection model $U(x) = \mathbf{1}\{x \geqslant \kappa\}$, the result of Theorem 1.1 was previously shown by Talagrand (2000, 2011b). Our proof is very different, and is based on the idea of **conditioning on the AMP (approximate message passing) iteration**: this method was previously introduced by Ding and Sun (2018) and Bolthausen (2019) (see also Alaoui and Sellke, 2020; Fan and Wu, 2021; Brennecke and Yau, 2021); and is described in §1.2.5 and §1.3 below. By contrast, Talagrand uses an interpolation approach, which seemingly necessitates more conditions on $U$, while our result covers the much more general class of functions $U$ satisfying only Assumptions 1 and 2. To name a simple example, we will see below that the function $U(x) = \mathbf{1}\{x \in [-1, 2]\}$ is covered by Theorem 1.1 but not by Talagrand's results. The main contributions of this work are the implementation of the AMP conditioning approach, together with new concentration results, for a more general model than has been considered in prior works. See §1.2.3 below for further discussion and comparison.

In general terms, the left-hand side of (4), whenever it exists, is called the **asymptotic free energy density** of the model. The right-hand side of (4) is the **replica symmetric free energy** of the model: it is an exact expression which was derived by heuristic methods of statistical physics, and conjectured to coincide with the left-hand side in the high-temperature regime — i.e., at least for $\alpha$ small enough, and potentially for all $\alpha$ where the left-hand side has a positive limit. In the case of the perceptron model this calculation was done by physicists in the late 1980s; the historical background is given in §1.2.1. It is not very difficult but requires some care to show that the formula $\mathrm{RS}(\alpha; U)$ is in fact even well-defined; the details of this will be given in §A.1 below. The physics derivation of (4) is non-rigorous because it relies on unproven hypotheses about the structure of the perceptron model, as we will discuss further in §1.2.1. One of the motivations of this project is to develop a deeper rigorous understanding of the perceptron model.

**Remark 1.2** *We make some further comments on our assumptions:*
*(1) From our perspective, Assumption 1 is relatively mild. It may be possible to relax the condition $U \leqslant 1$ to accommodate functions $U(x)$ that do not grow too quickly in $|x|$, but we will not pursue this here. Next, if the condition (3) fails — meaning that $\mathbb{E}_\xi[\xi U(\xi)] = 0$ — then the replica symmetric free energy $\mathrm{RS}(\alpha; U)$ reduces*[2] *to the* ***annealed free energy***

$$\mathrm{ann}(\alpha; U) = \frac{1}{N} \log \mathbb{E}\boldsymbol{Z}(\boldsymbol{G}) = \log 2 + \alpha \log \mathbb{E} U(\xi)\,. \tag{5}$$

[2] To see that this occurs, note that the fixed-point equation (9) is solved by $q = \psi = 0$. As a result, the expression (12) for $\mathrm{RS}(\alpha; U)$ simplifies to the right-hand side of (5).

*In this case, it is known that the limiting free energy can be obtained by a direct first and second moment method approach, without the need of a conditioning scheme. This is done for the case of symmetric $U$ by Aubin et al. (2019), and the argument of that paper can be extended to cover the case $\mathbb{E}_\xi[\xi U(\xi)] = 0$. Moreover it is expected that this case may be more tractable to analyze for finer properties of the solution space, following Perkins and Xu (2021); Abbe et al. (2021) (further discussed in §1.2.6 below).*

*(2) We view Assumption 2 as the somewhat more restrictive condition, although we will show (by straightforward arguments) that it holds if $U$ is bounded away from zero, compactly supported, or logconcave (see Proposition 1.3 below). Moreover, Assumption 2 is essentially necessary to ensure that in the approximate message passing (AMP) iteration associated with our model ((14) and (15)), the message-passing functions are Lipschitz — this is by an easy calculation, which we give in Lemma B.14. This allows us to use existing results on AMP and state evolution (Bayati and Montanari, 2011; Bolthausen, 2014) — see §1.3 and §A.2 — which all require the message-passing functions to be Lipschitz. On the other hand, we give in Remark B.5 an example of a function $U$ that does not satisfy Assumption 2.*

***Assumption 1 holds throughout this paper, even if not explicitly stated.** However, we will point out explicitly each place where Assumption 2 is used.*

**Proposition 1.3 (proved in §B.4)** *Suppose $U$ satisfies Assumption 1. If in addition $U$ is bounded away from zero, compactly supported, or logconcave, then $U$ also satisfies Assumption 2.*[3]

## 1.2. Background and related work

In this subsection we give some background on the perceptron model, and survey the related work. **Some high-level discussion of key ideas in this paper is given in §1.2.3–1.2.5.**

The perceptron problem originates from a toy model of a single-layer neural network, as follows. Suppose we have $N+1$ input nodes, labelled $0 \leqslant j \leqslant N$. Likewise we have $N+1$ output nodes, labelled $0 \leqslant i \leqslant N$. For all $i \neq j$, between the $j$-th input node and the $i$-th output node there is an edge weight $J_{i,j}$, to be determined. It will be convenient to fix $J_{i,i} \equiv 0$ for all $i$. The system is given $M$ input "patterns" $g^1, \ldots, g^M$, which are vectors in $\mathbb{R}^{N+1}$. We then say that the system **memorizes** the pattern $g^a$ if

$$\operatorname{sgn}\left(\sum_{j=0}^{N} J_{i,j}(g^a)_j\right) = \operatorname{sgn}\left((g^a)_i\right) \tag{6}$$

for all $0 \leqslant i \leqslant N$. One can then ask, given $M = N\alpha$ i.i.d. random patterns, whether there exists a choice of edge weights $J$ such that the system memorizes all $M$ patterns. The **storage capacity** $\alpha_{\mathrm{c}}$ of the model is the supremum of all $\alpha = M/N$ for which memorization of all $M$ given patterns is possible with probability $1 - o_N(1)$. Models of this type have been considered at least since the mid-20th century (e.g. McCulloch and Pitts, 1943; Hebb, 1949; Little, 1974; Hopfield, 1982).

Suppose the random patterns $g^a$ are modeled as i.i.d. standard gaussian vectors in $\mathbb{R}^{N+1}$. One can consider the constraint (6) separately for each $0 \leqslant i \leqslant N$, and by symmetry it suffices to understand the case $i = 0$. Recall that $J_{0,0} \equiv 0$, and denote $J_j \equiv J_{j,0}$ for $1 \leqslant j \leqslant N$. Denote $g_{a,j} \equiv \operatorname{sgn}((g^a)_0)(g^a)_j$ for all $1 \leqslant a \leqslant M$ and $1 \leqslant j \leqslant N$, and note the $g_{a,i}$ are i.i.d. standard

[3] Note that Proposition 1.3 implies that the function $U(x) = \mathbf{1}\{x \in [-1,2]\}$ indeed satisfies Assumptions 1 and 2, as was mentioned above.

gaussian random variables. Writing $\mathbf{g}^a \equiv (g_{a,i})_{i\leqslant N}$, we see that (6) is equivalent to $(\mathbf{g}^a, J)/N^{1/2} \geqslant \kappa$ for $\kappa = 0$. Of course, one can then generalize the model by taking a non-zero parameter $\kappa$: taking $\kappa < 0$ weakens the original constraint (6), while taking $\kappa > 0$ gives a more restrictive constraint than (6). This is equivalent to the model (1) with $U(x) = \mathbf{1}\{x \geqslant \kappa\}$. The configurations $J \in \{-1,+1\}^N$ which have a positive weight in (1) are precisely the choices of $(J_{j,0})_{1\leqslant i\leqslant N}$ such that the neural network memorizes the $i = 0$ spin on all $M$ input patterns. To make the connection with the question considered in this paper, note that if the asymptotic free energy density is positive, there are many valid choices of $(J_{j,0})_{1\leqslant i\leqslant N}$, so we expect that this corresponds to $\alpha = M/N$ being below the storage capacity $\alpha_{\mathrm{c}}$. For the models discussed in this paper, it is conjectured that $\mathrm{RS}(\alpha; U)$ is a strictly decreasing function of $\alpha \geqslant 0$, and that $\alpha_{\mathrm{c}}$ corresponds to the unique positive root of this function. Our main result Theorem 1.1 addresses a subcritical regime, where $\alpha/\alpha_{\mathrm{c}}$ is small.

The two most commonly studied variants of the model are the **Ising perceptron** where $J_i \in \{-1,+1\}$ (as in this paper), and the **spherical perceptron** where $J = (J_i)_{i\leqslant N}$ is restricted to the sphere of radius $N^{1/2}$; these are both discussed further below. (Both the replica symmetric formula and the value of $\alpha_{\mathrm{c}}$ depend on $U$, and on whether the model is spherical versus Ising.)

### 1.2.1. NON-RIGOROUS RESULTS FROM STATISTICAL PHYSICS

In the physics literature, the spherical perceptron model with the threshold activation function $U(x) = \mathbf{1}\{x \geqslant \kappa\}$ for $\kappa \geqslant 0$ was analyzed in a series of celebrated works (Gardner, 1987, 1988; Gardner and Derrida, 1988, 1989), using the non-rigorous **replica method**. In general terms, the replica method starts from the observation that

$$\log \boldsymbol{Z} = \lim_{n\downarrow 0} \frac{\boldsymbol{Z}^n - 1}{n}\,.$$

The replica method is then to calculate $\mathbb{E}(\boldsymbol{Z}^n)$ for large integer $n$, and apply analytic continuation to take the limit $n \downarrow 0$. The expectation $\mathbb{E}$ is over the disorder of the system, which in the case of the perceptron model is the random matrix $\boldsymbol{G}$. The $n$-th moment $\mathbb{E}(\boldsymbol{Z}^n)$ is the expected partition function of $n$ **replicas** of the same random system. The calculation of $\mathbb{E}(\boldsymbol{Z}^n)$ is typically a saddle point analysis, and the result is called **replica symmetric** if the optimal saddle point has the $n$ replicas behaving independently, even though they are coupled through the shared disorder $\boldsymbol{G}$. For the spherical perceptron with $U(x) = \mathbf{1}\{x \geqslant \kappa\}$ — where $\boldsymbol{Z}$ is the volume of the intersection of the sphere in $\mathbb{R}^N$ with the random half-spaces — this calculation was carried out by Gardner and Derrida, yielding a conjectured replica symmetric limiting formula for $N^{-1}\log \boldsymbol{Z}$ similar to (4).

The replica method also applies to the Ising perceptron with $U(x) = \mathbf{1}\{x \geqslant \kappa\}$ for any $\kappa \in \mathbb{R}$, but the original Gardner–Derrida analysis contained an error leading to incorrect predictions. A corrected replica calculation for the Ising model was given by Krauth and Mézard (1989); this is the first appearance of the correct prediction for the right-hand side of (4). The same results were rederived using the **cavity method** by Mézard (1989). Roughly speaking, the basic idea of this method is to estimate

$$\frac{1}{N}\log \boldsymbol{Z}(\boldsymbol{G}_{M\times N}) \approx \mathbb{E}\log\frac{\boldsymbol{Z}(\boldsymbol{G}_{M\times(N+1)})}{\boldsymbol{Z}(\boldsymbol{G}_{M\times N})} + \alpha\,\mathbb{E}\log\frac{\boldsymbol{Z}(\boldsymbol{G}_{(M+1)\times N})}{\boldsymbol{Z}(\boldsymbol{G}_{M\times N})}\,,$$

where on the right-hand side the first term is the effect of adding one more spin $J_{N+1}$, and the second term is the effect of adding one more pattern $\mathbf{g}^a$. Both terms can be computed heuristically by making assumptions about the structure of the **Gibbs measure**

$$\mu(J) \equiv \frac{1}{\boldsymbol{Z}(\boldsymbol{G})} \prod_{a \leqslant M} U\left(\frac{(\mathbf{g}^a, J)}{N^{1/2}}\right). \tag{7}$$

(When $U$ is $\{0,1\}$-valued, $\mu$ is simply the uniform probability measure on all configurations $J$ that give a non-zero contribution in the sum (1). For instance, in the half-space intersection model $U(x) = \mathbf{1}\{x \geqslant \kappa\}$, $\mu$ is the uniform measure on the intersection of half-spaces appearing in (2).) In particular, the **replica symmetric** hypothesis says, roughly speaking, that any $O(1)$ subset of coordinates are asymptotically independent under the Gibbs measure $\mu$. The replica and cavity methods are both non-rigorous, and are regarded by physicists to be morally equivalent to one another — in particular, the interpretation of replica symmetry in the replica method (independent replicas) is expected to be essentially equivalent to the meaning in the cavity method (independence on any $O(1)$ subset of coordinates). However, the cavity method may be generally considered to yield more transparent derivations.

The Gardner–Derrida and Krauth–Mézard predictions primarily concern the replica symmetric regime. The spherical perceptron with $U(x) = \mathbf{1}\{x \geqslant \kappa\}$ (also called the *positive spherical perceptron*) is expected to be replica symmetric for all $\kappa \geqslant 0$ and all $\alpha \leqslant \alpha_{\mathrm{c}}$. In contrast, the Ising perceptron with $U(x) = \mathbf{1}\{x \geqslant \kappa\}$ is expected to be replica symmetric for all $\kappa \in \mathbb{R}$. Our Theorem 1.1 shows that for a more general class of activation functions $U$, the Ising perceptron has the replica symmetric free energy for $\alpha$ small enough; it leaves open the question of what happens for larger $\alpha$. More recently there have been several works in the physics literature investigating the spherical perceptron model with $U(x) = \mathbf{1}\{x \geqslant \kappa\}$ for $\kappa < 0$ (also called the *negative spherical perceptron*), which is expected to exhibit replica symmetry breaking, e.g. Franz and Parisi (2016); Franz et al. (2017).

### 1.2.2. RIGOROUS RESULTS ON THE SPHERICAL PERCEPTRON

The mathematical literature contains numerous very strong results on the spherical perceptron for $U(x) = \mathbf{1}\{x \geqslant \kappa\}$, especially for $\kappa \geqslant 0$ (conjecturally the replica symmetric regime). For $\kappa = 0$, the storage capacity $\alpha_{\mathrm{c}} = 2$ was known since the 1960s (Wendel, 1962; Cover, 1965). For general $\kappa \geqslant 0$, the storage capacity $\alpha_{\mathrm{c}}(\kappa)$ was proved by a short and elegant argument (Stojnic, 2013), using convex duality together with Gordon's gaussian minimax comparison inequality (Gordon, 1985, 1988; Thrampoulidis et al., 2014). However, perhaps the most striking result for this model is that of Shcherbina and Tirozzi (2003), proving the Gardner free energy formula for the spherical perceptron for all $\kappa \geqslant 0$ and all $\alpha$ up to $\alpha_{\mathrm{c}}(\kappa)$. The proof of Shcherbina and Tirozzi (2003) makes crucial use of the classical Brunn–Minkowski inequality for volumes of bodies in euclidean space (Lusternik, 1935; Hadwiger and Ohmann, 1956). The main result of Shcherbina and Tirozzi (2003) was later reproved (Talagrand, 2011a, Ch. 3) and (Talagrand, 2011b, Ch. 8) with a perhaps simpler argument, using instead the functional Brunn–Minkowski (Prékopa–Leindler) inequality (Prékopa, 1971; Leindler, 1972; Prékopa, 1973). This inequality implies concentration of Lipschitz functionals under strongly logconcave measures (Maurey, 1991), which can be used to deduce concentration of overlaps and cavity equations (see e.g. Talagrand, 2011a, Thm. 3.1.11).[4] As noted by Shcherbina and Tirozzi (2003) and Talagrand (2011a, §3.4), similar concentration results can also be obtained

[4] In this work we have also used the result of Maurey (1991) (restated in Theorem B.12), but only to prove Proposition 1.3 which is not required for the main result Theorem 1.1.

using instead the Brascamp–Lieb inequality (Brascamp and Lieb, 1976); and indeed this idea appears in earlier work on the Hopfield model (Bovier and Gayrard, 1998). Thus, all existing results on the positive spherical perceptron (excluding the case $\kappa = 0$) use powerful tools from **convex geometry**.[5]

### 1.2.3. RIGOROUS RESULTS ON THE ISING PERCEPTRON

The mathematical literature on the Ising perceptron is far less advanced than for the spherical perceptron. For the half-space model, the free energy was computed heuristically by Krauth and Mézard (1989); their method applies also to the more general model (1). One consequence of that calculation is an explicit prediction $\alpha_\star$ for the storage capacity $\alpha_{\rm c}$ for the model $U(x) = \mathbf{1}\{x \geqslant \kappa\}$ — for $\kappa = 0$, the conjectured threshold $\alpha_\star$ is approximately 0.83.

In the rigorous literature, most results concern the half-space model $U(x) = \mathbf{1}\{x \geqslant 0\}$.[6] For this model, it was shown by Kim and Roche (1998) and Talagrand (1999b) that there is a small absolute constant $\epsilon > 0$ such that the transition must occur between $\epsilon$ and $1-\epsilon$: that is, the partition function (1) is non-zero with high probability for $\alpha \leqslant \epsilon$, and zero with high probability for $\alpha \geqslant 1-\epsilon$. A more recent work of Ding and Sun (2018) (further discussed below) uses some of the methods of this paper to show, under a certain variational hypothesis, that the partition function is non-zero with *non-negligible* probability for $\alpha < \alpha_\star$, where $\alpha_\star$ is the conjectured threshold from Krauth and Mézard (1989). A more recent work of Xu (2021) confirms that the model indeed has a *sharp* threshold, meaning that $\mathbb{P}(\boldsymbol{Z} > 0)$ transitions from $1 - o_N(1)$ to $o_N(1)$ in an $o_N(1)$ window of $\alpha$.[7]

For the situation where we have a more general function $U$ in (1), Talagrand (2000) (see also Talagrand, 2011a, Ch. 2) proves that the limiting free energy is given by the replica symmetric formula $\mathrm{RS}(\alpha; U)$, for small enough $\alpha$, under the assumption that the function $u \equiv \log U$ is **uniformly bounded**. This corresponds to the case of our main result Theorem 1.1 where $u$ is bounded, which we prove at the end of Section D. Even for bounded $u$, the two proofs are very different: Talagrand (2000) uses an interpolation method to derive replica symmetric equations, while this paper uses first and second moments conditional on the AMP iteration. We remark also that the argument of Talagrand (2000) seemingly needs to go through a smoothed approximation of $u$, while our proof for bounded $u$ requires no smoothing.

In comparison with previous work of Talagrand, the main new result of this work is that the limiting free energy is given by the replica symmetric formula $\mathrm{RS}(\alpha; U)$, for small enough $\alpha$, for all $U$ satisfying Assumptions 1 and 2. A special case of this result, for the half-space model $U(x) = \mathbf{1}\{x \geqslant \kappa\}$, was previously obtained in (Talagrand, 2011a, Ch. 9) (with partial results appearing in a previous work (Talagrand, 1999a)).[8] Talagrand's proof for the half-space model relies crucially on an estimate (Talagrand, 2011b, Thm. 8.2.4) which says roughly that if $(u_i)_{i \leqslant n}$ is a near-isotropic gaussian process, then the fraction of indices $i$ where $u_i \geqslant \kappa$ cannot be too small. The proof

[5] The Prékopa–Leindler inequality generalizes the Brunn–Minkowski inequality, and also can be used to deduce the Brascamp–Lieb inequality (Bobkov and Ledoux, 2000). For more on the relations among these inequalities we refer to the survey of Gardner (2002).

[6] The existing results for $U(x) = \mathbf{1}\{x \geqslant 0\}$ can likely be extended to cover $U(x) = \mathbf{1}\{x \geqslant \kappa\}$ for any $\kappa \in \mathbb{R}$.

[7] To be precise, the result of Ding and Sun (2018) is with gaussian noise $\boldsymbol{G}$ (as in this paper), while the other results (Kim and Roche, 1998; Talagrand, 1999b; Xu, 2021) are for the Bernoulli noise model where $g_{a,i}$ are i.i.d. symmetric random signs. It is reasonable to expect that the results of Kim and Roche (1998); Talagrand (1999b); Xu (2021) can be transferred to the gaussian noise model.

[8] The function $U(x) = \mathbf{1}\{x \geqslant \kappa\}$ satisfies the hypothesis of Theorem 1.1: it clearly satisfies Assumption 1, and one can check that it satisfies Assumption 2 either by direct calculation or by applying Proposition 1.3.

of this estimate uses a gaussian comparison inequality (see (Talagrand, 2011a, Lem. 1.3.1) and (Talagrand, 2011b, Propn. 8.2.2)), and does not extend for instance to the event $u_i \in E$ where $E$ is a bounded measurable subset of $\mathbb{R}$. In this paper we prove an analogous (although quantitatively weaker) estimate for general $E$ by different methods (Proposition F.1), and use this in the proof of Theorem 1.1 in the case of unbounded $u$.

### 1.2.4. BELIEF PROPAGATION AND TAP

The main idea in the proof of Theorem 1.1, which we discuss further in §1.3 below, is to **compute (first and second) moments of the partition function** (1) **conditional on the AMP filtration**. The motivation originates from the **TAP (Thouless–Anderson–Palmer)** framework, which was introduced for the classical Sherrington–Kirkpatrick model (Sherrington and Kirkpatrick, 1975) by Thouless et al. (1977) (and further investigated by de Almeida and Thouless (1978); Plefka (1982)). We describe the TAP idea heuristically, in the context of the perceptron (1). Given $q \in [0,1)$ let

$$F_q(x) \equiv \frac{1}{(1-q)^{1/2}} \frac{\mathbb{E}_\xi[\xi U(x+(1-q)^{1/2}\xi)]}{\mathbb{E}_\xi U(x+(1-q)^{1/2}\xi)} \,. \tag{8}$$

In Proposition A.1 we will show that the fixed-point equation

$$\begin{pmatrix} q \\ \psi \end{pmatrix} = \begin{pmatrix} \bar{q}(\psi) \\ \alpha\bar{r}(q) \end{pmatrix} \equiv \begin{pmatrix} \mathbb{E}[\operatorname{th}(\psi^{1/2}Z)^2] \\ \alpha\mathbb{E}[F_q(q^{1/2}Z)^2] \end{pmatrix} \tag{9}$$

has a unique solution in a certain regime, which we hereafter denote $(q, \psi)$. For the model (1), the TAP equations (see Mézard (1989, 2017); and explained futher below) read

$$\mathbf{m} \equiv \operatorname{th}(\mathbf{H}) = \operatorname{th}\left(\frac{\boldsymbol{G}^{\mathsf{t}}\mathbf{n}}{N^{1/2}} - \beta\mathbf{m}\right), \quad \beta = \alpha\mathbb{E}(F_q)'(q^{1/2}Z) \tag{10}$$

$$\mathbf{n} \equiv F_q(\mathbf{h}) = F_q\left(\frac{\boldsymbol{G}\mathbf{m}}{N^{1/2}} - \beta'\mathbf{n}\right), \quad \beta' = 1-q\,, \tag{11}$$

where the functions th and $F_q$ are applied coordinatewise, $\mathbf{m} \equiv \operatorname{th}(\mathbf{H})$ is a vector in $(-1,+1)^N$ with $\|\mathbf{m}\|^2/N = q$, and $\mathbf{n} \equiv F_q(\mathbf{h})$ is a vector in $\mathbb{R}^M$ with $\|\mathbf{n}\|^2/N = \psi$. The terms $\beta\mathbf{m}$ and $\beta'\mathbf{n}$ are the **Onsager corrections** (more below). For the model (1) at small $\alpha$, it is conjectured that the TAP equations (10) and (11) have a unique solution $(\mathbf{m}^\star, \mathbf{n}^\star)$, such that the vector $\mathbf{m}^\star$ approximates the mean value of a random configuration $J$ sampled from the **Gibbs measure** $\mu$ defined by (7). The vector $\mathbf{n}^\star$ describes the distribution of the vector $\boldsymbol{G}J/N^{1/2}$ where $J$ is sampled from $\mu$.[9] It is further expected that $N^{-1}\log \boldsymbol{Z}$ concentrates very well around a **TAP free energy** $\Phi(\mathbf{m}^\star, \mathbf{n}^\star)$, which in turn concentrates (more on this below) around the **replica symmetric value**

$$\mathrm{RS}(\alpha; U) = -\frac{\psi(1-q)}{2} + \mathbb{E}\left\{\log 2\operatorname{ch}(\psi^{1/2}Z) + \alpha\log\mathbb{E}_\xi U\Big(q^{1/2}Z + (1-q)^{1/2}\xi\Big)\right\}, \tag{12}$$

where $Z$ and $\xi$ are independent standard gaussians. Note (12) is the quantity in Theorem 1.1.

The TAP equations and TAP free energy can be viewed as a dense limit of the **belief propagation (BP) equations** and **Bethe free energy**. We describe this briefly, and refer to Mézard (1989,

[9] Note that $\mathbf{m}^\star$, $\mathbf{n}^\star$, and $\mu$ all depend on $\boldsymbol{G}$. These statements are conditional on a typical realization $\boldsymbol{G}$.

2017) for the details. The basic idea is to consider the analogues of (7) with the $a$-th factor removed, or with the $i$-th spin removed; let us denote these $\mu^{-a}$ and $\mu_{-i}$. Write $\Delta_a \equiv (\mathbf{g}^a, J)/N^{1/2}$. The belief propagation (BP) equations for the model (1) have a total of $2MN$ variables $m_{i\to a}$ and $n_{a\to i}$ (for $i \leqslant N$ and $a \leqslant M$), with the following interpretation:

$$\begin{aligned} m_{i\to a} &= \text{“mean of } J_i \text{ under } \mu^{-a}\text{, i.e. in absence of } a\text{-th factor,”}\\ n_{a\to i} &= \text{“mean of } \Delta_a \text{ under } \mu_{-i}\text{, i.e. in absence of } i\text{-th spin.”}\end{aligned}$$

The **BP equations** are a closed system of heuristic equations among these $2MN$ variables: $m_{i\to a}$ is expressed as a function of $(g_{bi}, n_{b\to i})$ for $b \in [M]\backslash a$, and $n_{a\to i}$ is expressed as a function of $(g_{aj}, m_{j\to a})$ for $j \in [N]\backslash i$. The equations are derived assuming the “replica symmetric” hypothesis described in §1.2.1. The **Bethe free energy** $\Phi^{\text{Bethe}}(\mathbf{m}_{\text{BP}}, \mathbf{n}_{\text{BP}})$ is a heuristic approximation for $N^{-1}\log \boldsymbol{Z}$ as a function of the BP solution $(\mathbf{m}_{\text{BP}}, \mathbf{n}_{\text{BP}})$. Note the BP solution depends on the random disorder $\boldsymbol{G}$, so the Bethe free energy depends on $\boldsymbol{G}$ also. The Bethe free energy is expected to be a good approximation for the true free energy in the replica symmetric regime.

The TAP equations above can be viewed as a dense limit of the BP equations, as follows. Since every spin $i \leqslant N$ interacts with every factor $a \leqslant N$, the differences $m_{i\to a} - m_i$ will be small in the large-$N$ limit, although not completely negligible. Similarly, all the $n_{a\to i}$ ($i \leqslant N$) will be close to a single value $n_a$. In absence of the $a$-th factor, we have $\Delta_a = (\mathbf{g}^a, J)/N^{1/2}$ where each $J_i$ is a random sign with mean $m_{i\to a}$. If the $J_i$ are not too correlated (cf. the discussion of replica symmetry in §1.2.1), it is reasonable to expect that the law of $\Delta_a$ under $\mu^{-a}$ is roughly gaussian with mean $h_a$ and variance $1 - q_a$, where

$$h_a \equiv \frac{1}{N^{1/2}}\sum_{i\leqslant N} g_{a,i} m_{i\to a} \qquad 1 - q_a \equiv \frac{1}{N}\sum_{i\leqslant N} (g_{a,i})^2\Big(1 - (m_{i\to a})^2\Big)\,.$$

This suggests that, once we add back in the $a$-th factor, the mean of $\Delta_a$ under $\mu$ will be

$$\frac{\mathbb{E}_\xi[(h_a + (1-q_a)^{1/2}\xi)U(h_a + (1-q_a)^{1/2}\xi)]}{\mathbb{E}_\xi U(h_a + (1-q_a)^{1/2}\xi)} = h_a + (1-q_a)F_{q_a}(h_a)\,.$$

On the other hand, from the definition $\Delta_a = (\mathbf{g}^a, J)/N^{1/2}$, the mean of $\Delta_a$ under $\mu$ should also coincide with $(\mathbf{g}^a, \mathbf{m})$ where $\mathbf{m}$ is the mean of $J$ under $\mu$. This explains the rationale for the second TAP equation (11) above, which arises from equating the last two displays and substituting $q_a = q$. The reason for this substitution is that $\|\mathbf{m}\|^2/N = q$, and $m_{i\to a}$ is close to $m_i$. On the other hand, in the equation for $h_a$ we cannot simply replace $m_{i\to a}$ by $m_i$, and the Onsager correction in (11) takes into account that the discrepancy $m_{i\to a} - m_i$ is correlated with $g_{a,i}$. The other TAP equation (10) is derived by analogous considerations.

Ultimately, the **TAP equations** are a closed system of equations among the $M + N$ variables $m_i$ and $n_a$, which can be viewed as a simplification of the BP equations described above. The **TAP free energy** $\Phi(\mathbf{m}_\star, \mathbf{n}_\star)$ is a heuristic approximation for $N^{-1}\log\boldsymbol{Z}$ as a function of the TAP solution $(\mathbf{m}_\star, \mathbf{n}_\star)$, and it can be regarded as a simplification of the Bethe free energy. The TAP solution depends on the random disorder $\boldsymbol{G}$, so the TAP free energy depends on $\boldsymbol{G}$ also. The TAP approximation is expected to be valid throughout the replica symmetric regime, where we expect

$$\frac{1}{N}\Big|\log \boldsymbol{Z}(\boldsymbol{G}) - \Phi(\mathbf{m}_\star, \mathbf{n}_\star; \boldsymbol{G})\Big| \leqslant \frac{O_p(1)}{N}\,, \qquad \Big|\frac{1}{N}\Phi(\mathbf{m}_\star, \mathbf{n}_\star; \boldsymbol{G}) - \text{RS}(\alpha; U)\Big| \leqslant \frac{O_p(1)}{N^{1/2}}\,. \tag{13}$$

That is, conjecturally, the TAP solution captures “most” of the randomness in the disordered system, which fluctuates around a deterministic thermodynamic limit described by $\mathrm{RS}(\alpha; U)$. For more work on the general TAP framework in a variety of settings, we refer to Chen et al. (2018, 2021); Fan et al. (2021); Ben Arous and Jagannath (2021); Adhikari et al. (2021).

### 1.2.5. AMP AND CONDITIONING

As we commented in Remark 1.2, if we have $\mathbb{E}_\xi[\xi U(\xi)] = 0$ (i.e. if the assumption (3) does not hold) then the (unconditional) first and second moment method can be used to analyze the partition function $\boldsymbol{Z}$ from (1), following Aubin et al. (2019). If $\mathbb{E}_\xi[\xi U(\xi)] \neq 0$, however, it is well known that the unconditional moment method does not say anything about the random variable $\boldsymbol{Z}$, because in fact $\boldsymbol{Z} \ll \mathbb{E}\boldsymbol{Z}$ with high probability at any positive $\alpha = M/N$. The first moment $\mathbb{E}\boldsymbol{Z}$ overestimates the typical value of $\boldsymbol{Z}$ because it is dominated by rare events where the disorder $\boldsymbol{G}$ favors large $\boldsymbol{Z}$ in some atypical way.

The discussion of §1.2.4 leads to the following idea for improving the moment calculation. Since the TAP fixed point $(\mathbf{m}^\star, \mathbf{n}^\star)$ is described by a relatively simple set of equations (10) and (11), and is conjectured to carry a great deal of information about the random measure (7), it is natural to consider the first and second moment method **conditional on the TAP solution** $(\mathbf{m}^\star, \mathbf{n}^\star)$. Indeed, the prediction (13) suggests that the fluctuations of $N^{-1} \log \boldsymbol{Z}$ away from $\mathrm{RS}(\alpha; U)$ are mostly accounted for by the randomness in the TAP free energy $\Phi(\mathbf{m}^\star, \mathbf{n}^\star)$. It is then natural to attempt to show that

$$\frac{\mathbb{E}(\boldsymbol{Z} \,|\, \mathbf{m}^\star, \mathbf{n}^\star)}{\exp(N\mathrm{RS}(\alpha; U))} \approx \frac{\mathbb{E}(\boldsymbol{Z}^2 \,|\, \mathbf{m}^\star, \mathbf{n}^\star)}{\mathbb{E}(\boldsymbol{Z} \,|\, \mathbf{m}^\star, \mathbf{n}^\star)^2} \approx 1\,,$$

and thereby deduce the desired conclusion (4).

A major problem with the above approach is that it is not in fact known that the equations (10) and (11) have a unique solution, although this is conjectured to be true in the replica symmetric regime. As a result, “conditioning on the TAP solution” is not a mathematically justified approach. A way to get around this issue (while implementing the same high-level strategy) is to condition instead on the **AMP (approximate message passing) iteration**, which constructs approximate solutions of the TAP equations, and will be described in more detail in §1.3 below. The asymptotic behavior of AMP has been rigorously characterized (Bayati and Montanari, 2011; Bolthausen, 2014), and this substitutes for the unproven properties of the TAP solution.

The idea of **conditioning on the AMP iteration** was introduced by Ding and Sun (2018); Bolthausen (2019) and has been developed in subsequent works (Alaoui and Sellke, 2020; Fan and Wu, 2021; Brennecke and Yau, 2021). Of these prior works, Bolthausen (2019) and Brennecke and Yau (2021) concern the classical Sherrington–Kirkpatrick (SK) model with a gaussian coupling matrix (i.e., the Hamiltonian is a scalar multiple of $J^{\mathrm{t}}\boldsymbol{G}J$ where $\boldsymbol{G}$ is an $N \times N$ matrix with i.i.d. random gaussian entries). To make the analogy, the condition $\mathbb{E}_\xi[\xi U(\xi)] = 0$ in the perceptron (cf. (3)) is analogous to having zero external field in the SK model. For the SK model with zero external field, the asymptotic behavior of the partition function is characterized in the entire high-temperature regime by Aizenman et al. (1987, 1988). By contrast, the SK model with non-zero external field remains not fully understood in the high-temperature regime. The work of Fan and Wu (2021) concerns more general SK models with random orthogonally invariant coupling matrices, and uses a simplified “memory-free” AMP iteration that was developed and analyzed by Opper and Winther (2001); Opper et al. (2016); Çakmak and Opper (2019); Fan (2020). The works of Ding and Sun (2018) and Alaoui and Sellke (2020) concern the perceptron model, but only use the AMP conditioning method for lower bounds. In the current work, we show that the AMP conditioning method gives sharp upper and lower bounds for the generalized perceptron (1) at small $\alpha$.

### 1.2.6. OTHER RELATED WORK

As noted above, in the special case that $U$ satisfies $\mathbb{E}_\xi[\xi U(\xi)] = 0$ (i.e. if assumption (3) does not hold), the model (1) is mathematically much more tractable, and can be analyzed by an (unconditional) second moment method. The condition $\mathbb{E}_\xi[\xi U(\xi)] = 0$ holds for instance if $U$ is a bounded **symmetric** function. The second moment analysis was done for the cases $U(x) = \mathbf{1}\{|x| \leqslant \kappa\}$ and $U(x) = \mathbf{1}\{|x| \geqslant \kappa\}$ in Aubin et al. (2019). For the model $U(x) = \mathbf{1}\{|x| \leqslant \kappa\}$, much finer structural results (on the typical geometry of the solution space) were obtained by Perkins and Xu (2021); Abbe et al. (2021). These results were inspired in part by questions raised in the physics literature about the algorithmic accessibility of CSP solutions (see e.g. Baldassi et al., 2016; Budzynski et al., 2019). For the perceptron model in statistical settings, there is an extensive literature which we will not describe here; we refer the reader for instance to Barbier et al. (2019); Montanari et al. (2021) and many references therein. Lastly, we remark that while "naive mean field" would approximate the entire Gibbs measure (7) by product measures, the TAP framework goes beyond this by requiring independence only on $O(1)$ subsets of coordinates. It remains an open question to prove general results for TAP in the spirit of what has been done for the mean-field approximation by Jain et al. (2018, 2019); Eldan (2020); Eldan and Gross (2018); this was another motivation for this project.

## 1.3. AMP iteration and conditional moment results

In this subsection we outline the main steps in the proof of Theorem 1.1. We first introduce the AMP iteration in more detail. Our convention throughout is that if $f : \mathbb{R} \to \mathbb{R}$ and $\mathbf{z} \equiv (z_j)_j$ is any vector, then $f(\mathbf{z}) \equiv (f(z_j))_j$ denotes the vector of the same length which results from applying $f$ componentwise to $\mathbf{z}$. Recall $F \equiv F_q$ from (8). Let $\mathbf{m}^{(0)} = \mathbf{0} \in \mathbb{R}^N$, $\mathbf{n}^{(0)} = \mathbf{0} \in \mathbb{R}^M$, $\mathbf{m}^{(1)} = q^{1/2}\mathbf{1} \in \mathbb{R}^N$, $\mathbf{n}^{(1)} = (\psi/\alpha)^{1/2}\mathbf{1} \in \mathbb{R}^M$. The **approximate message passing (AMP)** iteration for the perceptron model is given by (cf. (228) and (229))

$$\mathbf{m}^{(t+1)} \equiv \operatorname{th}(\mathbf{H}^{(t+1)}) = \operatorname{th}\left(\frac{\boldsymbol{G}^{\mathsf{t}}\mathbf{n}^{(t)}}{N^{1/2}} - \beta\mathbf{m}^{(t-1)}\right), \tag{14}$$

$$\mathbf{n}^{(t+1)} \equiv F(\mathbf{h}^{(t+1)}) = F\left(\frac{\boldsymbol{G}\mathbf{m}^{(t)}}{N^{1/2}} - \beta'\mathbf{n}^{(t-1)}\right). \tag{15}$$

Recall from the discussion of §1.2.5 that the main idea in the proof of Theorem 1.1 is to **compute (first and second) moments of the partition function (1) conditional on the AMP filtration**

$$\mathscr{F} \equiv \mathscr{F}(t) \equiv \sigma\Big(\Big(\boldsymbol{G}\mathbf{m}^{(s)}, \mathbf{n}^{(s+1)} : s \leqslant t\Big), \Big(\boldsymbol{G}^{\mathsf{t}}\mathbf{n}^{(\ell)}, \mathbf{m}^{(\ell+1)} : \ell \leqslant t-1\Big)\Big) \tag{16}$$

in the limit $t \to \infty$. The computation relies on existing results on the asymptotic behavior of AMP in the large-$N$ limit from Bayati and Montanari (2011) and Bolthausen (2014) (see also Donoho et al., 2009; Javanmard and Montanari, 2013; Rush and Venkataramanan, 2018; Berthier et al., 2020). In §A.2 we review the relevant results from Bayati and Montanari (2011); Bolthausen (2014) that are used in our proofs. The results from our conditional method of moments calculation are summarized as follows:

**Theorem 1.4 (conditional first moment)** *If $U$ satisfies Assumptions 1 and 2, then there exists a positive constant $\alpha(U) > 0$ such that, if $\boldsymbol{G}$ is an $M \times N$ matrix with i.i.d. standard gaussian entries and $M/N \to \alpha$ with $0 \leqslant \alpha \leqslant \alpha(U)$, and $\mathscr{F}(t)$ is the AMP filtration defined by (16), then*

$$\mathbb{E}\Big(\boldsymbol{Z}\,\Big|\,\mathscr{F}(t)\Big) \leqslant \exp\Big\{N\Big(\mathrm{RS}(\alpha;U) + o_t(1)\Big)\Big\}$$

*with high probability (i.e., with probability $1 - o_N(1)$).*

Theorem 1.4 implies the upper bound in Theorem 1.1 by standard arguments, using Markov's inequality. The proof of the upper bound in Theorem 1.1 is therefore given at the end of Section C, after the proof of Theorem 1.4.

**Theorem 1.5 (conditional second moment)** *Suppose $U$ satisfies Assumptions 1 and 2, and $0 \leqslant \alpha \leqslant \alpha(U)$ as defined by (27). If $\boldsymbol{G}$ is an $M \times N$ matrix with i.i.d. standard gaussian entries and $M/N \to \alpha$, we can construct a random variable $\bar{\boldsymbol{Z}} \leqslant \boldsymbol{Z}$ (formally defined by (144)) such that*

$$\mathbb{E}\Big(\bar{\boldsymbol{Z}}(\boldsymbol{G})\,\Big|\,\mathscr{F}(t)\Big) \geqslant \exp\Big\{N\Big(\mathrm{RS}(\alpha;U) - o_t(1)\Big)\Big\} \tag{17}$$

*with high probability, and for which we have the second moment estimate*

$$\mathbb{E}\Big(\bar{\boldsymbol{Z}}(\boldsymbol{G})^2\,\Big|\,\mathscr{F}(t)\Big) \leqslant \exp\Big\{2N\Big(\mathrm{RS}(\alpha;U) + o_t(1)\Big)\Big\}, \tag{18}$$

*also with high probability.*

In Theorem 1.5, the restricted partition function $\bar{\boldsymbol{Z}}$ is essentially the contribution to the partition function (1) from all configurations $J$ that approximately satisfy

$$J - \mathbf{m}^{(t)} \perp \operatorname{span}\Big\{\mathbf{m}^{(s)}, \mathbf{H}^{(s)} : s \leqslant t\Big\} \tag{19}$$

(this condition is formalized by (144)). A similar restriction was introduced by Ding and Sun (2018) in the context of the Ising perceptron, and was also subsequently used by Brennecke and Yau (2021) to obtain an improvement on the result of Bolthausen (2019) in the context of the SK model.

In the *bounded case* $\|u\|_\infty < \infty$ (recall $u \equiv \log U$), Theorem 1.5 implies the lower bound in Theorem 1.1 by standard arguments, using the Azuma–Hoeffding martingale inequality. The proof of the lower bound in Theorem 1.1 in the bounded case is given at the end of Section D, after the proof of Theorem 1.5. In the more general setting where $u$ may be unbounded, the proof of Theorem 1.1 requires further estimates, as we outline in the next subsection.

### 1.4. Concentration results for unbounded case

Assumption 1 implies that we must have

$$1 \geqslant U(x) > \delta' \mathbf{1}\{x \in E(U)\} \tag{20}$$

where $\delta'$ is a positive constant, and $E(U)$ is a subset of the real line of positive Lebesgue measure (which we denote $|E(U)|$). Moreover we can assume without loss that $E(U)$ is bounded, i.e., $E(U) \subseteq [-E_{\max}(U), E_{\max}(U)]$ for some finite $E_{\max}(U)$. Following (Talagrand, 2011b, §8.3), define the truncated logarithm $\log_A(x) \equiv \max\{-A, \log x\}$. The following is an adaptation of (Talagrand, 2011b, Propn. 9.2.6) (see also (Talagrand, 2011b, Propn. 8.3.6)):

**Proposition 1.6** *Suppose $U$ satisfies Assumption 1, and let $\delta'$ and $E(U)$ be as above. Then for $\tau = \exp(-12)$ we have*

$$\mathbb{P}\bigg(\frac{1}{N}\bigg|\log_{N\tau}\bigg(\frac{\boldsymbol{Z}}{2^N}\bigg) - \mathbb{E}\log_{N\tau}\bigg(\frac{\boldsymbol{Z}}{2^N}\bigg)\bigg| \geqslant \frac{(\log N)^2}{N^{1/2}}\bigg) \leqslant \frac{1}{N^2}$$

*for all $N$ large enough (depending on $|E(U)|$, $E_{\max}(U)$, and $\delta'$).*

Next let $\eta$ be a small positive constant, and consider the smoothed function

$$U_\eta(x) \equiv (U * \varphi_\eta)(x) = \int U(x+\eta z)\varphi(z)\,dz = \mathbb{E}_\xi U(x+\eta\xi)\,. \tag{21}$$

Let $\boldsymbol{Z}(\eta)$ denote the perceptron partition function with $U_\eta$ in place of $U$:

$$\boldsymbol{Z}(\eta) \equiv \sum_J \prod_{a\leqslant M} U_\eta\bigg(\frac{(\mathbf{g}^a, J)}{N^{1/2}}\bigg)\,. \tag{22}$$

Note that $U_\eta$ satisfies Assumption 1: it is a smooth mapping from $\mathbb{R}$ into $[0,1]$ for any $\eta > 0$, and condition (3) holds for $\eta$ small enough. We will show (see Lemma B.9) that $K_2(U_\eta)$ can be bounded in terms of $K_{2,\wr}(U)$. We then have the following approximation result:

**Proposition 1.7** *Suppose $U$ satisfies Assumption 1, and let $\delta'$ and $E(U)$ be as above. Then for $\tau = \exp(-12)$ we have*

$$\limsup_{N\to\infty}\frac{1}{N}\bigg|\mathbb{E}\bigg[\log_{N\tau}\bigg(\frac{\boldsymbol{Z}(\eta)}{2^N}\bigg) - \log_{N\tau}\bigg(\frac{\boldsymbol{Z}}{2^N}\bigg)\bigg]\bigg| \leqslant o_\eta(1)\,.$$

Propositions 1.6 and 1.7 are proved in Section F. The proofs rely on a bound for near-isotropic gaussian processes, Proposition F.1, which we mentioned in §1.2.3 above. Finally, we have:

**Proposition 1.8** *If $U$ satisfies Assumption 1, then we have $\lim_{\eta\downarrow 0}\mathrm{RS}(\alpha; U_\eta) = \mathrm{RS}(\alpha; U)$ for all $0 \leqslant \alpha \leqslant \alpha_\wr(U)$ (as defined by (31)).*

**Proposition 1.9** *Suppose $U$ satisfies Assumption 1, and let $\boldsymbol{Z}(\eta)$ be as in (22). Then we have*

$$\mathbb{P}\bigg(\Big|\log\boldsymbol{Z}(\eta) - \mathbb{E}\log\boldsymbol{Z}(\eta)\Big| \geqslant Nx\bigg) \leqslant 32N\cdot\exp\bigg\{-\frac{Nx^2}{32C_2C_1(U;\eta)^2}\bigg\}$$

*for all $0 \leqslant x \leqslant 5(C_2)^{1/2}C_1(U;\eta)$, where $C_2$ is an absolute constant while $C_1(U;\eta)$ depends on $U$ and $\eta$.*

The proof of Proposition 1.8 is given in Section B, while the proof of Proposition 1.9 is given in Section F. Then Propositions 1.6, 1.7, 1.8, and 1.9 can be combined to finish the proof of Theorem 1.1 in the unbounded case $\|u\|_\infty = \infty$. The argument goes roughly as follows: by Propositions 1.6 and 1.7, with high probability

$$\frac{1}{N}\log_{N\tau}\frac{\boldsymbol{Z}}{2^N} - o_N(1) = \frac{1}{N}\mathbb{E}\log_{N\tau}\frac{\boldsymbol{Z}}{2^N} = \frac{1}{N}\mathbb{E}\log_{N\tau}\frac{\boldsymbol{Z}(\eta)}{2^N} + o_\eta(1)\,.$$

By applying Theorem 1.5 to $U_\eta$, and combining with Proposition 1.8 and Proposition 1.9, we obtain

$$\frac{1}{N}\mathbb{E}\log_{N\tau}\frac{\boldsymbol{Z}(\eta)}{2^N} - o_N(1) = \mathrm{RS}(\alpha;U_\eta) - \log 2 = \mathrm{RS}(\alpha;U) - \log 2 + o_\eta(1)\,.$$

For $0 < \alpha \leqslant \alpha(U)$, the above is $\geqslant -\tau/2$ by straightforward estimates (Corollary B.8). Therefore

$$-\frac{\tau}{2} \leqslant \mathrm{RS}(\alpha;U) - \log 2 = o_N(1) + \frac{1}{N}\log_{N\tau}\frac{\boldsymbol{Z}}{2^N} = o_N(1) + \frac{1}{N}\log\frac{\boldsymbol{Z}}{2^N}$$

with high probability, as desired. At the end of Section F we give the conclusion of the proof of Theorem 1.1, where the above sketch is made precise.

### Organization

The remaining sections of the paper are organized as follows:

- In Section A we give a preliminary expression (see Theorem A.12) for the first moment of the perceptron partition function conditional on $\mathscr{F}(t)$.
- In Section B we collect some technical results, including basic consequences of Assumptions 1 and 2. We also give the proofs of Propostions A.1, 1.3, and 1.8.
- In Section C we analyze the conditional first moment calculations from Section A and complete the proof of Theorem 1.4. This leads to the upper bound in Theorem 1.1.
- In Section D we prove Theorem 1.5, which bounds the first and second moments of the (truncated) perceptron partition function conditional on $\mathscr{F}(t)$. From this we deduce the lower bound in Theorem 1.1 for the case $\|u\|_\infty < \infty$.
- In Section E we prove a local central limit theorem (Proposition E.13) which is required for the calculations of Sections A–D.
- In Section F we prove Propositions 1.6, 1.7, and 1.9; and use these to conclude the proof of Theorem 1.1.
- Lastly, in Section G we prove a gaussian resampling identity (Lemma A.16) which is used in the conditional moment calculations of Sections A–D. We also give a heuristic review of the state evolution limit of AMP, which was rigorously established in earlier works (Bayati and Montanari, 2011; Bolthausen, 2014). Finally, in §G.5 we present a simplified version of the moment calculations of this paper, which highlights some of the main ideas.

## Acknowledgments

We are grateful to Andrew Lawrie, Joe Neeman, Elchanan Mossel, and Ofer Zeitouni for many helpful conversations. We also wish to thank the anonymous reviewers of the paper for many helpful comments. Research of S.N. is supported by SNSF grant 176918. Research of N.S. is supported by NSF CAREER grant DMS-1940092 and NSF-Simons grant DMS-2031883.

## References

Emmanuel Abbe, Shuangping Li, and Allan Sly. Proof of the contiguity conjecture and lognormal limit for the symmetric perceptron. arXiv:2102.13069, 2021.

Arka Adhikari, Christian Brennecke, Per von Soosten, and Horng-Tzer Yau. Dynamical approach to the TAP equations for the Sherrington-Kirkpatrick model. *J. Stat. Phys.*, 183(3):Paper No. 35, 27, 2021. ISSN 0022-4715. doi: 10.1007/s10955-021-02773-7. URL https://doi.org/10.1007/s10955-021-02773-7.

M. Aizenman, J. L. Lebowitz, and D. Ruelle. Some rigorous results on the Sherrington-Kirkpatrick spin glass model. *Comm. Math. Phys.*, 112(1):3–20, 1987. ISSN 0010-3616. URL http://projecteuclid.org/euclid.cmp/1104159806.

M. Aizenman, J. L. Lebowitz, and D. Ruelle. Addendum: "Some rigorous results on the Sherrington-Kirkpatrick spin glass model". *Comm. Math. Phys.*, 116(3):527, 1988. ISSN 0010-3616. URL http://projecteuclid.org/euclid.cmp/1104161426.

Ahmed El Alaoui and Mark Sellke. Algorithmic pure states for the negative spherical perceptron. arXiv:2010.15811, 2020.

Benjamin Aubin, Will Perkins, and Lenka Zdeborová. Storage capacity in symmetric binary perceptrons. *J. Phys. A*, 52(29):294003, 32, 2019. ISSN 1751-8113. doi: 10.1088/1751-8121/ab227a. URL https://doi.org/10.1088/1751-8121/ab227a.

Carlo Baldassi, Christian Borgs, Jennifer T Chayes, Alessandro Ingrosso, Carlo Lucibello, Luca Saglietti, and Riccardo Zecchina. Unreasonable effectiveness of learning neural networks: From accessible states and robust ensembles to basic algorithmic schemes. *Proc. Nat. Acad. Sci. U.S.A.*, 113(48):E7655–E7662, 2016.

Jean Barbier, Florent Krzakala, Nicolas Macris, Léo Miolane, and Lenka Zdeborová. Optimal errors and phase transitions in high-dimensional generalized linear models. *Proc. Natl. Acad. Sci. USA*, 116(12):5451–5460, 2019. ISSN 0027-8424. doi: 10.1073/pnas.1802705116. URL https://doi.org/10.1073/pnas.1802705116.

Mohsen Bayati and Andrea Montanari. The dynamics of message passing on dense graphs, with applications to compressed sensing. *IEEE Trans. Inform. Theory*, 57(2):764–785, 2011. ISSN 0018-9448. doi: 10.1109/TIT.2010.2094817. URL https://doi.org/10.1109/TIT.2010.2094817.

Gérard Ben Arous and Aukosh Jagannath. Shattering versus metastability in spin glasses. arXiv:2104.08299, 2021.

Raphaël Berthier, Andrea Montanari, and Phan-Minh Nguyen. State evolution for approximate message passing with non-separable functions. *Inf. Inference*, 9(1):33–79, 2020. ISSN 2049-8764. doi: 10.1093/imaiai/iay021. URL https://doi.org/10.1093/imaiai/iay021.

S. G. Bobkov and M. Ledoux. From Brunn-Minkowski to Brascamp-Lieb and to logarithmic Sobolev inequalities. *Geom. Funct. Anal.*, 10(5):1028–1052, 2000. ISSN 1016-443X. doi: 10.1007/PL00001645. URL https://doi.org/10.1007/PL00001645.

Erwin Bolthausen. An iterative construction of solutions of the TAP equations for the Sherrington-Kirkpatrick model. *Comm. Math. Phys.*, 325(1):333–366, 2014. ISSN 0010-3616. doi: 10.1007/s00220-013-1862-3. URL https://doi.org/10.1007/s00220-013-1862-3.

Erwin Bolthausen. A Morita type proof of the replica-symmetric formula for SK. In *Statistical mechanics of classical and disordered systems*, volume 293 of *Springer Proc. Math. Stat.*, pages 63–93. Springer, Cham, 2019. doi: 10.1007/978-3-030-29077-1_4. URL https://doi.org/10.1007/978-3-030-29077-1_4.

Christer Borell. The Brunn-Minkowski inequality in Gauss space. *Invent. Math.*, 30(2):207–216, 1975. ISSN 0020-9910. doi: 10.1007/BF01425510. URL https://doi.org/10.1007/BF01425510.

AA Borovkov. Generalization and refinement of the integro-local Stone theorem for sums of random vectors. *Theory Probab. Appl.*, 61(4):590–612, 2017.

Anton Bovier and Véronique Gayrard. Hopfield models as generalized random mean field models. In *Mathematical aspects of spin glasses and neural networks*, volume 41 of *Progr. Probab.*, pages 3–89. Birkhäuser Boston, Boston, MA, 1998.

Herm Jan Brascamp and Elliott H. Lieb. On extensions of the Brunn-Minkowski and Prékopa-Leindler theorems, including inequalities for log concave functions, and with an application to the diffusion equation. *J. Functional Analysis*, 22(4):366–389, 1976. doi: 10.1016/0022-1236(76)90004-5. URL https://doi.org/10.1016/0022-1236(76)90004-5.

Christian Brennecke and Horng-Tzer Yau. A note on the replica symmetric formula for the SK model. arXiv:2109.07354, 2021.

Louise Budzynski, Federico Ricci-Tersenghi, and Guilhem Semerjian. Biased landscapes for random constraint satisfaction problems. *Journal of Statistical Mechanics: Theory and Experiment*, 2019(2):023302, 2019.

Burak Çakmak and Manfred Opper. Memory-free dynamics for the Thouless–Anderson–Palmer equations of Ising models with arbitrary rotation-invariant ensembles of random coupling matrices. *Phys. Rev. E*, 99(6):062140, 2019.

Wei-Kuo Chen, Dmitry Panchenko, and Eliran Subag. The generalized TAP free energy. arXiv:1812.05066, 2018.

Wei-Kuo Chen, Dmitry Panchenko, and Eliran Subag. The generalized TAP free energy II. *Comm. Math. Phys.*, 381(1):257–291, 2021. ISSN 0010-3616. doi: 10.1007/s00220-020-03887-x. URL https://doi.org/10.1007/s00220-020-03887-x.

Thomas M Cover. Geometrical and statistical properties of systems of linear inequalities with applications in pattern recognition. *IEEE. Trans. Electron.*, 3:326–334, 1965.

Jairo RL de Almeida and David J Thouless. Stability of the Sherrington–Kirkpatrick solution of a spin glass model. *J. Phys. A*, 11(5):983, 1978.

Jian Ding and Nike Sun. Capacity lower bound for the Ising perceptron. arXiv:1809.07742, 2018.

David L Donoho, Arian Maleki, and Andrea Montanari. Message-passing algorithms for compressed sensing. *Proc. Natl. Acad. Sci.*, 106(45):18914–18919, 2009.

Ronen Eldan. Taming correlations through entropy-efficient measure decompositions with applications to mean-field approximation. *Probab. Theory Related Fields*, 176(3-4):737–755, 2020. ISSN 0178-8051. doi: 10.1007/s00440-019-00924-2. URL https://doi.org/10.1007/s00440-019-00924-2.

Ronen Eldan and Renan Gross. Decomposition of mean-field Gibbs distributions into product measures. *Electron. J. Probab.*, 23:Paper No. 35, 24, 2018. doi: 10.1214/18-EJP159. URL https://doi.org/10.1214/18-EJP159.

Zhou Fan. Approximate message passing algorithms for rotationally invariant matrices. arXiv:2008.11892, 2020.

Zhou Fan and Yihong Wu. The replica-symmetric free energy for Ising spin glasses with orthogonally invariant couplings. arXiv:2105.02797, 2021.

Zhou Fan, Song Mei, and Andrea Montanari. TAP free energy, spin glasses and variational inference. *Ann. Probab.*, 49(1):1–45, 2021. ISSN 0091-1798. doi: 10.1214/20-AOP1443. URL https://doi.org/10.1214/20-AOP1443.

Silvio Franz and Giorgio Parisi. The simplest model of jamming. *J. Phys. A*, 49(14):145001, 2016.

Silvio Franz, Giorgio Parisi, Maxime Sevelev, Pierfrancesco Urbani, and Francesco Zamponi. Universality of the SAT-UNSAT (jamming) threshold in non-convex continuous constraint satisfaction problems. *SciPost Physics*, 2(3):019, 2017.

E Gardner and B Derrida. Optimal storage properties of neural network models. *J. Phys. A*, 21(1): 271, 1988.

Elizabeth Gardner. Maximum storage capacity in neural networks. *Europhys. Lett.*, 4(4):481, 1987.

Elizabeth Gardner. The space of interactions in neural network models. *J. Phys. A*, 21(1):257, 1988.

Elizabeth Gardner and Bernard Derrida. Three unfinished works on the optimal storage capacity of networks. *J. Phys. A*, 22(12):1983, 1989.

R. J. Gardner. The Brunn-Minkowski inequality. *Bull. Amer. Math. Soc. (N.S.)*, 39(3):355–405, 2002. ISSN 0273-0979. doi: 10.1090/S0273-0979-02-00941-2. URL https://doi.org/10.1090/S0273-0979-02-00941-2.

Y. Gordon. On Milman's inequality and random subspaces which escape through a mesh in $\mathbf{R}^n$. In *Geometric aspects of functional analysis (1986/87)*, volume 1317 of *Lecture Notes in Math.*, pages 84–106. Springer, Berlin, 1988. doi: 10.1007/BFb0081737. URL https://doi.org/10.1007/BFb0081737.

Yehoram Gordon. Some inequalities for Gaussian processes and applications. *Israel J. Math.*, 50 (4):265–289, 1985. ISSN 0021-2172. doi: 10.1007/BF02759761. URL https://doi.org/10.1007/BF02759761.

H. Hadwiger and D. Ohmann. Brunn-Minkowskischer Satz und Isoperimetrie. *Math. Z.*, 66:1–8, 1956. ISSN 0025-5874. doi: 10.1007/BF01186589. URL https://doi.org/10.1007/BF01186589.

D. O. Hebb. *The organization of behavior*. Wiley, New York, 1949.

J. J. Hopfield. Neural networks and physical systems with emergent collective computational abilities. *Proc. Nat. Acad. Sci. U.S.A.*, 79(8):2554–2558, 1982. ISSN 0027-8424. doi: 10.1073/pnas.79.8.2554. URL https://doi.org/10.1073/pnas.79.8.2554.

Vishesh Jain, Frederic Koehler, and Elchanan Mossel. The mean-field approximation: Information inequalities, algorithms, and complexity. In *Proc. 31st COLT*, pages 1326–1347. PMLR, 2018.

Vishesh Jain, Andrej Risteski, and Frederic Koehler. Mean-field approximation, convex hierarchies, and the optimality of correlation rounding: a unified perspective. In *Proc. 51st STOC*, pages 1226–1236. ACM, New York, 2019. doi: 10.1145/3313276.3316299. URL https://doi.org/10.1145/3313276.3316299.

Adel Javanmard and Andrea Montanari. State evolution for general approximate message passing algorithms, with applications to spatial coupling. *Inf. Inference*, 2(2):115–144, 2013. ISSN 2049-8764. doi: 10.1093/imaiai/iat004. URL https://doi.org/10.1093/imaiai/iat004.

Jeong Han Kim and James R. Roche. Covering cubes by random half cubes, with applications to binary neural networks. *J. Comput. System Sci.*, 56(2):223–252, 1998. ISSN 0022-0000. doi: 10.1006/jcss.1997.1560. URL https://doi.org/10.1006/jcss.1997.1560. Eighth Annual Workshop on Computational Learning Theory (COLT) (Santa Cruz, CA, 1995).

Werner Krauth and Marc Mézard. Storage capacity of memory networks with binary couplings. *J. Physique*, 50(20):3057–3066, 1989.

L. Leindler. On a certain converse of Hölder's inequality. In *Linear operators and approximation (Proc. Conf., Oberwolfach, 1971)*, pages 182–184. Internat. Ser. Numer. Math., Vol. 20, 1972.

Elliott H. Lieb and Michael Loss. *Analysis*, volume 14 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 2001. ISBN 0-8218-2783-9. doi: 10.1090/gsm/014. URL https://doi.org/10.1090/gsm/014.

William A Little. The existence of persistent states in the brain. *Math. Biosci.*, 19(1-2):101–120, 1974.

LA Lusternik. Die Brunn–Minkowskische ungleichung für beliebige messbare mengen. *C. R. Acad. Sci. URSS*, 8:55–58, 1935.

B. Maurey. Some deviation inequalities. *Geom. Funct. Anal.*, 1(2):188–197, 1991. ISSN 1016-443X. doi: 10.1007/BF01896377. URL https://doi.org/10.1007/BF01896377.

Warren S McCulloch and Walter Pitts. A logical calculus of the ideas immanent in nervous activity. *B. Math. Biophys.*, 5(4):115–133, 1943.

M Mézard. The space of interactions in neural networks: Gardner's computation with the cavity method. *J. Phys. A*, 22(12):2181, 1989.

Marc Mézard. Mean-field message-passing equations in the Hopfield model and its generalizations. *Phys. Rev. E*, 95(2):022117, 2017.

Andrea Montanari, Yiqiao Zhong, and Kangjie Zhou. Tractability from overparametrization: the example of the negative perceptron. arXiv:2110.15824, 2021.

Manfred Opper and Ole Winther. Adaptive and self-averaging Thouless–Anderson–Palmer mean-field theory for probabilistic modeling. *Phys. Rev. E*, 64(5):056131, 2001.

Manfred Opper, Burak Çakmak, and Ole Winther. A theory of solving TAP equations for Ising models with general invariant random matrices. *J. Phys. A*, 49(11):114002, 2016.

Will Perkins and Changji Xu. Frozen 1-RSB structure of the symmetric Ising perceptron. In *Proc. 53rd STOC*, pages 1579–1588, 2021.

V. V. Petrov. *Sums of independent random variables*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 82. Springer-Verlag, New York-Heidelberg, 1975. Translated from the Russian by A. A. Brown.

Gilles Pisier. Probabilistic methods in the geometry of Banach spaces. In *Probability and analysis (Varenna, 1985)*, volume 1206 of *Lecture Notes in Math.*, pages 167–241. Springer, Berlin, 1986. doi: 10.1007/BFb0076302. URL https://doi.org/10.1007/BFb0076302.

Timm Plefka. Convergence condition of the tap equation for the infinite-ranged ising spin glass model. *J. Phys. A*, 15(6):1971, 1982.

András Prékopa. Logarithmic concave measures with application to stochastic programming. *Acta Sci. Math. (Szeged)*, 32:301–316, 1971. ISSN 0001-6969.

András Prékopa. On logarithmic concave measures and functions. *Acta Sci. Math. (Szeged)*, 34: 335–343, 1973. ISSN 0001-6969.

Mark Rudelson and Roman Vershynin. Non-asymptotic theory of random matrices: extreme singular values. In *Proceedings of the International Congress of Mathematicians. Volume III*, pages 1576–1602. Hindustan Book Agency, New Delhi, 2010.

Cynthia Rush and Ramji Venkataramanan. Finite sample analysis of approximate message passing algorithms. *IEEE Trans. Inform. Theory*, 64(11):7264–7286, 2018. ISSN 0018-9448. doi: 10.1109/TIT.2018.2816681. URL https://doi.org/10.1109/TIT.2018.2816681.

Mariya Shcherbina and Brunello Tirozzi. Rigorous solution of the Gardner problem. *Comm. Math. Phys.*, 234(3):383–422, 2003. ISSN 0010-3616. doi: 10.1007/s00220-002-0783-3. URL https://doi.org/10.1007/s00220-002-0783-3.

David Sherrington and Scott Kirkpatrick. Solvable model of a spin-glass. *Phys. Rev. Lett.*, 35(26): 1792, 1975.

Mihailo Stojnic. Another look at the Gardner problem. arXiv:1306.3979, 2013.

Michel Talagrand. Self-averaging and the space of interactions in neural networks. *Random Structures Algorithms*, 14(3):199–213, 1999a. ISSN 1042-9832. doi: 10.1002/(SICI)1098-2418(199905)14:3⟨199::AID-RSA1⟩3.3.CO;2-Y. URL https://doi.org/10.1002/(SICI)1098-2418(199905)14:3<199::AID-RSA1>3.3.CO;2-Y.

Michel Talagrand. Intersecting random half cubes. *Random Structures Algorithms*, 15(3-4):436–449, 1999b. ISSN 1042-9832. doi: 10.1002/(SICI)1098-2418(199910/12)15:3/4⟨436::AID-RSA11⟩3.0.CO;2-5. URL https://doi.org/10.1002/(SICI)1098-2418(199910/12)15:3/4<436::AID-RSA11>3.0.CO;2-5. Statistical physics methods in discrete probability, combinatorics, and theoretical computer science (Princeton, NJ, 1997).

Michel Talagrand. Intersecting random half-spaces: toward the Gardner-Derrida formula. *Ann. Probab.*, 28(2):725–758, 2000. ISSN 0091-1798. doi: 10.1214/aop/1019160259. URL https://doi.org/10.1214/aop/1019160259.

Michel Talagrand. On the Gaussian perceptron at high temperature. *Math. Phys. Anal. Geom.*, 5(1):77–99, 2002. ISSN 1385-0172. doi: 10.1023/A:1015840632110. URL https://doi.org/10.1023/A:1015840632110.

Michel Talagrand. *Mean field models for spin glasses. Volume I*, volume 54 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics*. Springer-Verlag, Berlin, 2011a. ISBN 978-3-642-15201-6. doi: 10.1007/978-3-642-15202-3. URL https://doi.org/10.1007/978-3-642-15202-3. Basic examples.

Michel Talagrand. *Mean field models for spin glasses. Volume II*, volume 55 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics*. Springer, Heidelberg, 2011b. ISBN 978-3-642-22252-8; 978-3-642-22253-5. Advanced replica-symmetry and low temperature.

David J Thouless, Philip W Anderson, and Robert G Palmer. Solution of 'solvable model of a spin glass'. *Philosophical Magazine*, 35(3):593–601, 1977.

Christos Thrampoulidis, Samet Oymak, and Babak Hassibi. The Gaussian min-max theorem in the presence of convexity. arXiv:1408.4837, 2014.

B. S. Tsirelson, I. A. Ibragimov, and V. N. Sudakov. Norms of Gaussian sample functions. In *Proceedings of the Third Japan-USSR Symposium on Probability Theory (Tashkent, 1975)*, pages 20–41. Lecture Notes in Math., Vol. 550, 1976.

J. G. Wendel. A problem in geometric probability. *Math. Scand.*, 11:109–111, 1962. ISSN 0025-5521. doi: 10.7146/math.scand.a-10655. URL https://doi.org/10.7146/math.scand.a-10655.

Changji Xu. Sharp threshold for the Ising perceptron model. *Ann. Probab.*, 49(5):2399–2415, 2021. ISSN 0091-1798. doi: 10.1214/21-aop1511. URL https://doi.org/10.1214/21-aop1511.

## Appendix A. First moment conditional on AMP

We consider the perceptron model (1) with an independent copy $\boldsymbol{G}'$ of the disorder matrix $\boldsymbol{G}$ — this is clearly equivalent (in law) to the original model. The (random) weight of the configuration $J$ is

$$\mathrm{S} \equiv \mathrm{S}_J(\boldsymbol{G}') \equiv \exp\left\{\left(\mathbf{1}, u\left(\frac{\boldsymbol{G}'J}{N^{1/2}}\right)\right)\right\}, \tag{23}$$

where $u \equiv \log U : \mathbb{R} \to [-\infty, 0]$ is applied componentwise by the convention of this paper. As in (1), the corresponding perceptron partition function is

$$\boldsymbol{Z}(\boldsymbol{G}') \equiv \sum_J \mathrm{S}_J(\boldsymbol{G}'). \tag{24}$$

Let $\mathbf{m}^{(s)}$ and $\mathbf{n}^{(\ell)}$ be generated from the AMP iteration (14) and (15) with $\boldsymbol{G}'$ in place of $\boldsymbol{G}$ (and with the same initial values for $\mathbf{m}^{(0)}$, $\mathbf{n}^{(0)}$, $\mathbf{m}^{(1)}$, $\mathbf{n}^{(1)}$ as before). Then, similarly as in (16), let

$$\mathscr{F}'(t) \equiv \sigma\Big(\Big(\boldsymbol{G}'\mathbf{m}^{(s)}, \mathbf{n}^{(s+1)} : s \leqslant t\Big), \Big((\boldsymbol{G}')^{\mathsf{t}}\mathbf{n}^{(\ell)}, \mathbf{m}^{(\ell+1)} : \ell \leqslant t-1\Big)\Big). \tag{25}$$

We emphasize that $\mathscr{F}'(t)$ in (25) is defined with respect to $\boldsymbol{G}'$ while $\mathscr{F}(t)$ in (16) was defined with respect to $\boldsymbol{G}$. This section is organized as follows:

- In §A.1 we state Proposition A.1, which allows us to formally define the parameters $(q, \psi)$ appearing in the definition (12) of the replica symmetric free energy.
- In §A.2 we give a brief review of known results (Bayati and Montanari, 2011; Bolthausen, 2014) on the state evolution limit of AMP.
- In §A.3 we decompose $\boldsymbol{Z}(\boldsymbol{G}')$ into two parts (see (59)): one part $\boldsymbol{Z}_\circ(\boldsymbol{G}')$ roughly captures the contribution of configurations $J \in \{-1, +1\}^N$ which lie close to $\mathbf{m}^{(t)}$ in some sense (see (57)), while $\boldsymbol{Z}_\bullet(\boldsymbol{G}')$ is the remainder of the partition function. We then state the main result of this section, Theorem A.12, which gives the conditional first moment upper bound for $\boldsymbol{Z}_\circ(\boldsymbol{G}')$.
- In §A.4 we state and prove Proposition A.13, which gives a conditional first moment upper bound for a single configuration $J \in \{-1, +1\}^N$.
- In §A.5 we complete the proof of Theorem A.12. We also supply some large deviations bounds, Lemmas A.22 and A.23, which will be used later to bound $\boldsymbol{Z}_\bullet(\boldsymbol{G}')$ (see Corollary C.1 in §C.1).

The bound from Theorem A.12 will be analyzed in Section C to conclude the proof of Theorem 1.4. Throughout this section, $U$ satisfies Assumption 1 and 2.

### A.1. Formal definition of replica symmetric free energy

In this subsection we formally define the quantity $\mathrm{RS}(\alpha; U)$ appearing in the statement of the main result Theorem 1.1. As above, let $\xi$ denote an independent standard gaussian random variable, and let $\mathbb{E}_\xi$ denote expectation over the law $\xi$. Given $q \in [0, 1)$ let

$$L_q(x) \equiv \log \mathbb{E}_\xi U\Big(x + (1-q)^{1/2}\xi\Big) \equiv \log \int U\Big(x + (1-q)^{1/2}z\Big)\varphi(z)\, dz, \tag{26}$$

where $\varphi$ denotes the standard gaussian density as above. Recall from (8) that we defined

$$F_q(x) = (L_q)'(x) = \frac{1}{(1-q)^{1/2}} \frac{\mathbb{E}_\xi[\xi U(x+(1-q)^{1/2}\xi)]}{\mathbb{E}_\xi U(x+(1-q)^{1/2}\xi)} .$$

We will sometimes abbreviate $L \equiv L_q$ and $F \equiv F_q$.

**Proposition A.1 (proved in Section B)** *If $U$ satisfies Assumption 1, then there exists a positive constant $\alpha(U) > 0$ such that for all $0 < \alpha \leqslant \alpha(U)$ there exists a unique pair $(q,\psi) \in [0, 1/25] \times [0,\infty)$ satisfying (9). Moreover we can take*

$$\alpha(U) \equiv \frac{1}{e^{10} \cdot c_1 \cdot C_1(U)^6 \cdot K_2(U)^4} , \tag{27}$$

*where $c_1$ is an absolute constant characterized by Lemma B.7 and Corollary B.8, and $C_1(U)$ is a finite constant depending only on $U$ which is characterized by Lemma B.3. The solution $(q,\psi)$ of (9) satisfies*

$$\frac{(\mathbb{E}_\xi[\xi U(\xi)])^2}{2} \leqslant \frac{q}{\alpha} \leqslant \frac{\psi}{\alpha} \leqslant 3 \cdot C_1(U)^2 \tag{28}$$

*for all $0 \leqslant \alpha \leqslant \alpha(U)$.*

For any $U$ and $\alpha$ such that (9) has a unique solution $(q,\psi) \in [0,1) \times [0,\infty)$, the **replica symmetric formula** for the free energy of the corresponding perceptron model (1) is given by (12), which can be written equivalently as

$$\mathrm{RS} \equiv \mathrm{RS}(\alpha; U) = -\frac{\psi(1-q)}{2} + \mathbb{E}\bigg\{ \log 2 \operatorname{ch}(\psi^{1/2}Z) + \alpha L_q(q^{1/2}Z) \bigg\} , \tag{29}$$

where the expectation is over an independent standard gaussian random variable $Z$. Let us also remark that since $\operatorname{th}'(x) = 1 - (\operatorname{th} x)^2$, it follows using (9) that we can rewrite the coefficients $\beta, \beta'$ from (14) and (15) as

$$\begin{pmatrix} \beta \\ \beta' \end{pmatrix} = \begin{pmatrix} \alpha \mathbb{E} F'(q^{1/2}Z) \\ \mathbb{E} \operatorname{th}'(\psi^{1/2}Z) \end{pmatrix} . \tag{30}$$

Lastly, we comment that in Theorem 1.1 we can take

$$\alpha_\wr(U) \equiv \frac{1}{e^{16} \cdot c_1 \cdot (C_1)^\wr(U)^6 \cdot K_{2,\wr}(U)^4} \leqslant \frac{\alpha(U)}{e^6} , \tag{31}$$

where $K_{2,\wr}(U)$ is defined by Assumption 2, $\alpha(U)$ is defined by (27), and $(C_1)^\wr(U)$ will be defined by Lemma B.3.

### A.2. Review of AMP state evolution

In this subsection we review the main results on approximate message passing (as introduced in §1.3) that will be used in our proofs. What follows is primarily based on Bayati and Montanari (2011) and Bolthausen (2014). A more detailed review (with heuristic derivations) is given in Section G.

**Definition A.2 (state evolution recursions)** *Let $(q,\psi)$ be as given by Proposition A.1, and abbreviate $F \equiv F_q$. Let*

$$\rho_1 \equiv \lambda_1 \equiv \left(\frac{1}{q}\right)^{1/2} \mathbb{E}\,\mathrm{th}(\psi^{1/2}Z) = 0\,, \quad \mu_1 \equiv \gamma_1 \equiv \left(\frac{\alpha}{\psi}\right)^{1/2} \mathbb{E}F(q^{1/2}Z) \tag{32}$$

*(cf. (240)). Next let $\xi, \xi'$ be independent standard gaussian random variables, and for $s \geqslant 1$ let*

$$\begin{aligned} \rho_{s+1} &\equiv \rho(\mu_s) \equiv \frac{1}{q}\mathbb{E}\bigg[\mathrm{th}\left(\psi^{1/2}\Big\{\mu_s\xi + [1-(\mu_s)^2]^{1/2}\xi'\Big\}\right)\mathrm{th}(\psi^{1/2}\xi)\bigg]\,, \\ \mu_{s+1} &\equiv \mu(\rho_s) \equiv \frac{\alpha}{\psi}\mathbb{E}\bigg[F\left(q^{1/2}\Big\{\rho_s\xi + [1-(\rho_s)^2]^{1/2}\xi'\Big\}\right)F(q^{1/2}\xi)\bigg] \end{aligned} \tag{33}$$

*(cf. (246) and (251)). Supposing that $\gamma_1, \ldots, \gamma_{s-1}$ and $\lambda_1, \ldots, \lambda_{s-1}$ have been defined, we let*

$$\lambda_s = \frac{\rho_s - \Lambda_{s-1}}{(1-\Lambda_{s-1})^{1/2}}\,, \quad \gamma_s = \frac{\mu_s - \Gamma_{s-1}}{(1-\Gamma_{s-1})^{1/2}} \tag{34}$$

*(cf. (255)), where we have used the abbreviations*

$$\Gamma_{s-1} \equiv \sum_{\ell \leqslant s-1} (\gamma_\ell)^2\,, \quad \Lambda_{s-1} \equiv \sum_{\ell \leqslant s-1} (\lambda_\ell)^2\,. \tag{35}$$

*The above recursions are standard in the AMP literature, so we defer the explanations to Section G. We will confirm in Lemma B.10 that the recursions result in well-defined quantities for all $s \geqslant 1$.*

We now explain how the constants given in Definition A.2 describe the large-$N$ behavior of the AMP iteration. To this end, we define the (deterministic) matrices

$$\mathbf{\Gamma} \equiv \begin{pmatrix} 1 & & & & \\ \gamma_1 & (1-\Gamma_1)^{1/2} & & & \\ \gamma_1 & \gamma_2 & (1-\Gamma_2)^{1/2} & & \\ \vdots & & & \ddots & \\ \gamma_1 & \gamma_2 & \cdots & & (1-\Gamma_{t-2})^{1/2} \end{pmatrix} \in \mathbb{R}^{(t-1)\times(t-1)}\,, \tag{36}$$

$$\mathbf{\Lambda} \equiv \begin{pmatrix} 1 & & & & \\ \lambda_1 & (1-\Lambda_1)^{1/2} & & & \\ \lambda_1 & \lambda_2 & (1-\Lambda_2)^{1/2} & & \\ \vdots & & & \ddots & \\ \lambda_1 & \lambda_2 & \cdots & & (1-\Lambda_{t-1})^{1/2} \end{pmatrix} \in \mathbb{R}^{t\times t}\,. \tag{37}$$

It will follow from Lemma B.10 below that in our setting we will have $\Gamma_s \in [0,1)$ and $\Lambda_s \in [0,1)$ for all $s \geqslant 0$, which implies that both $\mathbf{\Gamma}$ and $\mathbf{\Lambda}$ are non-singular matrices. As in (25), let $\mathbf{m}^{(s)}$ and $\mathbf{n}^{(\ell)}$ be generated from the AMP iteration (14) and (15) with $\boldsymbol{G}'$ in place of $\boldsymbol{G}$. Recall that $\mathbf{m}^{(s)} \equiv \mathrm{th}(\mathbf{H}^{(s)})$ and $\mathbf{n}^{(s)} \equiv F(\mathbf{h}^{(s)})$, where $F = F_q$ is given by (8). We define vectors $\mathbf{y}^{(s)}$ and

$\mathbf{x}^{(s)}$ by setting

$$\frac{\mathbf{H}[t-1]}{\psi^{1/2}} \equiv \frac{1}{\psi^{1/2}} \begin{pmatrix} (\mathbf{H}^{(2)})^{\mathsf{t}} \\ \vdots \\ (\mathbf{H}^{(t)})^{\mathsf{t}} \end{pmatrix} \equiv \mathbf{\Gamma} \begin{pmatrix} (\mathbf{y}^{(1)})^{\mathsf{t}} \\ \vdots \\ (\mathbf{y}^{(t-1)})^{\mathsf{t}} \end{pmatrix} \equiv \mathbf{\Gamma}\mathbf{y}[t-1] \in \mathbb{R}^{(t-1)\times N}, \tag{38}$$

$$\frac{\mathbf{h}[t]}{q^{1/2}} \equiv \frac{1}{q^{1/2}} \begin{pmatrix} (\mathbf{h}^{(2)})^{\mathsf{t}} \\ \vdots \\ (\mathbf{h}^{(t+1)})^{\mathsf{t}} \end{pmatrix} \equiv \mathbf{\Lambda} \begin{pmatrix} (\mathbf{x}^{(1)})^{\mathsf{t}} \\ \vdots \\ (\mathbf{x}^{(t)})^{\mathsf{t}} \end{pmatrix} \equiv \mathbf{\Lambda}\mathbf{x}[t] \in \mathbb{R}^{t\times M}, \tag{39}$$

for $\mathbf{\Gamma}$ and $\mathbf{\Lambda}$ as in (36) and (37). Then the $\mathbf{x}^{(s)}$ "behave like" i.i.d. standard gaussian vectors in $\mathbb{R}^M$, while the $\mathbf{y}^{(s)}$ "behave like" i.i.d. standard gaussian vectors in $\mathbb{R}^N$. For an intuitive explanation we refer to the heuristic derivation of (253) and (254) given in Section G. The formal version is given by the next definition and lemma:

**Definition A.3 (pseudo-Lipschitz functions)** *Following Bayati and Montanari (2011), we say that a function $f : \mathbb{R}^\ell \to \mathbb{R}$ (where $\ell$ is any positive integer) is **pseudo-Lipschitz of order** $k$ if there exists a constant $L > 0$ such that*

$$\|f(x) - f(y)\| \leqslant L\Big(1 + \|x\|^{k-1} + \|y\|^{k-1}\Big)\|x-y\|$$

*for all $x, y \in \mathbb{R}^\ell$. We say for short that $f$ is a* $\mathrm{PL}(k)$ *function.*

Throughout what follows we let $\mathbf{e}_i$ (for $i \leqslant N$) denote the $i$-th standard basis vector in $\mathbb{R}^N$. With a minor abuse of notation we also let $\mathbf{e}_a$ (for $a \leqslant M$) denote the $a$-th standard basis vector in $\mathbb{R}^M$; the dimension of the vector should be clear from context.

**Lemma A.4 ((Bayati and Montanari, 2011, Lem. 1))** *Suppose $U$ satisfies Assumptions 1 and 2. In particular, this guarantees that the function $F_q$ of (8) is Lipschitz (see Lemma B.14). Let $\boldsymbol{G}$ be an $M \times N$ matrix with i.i.d. standard gaussian entries, such that $M/N = \alpha$. Assume $0 \leqslant \alpha \leqslant \alpha(U)$, and let $(q,\psi)$ be the solution given by Proposition A.1. Then let $\mathbf{m}^{(s)} \equiv \mathrm{th}(\mathbf{H}^{(s)})$ and $\mathbf{n}^{(\ell)} \equiv F_q(\mathbf{h}^{(\ell)})$ be generated from the AMP iteration (14) and (15), with the same initial values for $\mathbf{m}^{(0)}$, $\mathbf{n}^{(0)}$, $\mathbf{m}^{(1)}$, $\mathbf{n}^{(1)}$ as before. If $f : \mathbb{R}^{t-1} \to \mathbb{R}$ is a* $\mathrm{PL}(k)$ *function, then*

$$\frac{1}{N}\sum_{i\leqslant N} f\Big((\mathbf{H}[t-1]\mathbf{e}_i)^{\mathsf{t}}\Big) \overset{N\to\infty}{\longrightarrow} \mathbb{E}f(\psi^{1/2}\mathbf{\Gamma}\boldsymbol{\xi})$$

*where $\boldsymbol{\xi}$ here denotes a standard gaussian vector in $\mathbb{R}^{t-1}$, and the convergence holds in probability as $N \to \infty$ for any fixed t. Likewise, if $f : \mathbb{R}^t \to \mathbb{R}$ is a* $\mathrm{PL}(k)$ *function, then*

$$\frac{1}{M}\sum_{a\leqslant M} f\Big((\mathbf{h}[t]\mathbf{e}_a)^{\mathsf{t}}\Big) \overset{N\to\infty}{\longrightarrow} \mathbb{E}f(q^{1/2}\mathbf{\Lambda}\boldsymbol{\xi})$$

*where $\boldsymbol{\xi}$ here denotes a standard gaussian vector in $\mathbb{R}^t$.*

We remark that the results of Bayati and Montanari (2011) are for a more general setting where the AMP iteration starts from a random initialization with bounded moments up to order $2k-2$; the result then holds for any $f$ which is PL$(k)$. In this paper we start from an initialization with bounded moments of all finite orders, so in Lemma A.4 we can take $f$ to be in PL$(k)$ for any finite $k$. We now present a few applications of Lemma A.4 which illustrate how some of the recursions from Definition A.2 naturally arise. First, it follows from Lemma A.4 and the definition (33) that

$$\frac{(\mathbf{m}^{(r)},\mathbf{m}^{(s)})}{Nq} = \frac{(\mathrm{th}(\mathbf{H}^{(r)}),\mathrm{th}(\mathbf{H}^{(s)}))}{Nq} \simeq \rho((\mathbf{\Gamma}\mathbf{\Gamma}^{\mathrm{t}})_{r-1,s-1})\,.$$

In the above and throughout this paper, we write $f \simeq g$ to indicate that $f-g$ converges to zero in probability as $N\to\infty$. In the case $r=s$ we have

$$(\mathbf{\Gamma}\mathbf{\Gamma}^{\mathrm{t}})_{r-1,r-1} \overset{(36)}{=} \sum_{\ell\leqslant r-2}(\gamma_\ell)^2 + (1-\Gamma_{r-2}) \overset{(35)}{=} \Gamma_{r-2} + (1-\Gamma_{r-2}) = 1\,. \tag{40}$$

If $r\neq s$, we can suppose without loss that $r<s$, in which case

$$(\mathbf{\Gamma}\mathbf{\Gamma}^{\mathrm{t}})_{r-1,s-1} \overset{(36)}{=} \sum_{\ell\leqslant r-2}(\gamma_\ell)^2 + \gamma_{r-1}(1-\Gamma_{r-2})^{1/2} \overset{(35)}{=} \Gamma_{r-2} + \gamma_{r-1}(1-\Gamma_{r-2})^{1/2} \overset{(34)}{=} \mu_{r-1}\,.$$

It follows that $\|\mathbf{m}^{(r)}\|^2 \simeq Nq$ for all $r$, and for $r<s$ we have

$$\frac{(\mathbf{m}^{(r)},\mathbf{m}^{(s)})}{Nq} \simeq \rho(\mu_{r-1}) \overset{(33)}{=} \rho_r \overset{(34)}{=} \Lambda_{r-1} + \lambda_r(1-\Gamma_{r-1})^{1/2} \overset{(36)}{=} (\mathbf{\Lambda}\mathbf{\Lambda}^{\mathrm{t}})_{r,s}\,. \tag{41}$$

A similar calculation gives that $\|\mathbf{n}^{(r)}\|^2 \simeq N\psi$ for all $r$, and for $r<s$ we have

$$\frac{(\mathbf{n}^{(r)},\mathbf{n}^{(s)})}{N\psi} \simeq \mu(\rho_{r-1}) = \mu_r = (\mathbf{\Gamma}\mathbf{\Gamma}^{\mathrm{t}})_{r,s}\,. \tag{42}$$

Let $\mathbf{r}^{(s)}$ be the Gram–Schmidt orthogonalization of the vectors $\mathbf{m}^{(s)}$ for $s\geqslant 1$: thus $\mathbf{r}^{(1)} = \mathbf{m}^{(1)}/\|\mathbf{m}^{(1)}\| = \mathbf{1}/N^{1/2}$,

$$\mathbf{r}^{(2)} = \frac{\mathbf{m}^{(2)} - (\mathbf{m}^{(2)},\mathbf{r}^{(1)})\mathbf{r}^{(1)}}{\|\mathbf{m}^{(2)} - (\mathbf{m}^{(2)},\mathbf{r}^{(1)})\mathbf{r}^{(1)}\|}\,,$$

and so on. The $\mathbf{r}^{(s)}$ form an orthonormal set in $N$-dimensional space (assuming the number of iterations is much smaller than the dimension). Likewise, let $\mathbf{c}^{(s)}$ be the Gram–Schmidt orthogonalization of the vectors $\mathbf{n}^{(s)}$ for $s\geqslant 1$; these form an orthonormal set in $M$-dimensional space. Let $\mathbf{\Lambda}_N,\mathbf{\Gamma}_N$ be the (random) matrices such that

$$\frac{\mathbf{m}[t]}{(Nq)^{1/2}} \equiv \frac{1}{(Nq)^{1/2}}\begin{pmatrix}(\mathbf{m}^{(1)})^{\mathrm{t}}\\ \vdots\\ (\mathbf{m}^{(t)})^{\mathrm{t}}\end{pmatrix} = \mathbf{\Lambda}_N\begin{pmatrix}(\mathbf{r}^{(1)})^{\mathrm{t}}\\ \vdots\\ (\mathbf{r}^{(t)})^{\mathrm{t}}\end{pmatrix} \equiv \mathbf{\Lambda}_N\mathbf{r}[t] \in \mathbb{R}^{t\times N}\,, \tag{43}$$

$$\frac{\mathbf{n}[t-1]}{(N\psi)^{1/2}} \equiv \frac{1}{(N\psi)^{1/2}}\begin{pmatrix}(\mathbf{n}^{(1)})^{\mathrm{t}}\\ \vdots\\ (\mathbf{n}^{(t-1)})^{\mathrm{t}}\end{pmatrix} = \mathbf{\Gamma}_N\begin{pmatrix}(\mathbf{c}^{(1)})^{\mathrm{t}}\\ \vdots\\ (\mathbf{c}^{(t-1)})^{\mathrm{t}}\end{pmatrix} \equiv \mathbf{\Gamma}_N\mathbf{c}[t-1] \in \mathbb{R}^{(t-1)\times M}\,. \tag{44}$$

It can be deduced from (41) and (42) that

$$\begin{pmatrix}\mathbf{\Lambda}_N\\ \mathbf{\Gamma}_N\end{pmatrix} \simeq \begin{pmatrix}\mathbf{\Lambda}\\ \mathbf{\Gamma}\end{pmatrix}\,. \tag{45}$$

(This means $\mathbf{\Lambda}_N - \mathbf{\Lambda}$ and $\mathbf{\Gamma}_N - \mathbf{\Gamma}$ converge entrywise to zero, in probability, as $N \to \infty$.) Since $\mathbf{r}[t]$ and $\mathbf{c}[t-1]$ have orthonormal rows, the above implies

$$\frac{\mathbf{m}[t]\mathbf{m}[t]^{\mathrm{t}}}{Nq} \overset{(43)}{=} \mathbf{\Lambda}_N\mathbf{r}[t]\mathbf{r}[t]^{\mathrm{t}}(\mathbf{\Lambda}_N)^{\mathrm{t}} = \mathbf{\Lambda}_N(\mathbf{\Lambda}_N)^{\mathrm{t}} \simeq \frac{\mathbf{h}[t]\mathbf{h}[t]^{\mathrm{t}}}{N\alpha q} \in \mathbb{R}^{t\times t}\,,$$
$$\frac{\mathbf{n}[t-1]\mathbf{n}[t-1]^{\mathrm{t}}}{N\psi} \overset{(44)}{=} \mathbf{\Gamma}_N\mathbf{c}[t-1]\mathbf{c}[t-1]^{\mathrm{t}}(\mathbf{\Gamma}_N)^{\mathrm{t}} = \mathbf{\Gamma}_N(\mathbf{\Gamma}_N)^{\mathrm{t}} \simeq \frac{\mathbf{H}[t]\mathbf{H}[t]^{\mathrm{t}}}{N\psi} \in \mathbb{R}^{(t-1)\times(t-1)}\,,$$

where the approximations on the right-hand side use Lemma A.4. The above is of course consistent with the previous calculations (41) and (42) (cf. (Bayati and Montanari, 2011, eq. (3.18) and (3.19))).

A further consequence of Lemma A.4 is that for all $k, \ell \geqslant 1$ we have

$$\begin{aligned}\frac{(\mathbf{m}^{(k+1)},\mathbf{y}^{(\ell)})}{Nq^{1/2}} &= \frac{(\mathrm{th}(\mathbf{H}^{(k+1)}),\mathbf{y}^{(\ell)})}{Nq^{1/2}} \overset{(38)}{=} \frac{1}{Nq^{1/2}}\bigg(\mathrm{th}\bigg(\psi^{1/2}\Big\{\sum_{\ell'\leqslant t-1}\Gamma_{k,\ell'}\mathbf{y}^{(\ell')}\Big\}\bigg),\mathbf{y}^{(\ell)}\bigg)\\ &\simeq \frac{\Gamma_{k,\ell}}{q^{1/2}}\mathbb{E}\Big[Z\,\mathrm{th}(\psi^{1/2}Z)\Big] = \frac{\Gamma_{k,\ell}}{q^{1/2}}\psi^{1/2}\mathbb{E}\Big[\,\mathrm{th}'(\psi^{1/2}Z)\Big] \overset{(9)}{=} \frac{\Gamma_{k,\ell}}{q^{1/2}}\psi^{1/2}(1-q)\,,\end{aligned}$$

where the transition from the first line to the second is an application of Lemma A.4, and we also used the gaussian integration by parts identity. Recall also that $\mathbf{m}^{(1)} = q^{1/2}\mathbf{1}$, so Lemma A.4 also implies

$$\frac{(\mathbf{m}^{(1)},\mathbf{y}^{(\ell)})}{Nq^{1/2}} \simeq \mathbb{E}\xi = 0$$

for all $\ell \leqslant t-1$, where $\xi$ is a standard gaussian random variable. The above calculations can be summarized as

$$\bigg\| \frac{\mathbf{y}[t-1]\mathbf{m}[t]^{\mathrm{t}}}{Nq^{1/2}} - \begin{pmatrix}\mathbf{0} & \dfrac{\psi^{1/2}}{q^{1/2}}(1-q)\mathbf{\Gamma}^{\mathrm{t}}\end{pmatrix}\bigg\|_\infty \leqslant \mathrm{ERR}_{t,1} \simeq 0\,, \tag{46}$$

where $\mathbf{0}$ denotes the zero vector in $t-1$ dimensions, and $\mathrm{ERR}_{t,1}$ is an an $\mathscr{F}(t)$-measurable random variable that converges to zero in probability as $N \to \infty$ (cf. (Bayati and Montanari, 2011, eq. (3.20) and (3.21))). This concludes our review of the required results on the state evolution of AMP, and we turn next to the conditional moment calculations. We introduce some notation which will be used later in the paper:

**Remark A.5 (bounds on $\mathbf{\Lambda}_N$ and $\mathbf{\Gamma}_N$)** *Since $\mathbf{\Lambda}$ and $\mathbf{\Gamma}$ are both non-singular (this will be verified in Lemma B.10 below), we can define a large finite constant $\varsigma_t$ such that we have the bound*

$$\max\Big\{\|\mathbf{\Lambda}_N\|_\infty, \|(\mathbf{\Lambda}_N)^{-1}\|_\infty, \|\mathbf{\Gamma}_N\|_\infty, \|(\mathbf{\Gamma}_N)^{-1}\|_\infty\Big\} \leqslant \left(\frac{\varsigma_t}{t}\right)^{1/2} \tag{47}$$

*with high probability. In the above, and throughout this paper, $\|\cdot\|_\infty$ denotes the entrywise maximum absolute value of a vector or matrix. On the other hand, we write $\|u\|$ for the euclidean norm of a vector $u$, and $\|A\|$ for the spectral norm a matrix $A$. It follows from (47) that we also have*

$$\max\left\{\|\mathbf{\Lambda}_N\|, \|(\mathbf{\Lambda}_N)^{-1}\|, \|\mathbf{\Gamma}_N\|, \|(\mathbf{\Gamma}_N)^{-1}\|\right\} \leqslant (\varsigma_t)^{1/2}$$

*with high probability.*

The proof of the following proposition is deferred to §B.4. It amounts to checking that an Almeida–Thouless (AT) condition (de Almeida and Thouless, 1978) is satisfied; see Lemma B.11.

**Proposition A.6** *Suppose $U$ satisfies Assumptions 1 and 2. For $0 < \alpha \leqslant \alpha(U)$ as defined by (27), the state evolution recursions from Definition A.2 result in $\Gamma_t \to 1$ and $\Lambda_t \to 1$ as $t \to \infty$.*

### A.3. Positions of configurations relative to AMP iterates

We now define parameters $\pi(J)$ and $\varpi(J)$ which summarize the position of configurations $J \in \{-1,+1\}^N$ relative to the vectors $\mathbf{r}^{(s)}$ and $\mathbf{y}^{(\ell)}$ from (43) and (38).

**Definition A.7 (parameters $\pi$ and $\varpi$)** *Let $\mathscr{F}'(t)$ be as in (25). For $J \in \{-1,+1\}^N$, define*

$$\pi(J) \equiv \frac{\mathbf{r}[t]J}{N^{1/2}} = \left(\frac{(\mathbf{r}^{(s)}, J)}{N^{1/2}}\right)_{s\leqslant t} \in \mathbb{R}^t\,, \tag{48}$$

$$\varpi(J) \equiv \frac{\mathbf{y}[t-1]J}{N} = \left(\frac{(\mathbf{y}^{(\ell)}, J)}{N}\right)_{\ell\leqslant t-1} \in \mathbb{R}^{t-1}\,. \tag{49}$$

*Note that for any given $J \in \{-1,+1\}^N$, its parameters $\pi(J)$ and $\varpi(J)$ are measurable with respect to $\mathscr{F}'(t)$.*

Recall that the vectors $\mathbf{r}^{(s)}$ and $\mathbf{m}^{(s)}$ ($1 \leqslant s \leqslant t$) are linearly related by (43), while the vectors $\mathbf{y}^{(\ell+1)}$ and $\mathbf{H}^{(\ell)}$ ($1 \leqslant \ell \leqslant t-1$) are linearly related by (38). For part of our calculation it is more convenient to work with $\mathbf{m}^{(s)}$ and $\mathbf{H}^{(\ell+1)}$ rather than with $\mathbf{r}^{(s)}$ and $\mathbf{y}^{(\ell)}$. For this reason we also define the following parameters:

**Definition A.8 (parameters $\hat\pi$ and $\delta$)** *Given $\mathscr{F}'(t)$ as in (25), and given any $J \in \{-1,+1\}^N$, we decompose $J$ as $J = J' + J''$ where $J'$ is the orthogonal projection of $J$ onto the span of the vectors $\mathbf{m}^{(s)}$, $1 \leqslant s \leqslant t$. We let $\hat\pi_s$ for $1 \leqslant s \leqslant t$ be the coefficients such that*

$$J' = \sum_{s\leqslant t} \hat\pi_s \frac{\mathbf{m}^{(s)}}{q^{1/2}} = \frac{\mathbf{m}[t]^{\mathrm{t}}\hat\pi}{q^{1/2}}\,. \tag{50}$$

*Next let $\mathbf{v} \equiv J''/\|J''\|$, and let $\delta \in \mathbb{R}^{t-1}$ be defined by*

$$\mathbf{\Gamma}_N(\mathbf{\Gamma}_N)^{\mathrm{t}}\delta = \frac{\mathbf{H}[t-1]\mathbf{v}}{(N\psi)^{1/2}}\,. \tag{51}$$

*Note that for any given $J \in \{-1,+1\}^N$, its parameters $\hat\pi(J)$ and $\delta(J)$ are measurable with respect to $\mathscr{F}'(t)$.*

The parameters $(\pi, \varpi)$ of Definition A.7 are related as follows to the parameters $(\hat{\pi}, \delta)$ of Definition A.8:

**Lemma A.9 (change of basis)** *Given $\mathscr{F}'(t)$ as in (25), suppose $J \in \{-1, +1\}^N$ has parameters $\pi(J)$, $\varpi(J)$, $\hat{\pi}(J)$, $\delta(J)$ as in Definitions A.7 and A.8. Then we have $\pi(J) = (\mathbf{\Lambda}_N)^{\mathrm{t}} \hat{\pi}(J)$, and*

$$\varpi(J) = \frac{\mathbf{y}[t-1]\mathbf{m}[t]^{\mathrm{t}}}{N q^{1/2}} \hat{\pi}(J) + \Big(1 - \|\pi(J)\|^2\Big)^{1/2} \mathbf{\Gamma}^{-1} \mathbf{\Gamma}_N (\mathbf{\Gamma}_N)^{\mathrm{t}} \delta(J) \,.$$

**Proof** For convenience we will often abbreviate $\pi \equiv \pi(J)$, etc. The expression (50) can be rewritten as

$$\frac{J'}{N^{1/2}} \overset{(50)}{=} \frac{\mathbf{m}[t]^{\mathrm{t}} \hat{\pi}}{(Nq)^{1/2}} \overset{(43)}{=} \mathbf{r}[t]^{\mathrm{t}} (\mathbf{\Lambda}_N)^{\mathrm{t}} \hat{\pi} \,,$$

so by comparing with (48) we see that $\pi(J) = (\mathbf{\Lambda}_N)^{\mathrm{t}} \hat{\pi}(J)$. Next we have

$$\frac{\mathbf{H}[t-1]J'}{N \psi^{1/2}} \overset{(50)}{=} \frac{\mathbf{H}[t-1]\mathbf{m}[t]^{\mathrm{t}} \hat{\pi}}{N (\psi q)^{1/2}} \overset{(38)}{=} \frac{\mathbf{\Gamma} \mathbf{y}[t-1]\mathbf{m}[t]^{\mathrm{t}} \hat{\pi}}{N q^{1/2}} \,. \tag{52}$$

It is clear from (48) that $\|J'\|/N^{1/2} = \|\pi\|$, and since $\mathbf{v} \equiv J''/\|J''\|$, it follows that

$$\frac{\mathbf{H}[t-1]J''}{N \psi^{1/2}} = \frac{\|J''\|}{N^{1/2}} \cdot \frac{\mathbf{H}[t-1]\mathbf{v}}{(N\psi)^{1/2}} = \Big(1 - \|\pi\|^2\Big)^{1/2} \frac{\mathbf{H}[t-1]\mathbf{v}}{(N\psi)^{1/2}} \overset{(51)}{=} \Big(1 - \|\pi\|^2\Big)^{1/2} \mathbf{\Gamma}_N (\mathbf{\Gamma}_N)^{\mathrm{t}} \delta \,. \tag{53}$$

Combining (38), (52), and (53) gives

$$\begin{aligned}\varpi(J) &\overset{(49)}{=} \frac{\mathbf{y}[t-1]J}{N} \overset{(38)}{=} \frac{\mathbf{\Gamma}^{-1}\mathbf{H}[t-1]J}{N\psi^{1/2}} \overset{(53)}{=} \frac{\mathbf{\Gamma}^{-1}\mathbf{H}[t-1]J'}{N\psi^{1/2}} + \Big(1 - \|\pi\|^2\Big)^{1/2} \mathbf{\Gamma}^{-1}\mathbf{\Gamma}_N(\mathbf{\Gamma}_N)^{\mathrm{t}} \delta \\ &\overset{(52)}{=} \frac{\mathbf{y}[t-1]\mathbf{m}[t]^{\mathrm{t}}}{N q^{1/2}} \hat{\pi} + \Big(1 - \|\pi\|^2\Big)^{1/2} \mathbf{\Gamma}^{-1}\mathbf{\Gamma}_N(\mathbf{\Gamma}_N)^{\mathrm{t}} \delta \,.\end{aligned}$$

This concludes the proof. ■

**Lemma A.10 (approximate change of basis)** *Given $\mathscr{F}'(t)$ as in (25), suppose again that $J \in \{-1, +1\}^N$ has parameters $\pi(J)$, $\varpi(J)$, $\hat{\pi}(J)$, $\delta(J)$ as in Definitions A.7 and A.8. Define also $\dot{\pi}(J) \equiv \mathbf{\Lambda}^{\mathrm{t}} \hat{\pi}(J)$ and*

$$\dot{\varpi}(J) \equiv (\mathbf{\Gamma}_N)^{\mathrm{t}} \bigg\{ \frac{\psi^{1/2}}{q^{1/2}} (1-q) \acute{\pi}(J) + \Big(1 - \|\pi(J)\|^2\Big)^{1/2} \delta(J) \bigg\} \,, \tag{54}$$

*where $\acute{\pi} \equiv \acute{\pi}(J) \equiv (\hat{\pi}_2, \ldots, \hat{\pi}_t) \in \mathbb{R}^{t-1}$. Then*

$$\max \bigg\{ \Big\| \pi(J) - \dot{\pi}(J) \Big\|_\infty + \Big\| \varpi(J) - \dot{\varpi}(J) \Big\|_\infty : J \in \{-1, +1\}^N \bigg\} \leqslant \mathrm{ERR}_{t,2} \,,$$

*where $\mathrm{ERR}_{t,2}$ is an an $\mathscr{F}'(t)$-measurable random variable that converges to zero in probability as $N \to \infty$.*

**Proof** It follows trivially from the definition (48) and the Cauchy–Schwarz inequality that

$$\|\pi(J)\|_\infty \leqslant \max\left\{\frac{\|\mathbf{r}^{(s)}\|\cdot\|J\|}{N^{1/2}} : s \leqslant t\right\} = 1\,,$$

where we emphasize that the bound clearly holds uniformly over all $J \in \{-1,+1\}^N$. Now recall from Lemma A.9 that $\dot\pi(J) = \mathbf{\Lambda}^{\mathrm{t}}\hat\pi(J)$ and $\pi(J) = (\mathbf{\Lambda}_N)^{\mathrm{t}}\hat\pi(J)$. It follows that

$$\Big\|\pi(J) - \dot\pi(J)\Big\|_\infty \leqslant \sup\left\{\left\|\Big((\mathbf{\Lambda}_N)^{-1}(\mathbf{\Lambda}_N - \mathbf{\Lambda})\Big)^{\mathrm{t}} u\right\|_\infty : \|u\|_\infty \leqslant 1\right\}.$$

The right-hand side above is $\mathscr{F}'(t)$-measurable and does not depend on $J$, and it follows from (45) that it tends to zero in probability as $N \to \infty$. Next, to compare $\varpi(J)$ with $\dot\varpi(J)$, we note that $\varpi(J) - \dot\varpi(J)$ can be expressed as $\mathrm{I}(J) + \mathrm{II}(J)$ where

$$\mathrm{I}(J) \equiv \left\{\frac{\mathbf{y}[t-1]\mathbf{m}[t]^{\mathrm{t}}}{Nq^{1/2}} - \begin{pmatrix}\mathbf{0} & \dfrac{\psi^{1/2}}{q^{1/2}}(1-q)(\mathbf{\Gamma}_N)^{\mathrm{t}}\end{pmatrix}\right\}(\mathbf{\Lambda}_N)^{-1}\pi(J)\,,$$

$$\mathrm{II}(J) \equiv \Big(1 - \|\pi(J)\|^2\Big)^{1/2}\mathbf{\Gamma}^{-1}(\mathbf{\Gamma}_N - \mathbf{\Gamma})(\mathbf{\Gamma}_N)^{\mathrm{t}}\delta(J)\,.$$

Since $\|\pi(J)\|_\infty \leqslant 1$ as noted above, it follows using (45) and (46) that $\|\mathrm{I}(J)\|_\infty$ can be bounded uniformly over $J$ by an $\mathscr{F}'(t)$-measurable quantity that tends to zero in probability as $N \to \infty$. Next we note that (51) combined with the Cauchy–Schwarz inequality gives, for all $J$,

$$\Big\|\mathbf{\Gamma}_N(\mathbf{\Gamma}_N)^{\mathrm{t}}\delta(J)\Big\|_\infty \leqslant \max\left\{\frac{\|\mathbf{H}^{(\ell)}\|}{N\psi^{1/2}} : \ell \leqslant t-1\right\}.$$

The right-hand side above is $\mathscr{F}'(t)$-measurable, and it can be deduced from Lemma A.4 that it converges in probability to 1 as $N \to \infty$. It follows by combining with (45) that $\|\mathrm{II}(J)\|_\infty$ can also be bounded uniformly over $J$ by an $\mathscr{F}'(t)$-measurable quantity that tends to zero in probability as $N \to \infty$. This proves the claim. ■

We next use the AMP iteration to define a convenient change of measure on the discrete cube:

**Definition A.11 (change of measure)** *Let $\mathbf{P}$ be the uniform probability measure on $\{-1,+1\}^N$, and let $\mathbf{Q}$ be the probability measure on the same space which is given by*

$$\frac{d\mathbf{Q}}{d\mathbf{P}} = \prod_{i\leqslant N}\frac{\exp((\mathbf{H}^{(t)})_i J_i)}{\operatorname{ch}(\mathbf{H}^{(t)})_i} = \frac{\exp\{(\mathbf{H}^{(t)}, J)\}}{\exp\{(\mathbf{1}, \log\operatorname{ch}\mathbf{H}^{(t)})\}}\,.$$

*If $J$ is sampled from the measure $\mathbf{Q}$, its expected value is exactly $\operatorname{th}(\mathbf{H}^{(t)}) = \mathbf{m}^{(t)}$. We now compute the expected values under $\mathbf{Q}$ of the parameters from Definition A.7. First we note that*

$$\dot\pi_* \equiv \frac{\mathbf{r}[t]\mathbf{m}^{(t)}}{N^{1/2}} = \frac{\mathbf{r}[t]\mathbf{m}[t]^{\mathrm{t}}\hat{e}_t}{N^{1/2}} \overset{(43)}{=} q^{1/2}\mathbf{r}[t]\mathbf{r}[t]^{\mathrm{t}}(\mathbf{\Lambda}_N)^{\mathrm{t}}\hat{e}_t = q^{1/2}(\mathbf{\Lambda}_N)^{\mathrm{t}}\hat{e}_t\,, \tag{55}$$

*where $\hat{e}_s$ denotes the $s$-th standard basis vector in $\mathbb{R}^t$. Let us define also $\pi_* \equiv q^{1/2}\mathbf{\Lambda}^{\mathrm{t}}\hat{e}_t$, and note that $\pi_* \simeq \dot\pi_*$ by (45). Next we note that*

$$\dot\varpi_* \equiv \frac{\mathbf{y}[t-1]\mathbf{m}^{(t)}}{N} \overset{(46)}{\simeq} \psi^{1/2}(1-q)(\mathbf{\Gamma}^{\mathrm{t}}\acute{e}_{t-1}) \equiv \varpi_* \in \mathbb{R}^{t-1}\,, \tag{56}$$

*where $\acute{e}_\ell$ denotes the $\ell$-th standard basis vector in $\mathbb{R}^{t-1}$.*

Recalling (1) and (23), we now define

$$\boldsymbol{N}_\circ \equiv \left\{(\pi, \varpi) : \max\left\{\|\pi(J) - \pi_*\|, \|\varpi(J) - \varpi_*\|\right\} \leqslant 16 \cdot C_1(U)\alpha^{1/2}\right\}, \tag{57}$$

where the constant $C_1(U)$ comes from Lemma B.3 below. We also let

$$\mathbb{H}_\circ \equiv \left\{J \in \{-1, +1\}^N : (\pi(J), \varpi(J)) \in \boldsymbol{N}_\circ\right\}, \tag{58}$$

and we let $\mathbb{H}_\bullet \equiv \{-1, +1\}^N \backslash \mathbb{H}_\circ$. Now decompose (24) as $\boldsymbol{Z}(\boldsymbol{G}') = \boldsymbol{Z}_\circ(\boldsymbol{G}') + \boldsymbol{Z}_\bullet(\boldsymbol{G}')$ where

$$\boldsymbol{Z}_\circ(\boldsymbol{G}') \equiv \sum_{J \in \mathbb{H}_\circ} \mathrm{S}_J(\boldsymbol{G}'), \quad \boldsymbol{Z}_\bullet(\boldsymbol{G}') \equiv \sum_{J \in \mathbb{H}_\bullet} \mathrm{S}_J(\boldsymbol{G}'), \tag{59}$$

The main result of this section is as follows:

**Theorem A.12** *Suppose $U$ satisfies Assumptions 1 and 2, and let $\mathscr{F}'(t)$ be as in (25). Given $\bar{\epsilon} \in \mathbb{R}$, define*

$$\boldsymbol{X}(\pi, \varpi) \equiv \mathbf{x}[t]^{\mathrm{t}}\pi_* + \left\{\mathbf{x}[t]^{\mathrm{t}}(\pi - \pi_*) + N^{1/2}\bar{\epsilon}\mathbf{c}[t-1]^{\mathrm{t}}(\varpi - \varpi_*)\right\} \in \mathbb{R}^M,$$

*for $\pi_*$ and $\varpi_*$ as in Definition A.11. (The parameter $\bar{\epsilon}$ will be fixed later in (114).) Then define*

$$\Psi(\pi, \varpi) \equiv \frac{\|\varpi - \bar{\epsilon}(\varpi - \varpi_*)\|^2}{2(1 - \|\pi\|^2)} - \frac{(\varpi_*, \varpi)}{1 - q} + \frac{1}{N}\sum_{a \leqslant M} L_{\|\pi\|^2}(\boldsymbol{X}_a(\pi, \varpi)).$$

*If $\mathbf{Q}$ is the measure on $\{-1, +1\}^N$ from Definition A.11, then we have*

$$\frac{\mathbb{E}(\boldsymbol{Z}_\circ(\boldsymbol{G}') \mid \mathscr{F}'(t))}{\exp\{(\mathbf{1}, \log(2\operatorname{ch}(\mathbf{H}^{(t)})))\}} \leqslant \sum_{J \in \mathbb{H}_\circ} \mathbf{Q}(J) \exp\left\{N\left[\Psi(\pi(J), \varpi(J)) + \mathrm{ERR}_{t,3}\right]\right\},$$

*where $\mathrm{ERR}_{t,3}$ is an an $\mathscr{F}'(t)$-measurable random variable that converges to zero in probability as $N \to \infty$.*

The proof of Theorem A.12 is given in §A.5.

### A.4. First moment for a single configuration

The main result of this subsection is the following:

**Proposition A.13** *Suppose $U$ satisfies Assumption 1 and 2, and let $\mathscr{F}'(t)$ be as in (25). Define*

$$\mathcal{A}(\pi, \dot{\pi}, \dot{\varpi}, \theta) \equiv \frac{\|\dot{\varpi} - \theta\|^2}{2(1 - \|\pi\|^2)} + \frac{1}{N}\sum_{a \leqslant M} L_{\|\pi\|^2}\left(\mathbf{x}[t]^{\mathrm{t}}\dot{\pi} + N^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\theta\right),$$

*where the function $L$ is defined by (26). Recall $\mathrm{S}_J(\boldsymbol{G}')$ from (23). There exists a finite constant $\wp_{t,1}$ such that for any large finite constant $\theta_{\max}$, it holds with probability $1 - o_N(1)$ that*

$$\frac{1}{N}\log\mathbb{E}\left(\mathrm{S}_J(\boldsymbol{G}') \,\middle|\, \mathscr{F}'(t)\right) \leqslant \inf\left\{\mathcal{A}\left(\pi(J), \dot{\pi}(J), \dot{\varpi}(J), \theta\right) : \|\theta\| \leqslant \theta_{\max}\right\} + \frac{\wp_{t,1}}{N}$$

*uniformly over all $J \in \{-1, +1\}^N$ with $\|\pi(J)\| \leqslant 4/5$.*

The proof of Proposition A.13 is given at the end of this subsection.

**Definition A.14 (row and column subspaces)** *Given $\mathscr{F}'(t)$ as in (25), define the linear subspaces*

$$V_{\mathrm{R}} \equiv V_{\mathrm{R}}(t) \equiv \operatorname{span}\left\{\mathbf{e}_a(\mathbf{m}^{(s)})^{\mathrm{t}} : 1 \leqslant a \leqslant M, 1 \leqslant s \leqslant t\right\},$$
$$V_{\mathrm{C}} \equiv V_{\mathrm{C}}(t-1) \equiv \operatorname{span}\left\{\mathbf{n}^{(\ell)}(\mathbf{e}_i)^{\mathrm{t}} : 1 \leqslant i \leqslant N, 1 \leqslant \ell \leqslant t-1\right\}.$$

*Let $V_{\mathrm{RC}} \equiv V_{\mathrm{R}} + V_{\mathrm{C}}$. Let $\operatorname{proj}_{\mathrm{R}}$ denote the orthogonal projection onto $V_{\mathrm{R}}$, and define analogously $\operatorname{proj}_{\mathrm{C}}$ and $\operatorname{proj}_{\mathrm{RC}}$. Note that $(\boldsymbol{G}')_{\mathrm{RC}} \equiv \operatorname{proj}_{\mathrm{RC}}(\boldsymbol{G}')$ is measurable with respect to $\mathscr{F}'(t)$.*

**Definition A.15 (row and column events)** *We now let $\boldsymbol{G}$ be an independent copy of $\boldsymbol{G}'$, and define the events*

$$\mathrm{R} \equiv \left\{\operatorname{proj}_{\mathrm{R}}(\boldsymbol{G}) = (\boldsymbol{G}')_{\mathrm{R}}\right\} = \left\{\frac{\boldsymbol{G}\mathbf{m}^{(s)}}{N^{1/2}} = \mathbf{h}^{(s+1)} + \beta'\mathbf{n}^{(s-1)} \text{ for all } 1 \leqslant s \leqslant t\right\}, \tag{60}$$
$$\mathrm{C} \equiv \left\{\operatorname{proj}_{\mathrm{C}}(\boldsymbol{G}) = (\boldsymbol{G}')_{\mathrm{C}}\right\} = \left\{\frac{\boldsymbol{G}^{\mathrm{t}}\mathbf{n}^{(\ell)}}{N^{1/2}} = \mathbf{H}^{(\ell+1)} + \beta\mathbf{m}^{(\ell-1)} \text{ for all } 1 \leqslant \ell \leqslant t-1\right\}. \tag{61}$$

*We shall refer to* R *as the* ***row event*** *(since it constrains the rows of the matrix $\boldsymbol{G}$). Likewise we shall refer to* C *as the* ***column event****.*

Recall $\mathscr{F}'(t)$ from (25), and define also

$$\mathscr{H}'(t) \equiv \sigma\Big(\Big(\mathbf{m}^{(s)} : s \leqslant t\Big), \Big(\mathbf{n}^{(\ell)} : \ell \leqslant t-1\Big)\Big) \subseteq \mathscr{F}'(t).$$

Our calculation is based on the following resampling principle (proved in §G.2):

**Lemma A.16 (resampling)** *If $f : \mathbb{R}^{M\times N} \to \mathbb{R}$ is any bounded measurable function, then*

$$\mathbb{E}\Big(f(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big) = \mathbb{E}\Big(f(\boldsymbol{G})\,\Big|\,\mathscr{H}'(t), \mathrm{R}, \mathrm{C}, (\boldsymbol{G}')_{\mathrm{RC}}\Big)$$

*where $\boldsymbol{G}$ denotes an independent copy of $\boldsymbol{G}'$; and the events* R *and* C *are defined by (60) and (61).*

**Definition A.17 (configuration-dependent subspaces)** *Given $\mathscr{F}'(t)$ as in (25), and a spin configuration $J \in \{-1,+1\}^N$, recall from Definition A.8 that we decompose $J = J' + J''$, and let $\mathbf{v} \equiv J''/\|J''\|$. We then define the linear subspaces*

$$V_{\mathrm{P}} \equiv \operatorname{span}\left\{\mathbf{e}_a\mathbf{v}^{\mathrm{t}} : 1 \leqslant a \leqslant M\right\},$$
$$V_{\mathrm{A}} \equiv \operatorname{span}\left\{\mathbf{n}^{(\ell)}\mathbf{v}^{\mathrm{t}} : 1 \leqslant \ell \leqslant t-1\right\}.$$

*Note that $V_{\mathrm{A}}$ is a subspace of $V_{\mathrm{P}}$, and is also a subspace of $V_{\mathrm{C}}$. Let $\operatorname{proj}_{\mathrm{A}}$ denote the orthogonal projection onto $V_{\mathrm{A}}$, and note that $(\boldsymbol{G}')_{\mathrm{A}} \equiv \operatorname{proj}_{\mathrm{A}}(\boldsymbol{G}')$ is measurable with respect to $\mathscr{F}'(t)$.*

**Definition A.18 (admissibility event)** *As in Definition A.15, let $\boldsymbol{G}$ be an independent copy of $\boldsymbol{G}'$, and define*

$$\mathrm{A} \equiv \Big\{ \mathrm{proj}_{\mathrm{A}}(\boldsymbol{G}) = (\boldsymbol{G}')_{\mathrm{A}} \Big\} \overset{(61)}{=} \left\{ \frac{\mathbf{n}[t-1]\boldsymbol{G}\mathbf{v}}{N\psi^{1/2}} = \frac{\mathbf{H}[t-1]\mathbf{v}}{(N\psi)^{1/2}} \right\}, \tag{62}$$

*where the last identity holds assuming that the event* C *from* (61) *occurs. Note that* $\mathbf{H}[t-1]\mathbf{v}$ *is determined by the parameter* $\delta(J)$ *from Definition A.8. We refer to* A *as the* ***admissibility event****, and note* $\mathrm{C} \subseteq \mathrm{A}$.

In the setting of the perceptron model, the calculation of Lemma A.16 can be simplified as follows:

**Lemma A.19 (reduction of column constraints)** *If* $h : \mathbb{R}^M \to \mathbb{R}$ *is any bounded measurable function, then*

$$\mathbb{E}\bigg( h(\boldsymbol{G}J) \,\bigg|\, \mathscr{H}'(t), \mathrm{R}, \mathrm{C}, (\boldsymbol{G}')_{\mathrm{RC}} \bigg) = \mathbb{E}\bigg( h(\boldsymbol{G}J) \,\bigg|\, \mathscr{H}'(t), \mathrm{R}, \mathrm{A}, (\boldsymbol{G}')_{\mathrm{RA}} \bigg)$$

*where* $\boldsymbol{G}$ *denotes an independent copy of* $\boldsymbol{G}'$ *and the events* $\mathrm{R}, \mathrm{C}, \mathrm{A}$ *are defined by* (60), (61)*, and* (62).

**Proof** Let $V_{\mathrm{C}\setminus\mathrm{R}}$ be the orthogonal complement of $V_{\mathrm{R}}$ inside $V_{\mathrm{R}} + V_{\mathrm{C}}$: that is,

$$V_{\mathrm{R}} + V_{\mathrm{C}} = V_{\mathrm{R}} \obot V_{\mathrm{C}\setminus\mathrm{R}}\,,$$

where we use $\obot$ to denote the sum of two orthogonal vector spaces. Note that $V_{\mathrm{A}}$ is a subspace of $V_{\mathrm{C}}$ which is orthogonal to $V_{\mathrm{R}}$, so it follows that $V_{\mathrm{A}}$ is also a subspace of $V_{\mathrm{C}\setminus\mathrm{R}}$. Let $\mathrm{proj}_{\mathrm{C}\setminus\mathrm{R}}$ denote the orthogonal projection onto $V_{\mathrm{C}\setminus\mathrm{R}}$. Note that $V_{\mathrm{A}}$ is a subspace of $V_{\mathrm{P}}$, and $V_{\mathrm{P}}$ is orthogonal to $V_{\mathrm{R}}$. We claim that

$$\mathrm{proj}_{\mathrm{C}\setminus\mathrm{R}}(V_{\mathrm{P}}) = V_{\mathrm{A}}\,. \tag{63}$$

Since we already noted that $V_{\mathrm{A}} \subseteq V_{\mathrm{C}\setminus\mathrm{R}}$, it suffices to show inclusion in the other direction. The space $V_{\mathrm{P}}$ is spanned by the elements $\mathbf{e}_a\mathbf{v}^{\mathrm{t}}$. Let $\mathbf{c}^{(\ell)}$, $1 \leqslant \ell \leqslant t-1$, be any orthonormal basis for the span of the vectors $\mathbf{n}^{(\ell)}$, $1 \leqslant \ell \leqslant t-1$. An orthonormal basis for $V_{\mathrm{A}}$ is then given by the matrices $\mathbf{c}^{(\ell)}\mathbf{v}^{\mathrm{t}}$, $1 \leqslant \ell \leqslant t-1$. On the other hand, the space $V_{\mathrm{C}}$ is spanned by the elements $\mathbf{c}^{(\ell)}(\mathbf{e}_i)^{\mathrm{t}}$. We therefore have

$$\begin{aligned}\bigg(\mathbf{e}_a\mathbf{v}^{\mathrm{t}} - \mathrm{proj}_{\mathrm{A}}\Big(\mathbf{e}_a\mathbf{v}^{\mathrm{t}}\Big), \mathbf{c}^{(\ell)}(\mathbf{e}_i)^{\mathrm{t}} - \mathrm{proj}_{\mathrm{R}}\Big(\mathbf{c}^{(\ell)}(\mathbf{e}_i)^{\mathrm{t}}\Big)\bigg) &= \bigg(\mathbf{e}_a\mathbf{v}^{\mathrm{t}} - \mathrm{proj}_{\mathrm{A}}\Big(\mathbf{e}_a\mathbf{v}^{\mathrm{t}}\Big), \mathbf{c}^{(\ell)}(\mathbf{e}_i)^{\mathrm{t}}\bigg) \\ = (\mathbf{c}^{(\ell)})_a\mathbf{v}_i - \bigg( \sum_{k \leqslant t-1} (\mathbf{e}_a\mathbf{v}^{\mathrm{t}}, \mathbf{c}^{(k)}\mathbf{v}^{\mathrm{t}})\mathbf{c}^{(k)}\mathbf{v}^{\mathrm{t}}, \mathbf{c}^{(\ell)}(\mathbf{e}_i)^{\mathrm{t}} \bigg) &= (\mathbf{c}^{(\ell)})_a\mathbf{v}_i - (\mathbf{c}^{(\ell)})_a\mathbf{v}_i = 0\,.\end{aligned}$$

It follows that for any $G_{\mathrm{P}} \in V_{\mathrm{P}}$ we have $G_{\mathrm{P}} - \mathrm{proj}_{\mathrm{A}}(G_{\mathrm{P}})$ orthogonal to $V_{\mathrm{C}\setminus\mathrm{R}}$, which concludes the proof of (63). It follows that $V_{\mathrm{P}} = V_{\mathrm{A}} \obot V_{\mathrm{P}\setminus\mathrm{A}}$ where $V_{\mathrm{P}\setminus\mathrm{A}}$ is the orthogonal complement of $V_{\mathrm{A}}$ inside $V_{\mathrm{P}}$, and $V_{\mathrm{P}\setminus\mathrm{A}}$ is orthogonal to $V_{\mathrm{C}\setminus\mathrm{R}}$. As a result, if $\boldsymbol{G}$ is an $M \times N$ matrix with i.i.d. standard gaussian entries, we can decompose $\boldsymbol{G}_{\mathrm{P}} = \boldsymbol{G}_{\mathrm{A}} + \boldsymbol{G}_{\mathrm{P}\setminus\mathrm{A}}$ where $\boldsymbol{G}_{\mathrm{P}\setminus\mathrm{A}} = \mathrm{proj}_{\mathrm{P}\setminus\mathrm{A}}(\boldsymbol{G})$ is independent of $\boldsymbol{G}_{\mathrm{C}\setminus\mathrm{R}}$. It follows that

$$\begin{aligned}\mathbb{E}\bigg(h(\boldsymbol{G}J)\,\bigg|\,\mathscr{H}'(t), \mathrm{R}, \mathrm{C}, (\boldsymbol{G}')_{\mathrm{RC}}\bigg) &= \mathbb{E}\bigg(h(\boldsymbol{G}_{\mathrm{R}}J' + \boldsymbol{G}_{\mathrm{P}}J'')\,\bigg|\,\mathscr{H}'(t), \mathrm{R}, \mathrm{A}, \mathrm{C}, (\boldsymbol{G}')_{\mathrm{RC}}\bigg)\\ &= \mathbb{E}\bigg(h(\boldsymbol{G}_{\mathrm{R}}J' + (\boldsymbol{G}_{\mathrm{A}} + \boldsymbol{G}_{\mathrm{P}\setminus\mathrm{A}})J'')\,\bigg|\,\mathscr{H}'(t), \mathrm{R}, \mathrm{A}, \mathrm{C}, (\boldsymbol{G}')_{\mathrm{RC}}\bigg)\\ &= \mathbb{E}\bigg(h(\boldsymbol{G}_{\mathrm{R}}J' + (\boldsymbol{G}_{\mathrm{A}} + \boldsymbol{G}_{\mathrm{P}\setminus\mathrm{A}})J'')\,\bigg|\,\mathscr{H}'(t), \mathrm{R}, \mathrm{A}, (\boldsymbol{G}')_{\mathrm{RA}}\bigg)\\ &= \mathbb{E}\bigg(h(\boldsymbol{G}J)\,\bigg|\,\mathscr{H}'(t), \mathrm{R}, \mathrm{A}, (\boldsymbol{G}')_{\mathrm{RA}}\bigg)\,,\end{aligned}$$

as claimed. ■

Further towards the proof of Proposition A.13, we record the following calculations:

**Lemma A.20** *For $J \in \{-1,+1\}^N$, recall the decomposition $J = J' + J''$, and define $\tilde{\boldsymbol{X}}_J \equiv \boldsymbol{G}J'/N^{1/2}$. On the event* R *from* (60)*, we have*

$$\begin{aligned}\tilde{\boldsymbol{X}}_J &= \frac{1}{q^{1/2}}\Big\{\mathbf{h}[t]^{\mathrm{t}}\hat{\pi}(J) + \beta'\mathbf{n}[t-1]^{\mathrm{t}}\acute{\pi}(J)\Big\}\\ &= \mathbf{x}[t]^{\mathrm{t}}\dot{\pi}(J) + N^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\bigg(\dot{\varpi}(J) - \Big(1 - \|\pi(J)\|^2\Big)^{1/2}(\boldsymbol{\Gamma}_N)^{\mathrm{t}}\delta\bigg)\,.\end{aligned}$$

*In the above, $\pi(J)$ is given by Definition A.7; $\hat{\pi}(J)$ and $\delta(J)$ are given by Definition A.8; and $\acute{\pi}(J)$, $\dot{\pi}(J)$, and $\dot{\varpi}(J)$ are defined by Lemma A.10.*

**Proof** Fix $J$ and abbreviate $\pi \equiv \pi(J)$, etc. Conditional on the event R from (60), we have

$$\tilde{\boldsymbol{X}}_J \equiv \frac{\boldsymbol{G}J'}{N^{1/2}} \overset{(50)}{=} \sum_{s\leqslant t}\hat{\pi}_s\frac{\boldsymbol{G}\mathbf{m}^{(s)}}{(Nq)^{1/2}} \overset{(60)}{=} \sum_{s\leqslant t}\frac{\hat{\pi}_s}{q^{1/2}}\Big(\mathbf{h}^{(s+1)} + \beta'\mathbf{n}^{(s-1)}\Big)\,.$$

Recall the notation (39) and (44), and also that $\mathbf{n}^{(0)} \equiv \mathbf{0} \in \mathbb{R}^M$. Therefore the above can be rewritten as

$$\tilde{\boldsymbol{X}}_J = \frac{\mathbf{h}[t]^{\mathrm{t}}\hat{\pi}}{q^{1/2}} + \frac{\beta'\mathbf{n}[t-1]^{\mathrm{t}}\acute{\pi}}{q^{1/2}}\,.$$

Recalling from (11) that $\beta' = 1 - q$, and combining with (39) and (44), gives

$$\tilde{\boldsymbol{X}}_J \overset{(39)}{=} \mathbf{x}[t]^{\mathrm{t}}\boldsymbol{\Lambda}^{\mathrm{t}}\hat{\pi} + \frac{(1-q)\mathbf{n}[t-1]^{\mathrm{t}}\acute{\pi}}{q^{1/2}} \overset{(44)}{=} \mathbf{x}[t]^{\mathrm{t}}\boldsymbol{\Lambda}^{\mathrm{t}}\hat{\pi} + \frac{N^{1/2}\psi^{1/2}(1-q)}{q^{1/2}}\mathbf{c}[t-1](\boldsymbol{\Gamma}_N)^{\mathrm{t}}\acute{\pi}\,.$$

Recalling the notation of Lemma A.10 gives, with $\dot{\pi} \equiv \boldsymbol{\Lambda}^{\mathrm{t}}\hat{\pi}$ and $\dot{\varpi}$ as in (54),

$$\tilde{\boldsymbol{X}}_J = \mathbf{x}[t]^{\mathrm{t}}\dot{\pi} + N^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\bigg(\dot{\varpi} - \Big(1 - \|\pi\|^2\Big)^{1/2}(\boldsymbol{\Gamma}_N)^{\mathrm{t}}\delta\bigg)\,.$$

This concludes the proof. ■

**Lemma A.21** *Given $J \in \{-1,+1\}^N$, define the cumulant-generating function*

$$\tilde{\mathcal{K}}_J(\tau) \equiv \frac{1}{N}\log\mathbb{E}\bigg[\exp\bigg\{N^{1/2}\sum_{\ell\leqslant t-1}\tau_\ell(\mathbf{c}^{(\ell)},\boldsymbol{G}\mathbf{v})\bigg\}\mathrm{S}_J(\boldsymbol{G})\,\bigg|\,\mathscr{H}'(t),\mathrm{R}\bigg]$$

*for $\tau \in \mathbb{R}^{t-1}$. Then, with $L$ as in (26), the function $\tilde{\mathcal{K}}_J$ satisfies*

$$\tilde{\mathcal{K}}_J(\tau) - \frac{\|\tau\|^2}{2} = \frac{1}{N}\bigg(\mathbf{1}, L_{\|\pi(J)\|^2}\bigg(\tilde{\boldsymbol{X}}_J + N^{1/2}\Big(1-\|\pi(J)\|^2\Big)^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\tau\bigg)\bigg) \equiv \tilde{\mathcal{L}}_J(\tau)\,,$$

*with $\pi(J)$ as in Definition A.7 and $\tilde{\boldsymbol{X}}_J$ is as in Lemma A.20.*

**Proof** Conditional on $\mathscr{H}'(t)$ and on the event R, it follows from Lemma A.20 that $\boldsymbol{G}J'/N^{1/2} = \tilde{\boldsymbol{X}}_J \equiv \tilde{\boldsymbol{X}}$. We also have

$$\frac{\boldsymbol{G}J''}{N^{1/2}} = \frac{\|J''\|}{N^{1/2}}\boldsymbol{G}\mathbf{v} \equiv \Big(1-\|\pi\|^2\Big)^{1/2}\boldsymbol{\xi}\,,$$

where $\pi \equiv \pi(J)$, and $\boldsymbol{\xi} \equiv \boldsymbol{G}\mathbf{v}$ is distributed as an independent gaussian vector in $\mathbb{R}^N$. It follows that

$$\tilde{\mathcal{K}}_J(\tau) = \frac{1}{N}\sum_{a\leqslant M}\log\mathbb{E}_\xi\bigg[\exp\bigg\{N^{1/2}\sum_{\ell\leqslant t-1}\tau_\ell(\mathbf{c}^{(\ell)})_a\xi\bigg\}U\bigg(\tilde{\boldsymbol{X}}_a + \Big(1-\|\pi\|^2\Big)^{1/2}\xi\bigg)\bigg]\,,$$

where $\xi$ denotes a standard gaussian random variable. Making a change of variable gives

$$\tilde{\mathcal{K}}_J(\tau) = \frac{\|\tau\|^2}{2} + \frac{1}{N}\sum_{a\leqslant M}\log\mathbb{E}_\xi U\bigg(\tilde{\boldsymbol{X}}_a + \Big(1-\|\pi\|^2\Big)^{1/2}\bigg[\xi + N^{1/2}\sum_{\ell\leqslant t-1}\tau_\ell\mathbf{c}_a^{(\ell)}\bigg]\bigg)\,,$$

from which the result follows. ■

Having collected most of the necessary ingredients, we now prove the main result of this subsection. The proof requires one more slightly technical estimate which we defer to Proposition E.13 in Section E.

**Proof** [Proof of Proposition A.13] With $\mathscr{F}'(t)$ as in (25) and $\mathrm{S}_J(\boldsymbol{G}')$ as in (23), let us abbreviate the quantity of interest as

$$E_J \equiv \mathbb{E}\Big(\mathrm{S}_J(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big)\,.$$

By the resampling principle from Lemma A.16, we can express

$$E_J = \mathbb{E}\Big(\mathrm{S}_J(\boldsymbol{G})\,\Big|\,\mathscr{H}'(t),\mathrm{R},\mathrm{C},(\boldsymbol{G}')_{\mathrm{RC}}\Big)\,,$$

where $\boldsymbol{G}$ is an independent copy of $\boldsymbol{G}'$, and R and C are the row and column events of Definition A.15. Applying Lemma A.19 then gives the further simplification

$$E_J = \mathbb{E}\Big(\mathrm{S}_J(\boldsymbol{G})\,\Big|\,\mathscr{H}'(t),\mathrm{R},\mathrm{A},(\boldsymbol{G}')_{\mathrm{RA}}\Big)\,, \tag{64}$$

where A is the admissibility event defined by (62).

Let $V_{\mathrm{R}}$ be as in Definition A.14, and note that an orthonormal basis for $V_{\mathrm{R}}$ is given by the elements $\mathbf{e}_a(\mathbf{r}^{(s)})^{\mathrm{t}}$ for $1 \leqslant a \leqslant M$, $1 \leqslant s \leqslant t$. Denote

$$\mathbf{g}_{\mathrm{R}} \equiv \bigg( (\boldsymbol{G}, \mathbf{e}_a(\mathbf{r}^{(s)})^{\mathrm{t}}) : 1 \leqslant a \leqslant M, 1 \leqslant s \leqslant t \bigg) \in \mathbb{R}^{Mt} \,.$$

Likewise let $V_{\mathrm{P}}$ and $V_{\mathrm{A}}$ be as in Definition A.17: recall that $V_{\mathrm{P}}$ is orthogonal to $V_{\mathrm{R}}$, and $V_{\mathrm{A}}$ is a subpsace of $V_{\mathrm{P}}$. An orthonormal basis for $V_{\mathrm{P}}$ is given by the elements $\mathbf{e}_a\mathbf{v}^{\mathrm{t}}$ for $1 \leqslant a \leqslant M$. Denote

$$\mathbf{g}_{\mathrm{P}} \equiv \bigg( (\boldsymbol{G}, \mathbf{e}_a\mathbf{v}^{\mathrm{t}}) : 1 \leqslant a \leqslant M \bigg) = \boldsymbol{G}\mathbf{v} \in \mathbb{R}^{M} \,. \tag{65}$$

An orthonormal basis for $V_{\mathrm{A}}$ is given by the elements $\mathbf{c}^{(\ell)}\mathbf{v}^{\mathrm{t}}$ for $1 \leqslant \ell \leqslant t-1$, and we shall denote

$$\mathbf{g}_{\mathrm{A}} \equiv \bigg( (\boldsymbol{G}, \mathbf{c}^{(\ell)}\mathbf{v}^{\mathrm{t}}) : 1 \leqslant \ell \leqslant t-1 \bigg) = \mathbf{c}[t-1]\boldsymbol{G}\mathbf{v} \in \mathbb{R}^{t-1} \,. \tag{66}$$

Lastly, as in the proof of Lemma A.19, let $V_{\mathrm{P}\setminus\mathrm{A}}$ be the orthogonal complement of $V_{\mathrm{A}}$ inside $V_{\mathrm{P}}$. Choose an orthonormal basis for $V_{\mathrm{P}\setminus\mathrm{A}}$, and denote it $\boldsymbol{B}_j$ for $1 \leqslant j \leqslant M-(t-1)$. We then let

$$\mathbf{g}_{\mathrm{B}} \equiv \bigg( (\boldsymbol{G}, \boldsymbol{B}_j) : 1 \leqslant j \leqslant M-(t-1) \bigg) \in \mathbb{R}^{M-t+1} \,. \tag{67}$$

Note that there is an orthogonal transformation of $\mathbb{R}^M$ which maps $\mathbf{g}_{\mathrm{P}}$ to the pair $(\mathbf{g}_{\mathrm{A}}, \mathbf{g}_{\mathrm{B}})$. In what follows we let $p_{\mathrm{R}}$ denote the probability density function for $\mathbf{g}_{\mathrm{R}}$, so

$$p_{\mathrm{R}}(g_{\mathrm{R}}) = \frac{1}{(2\pi)^{Mt/2}} \exp\bigg\{ -\frac{\|g_{\mathrm{R}}\|^2}{2} \bigg\} \,. \tag{68}$$

Likewise let $p_{\mathrm{A}}$ and $p_{\mathrm{B}}$ denote the densities for $\mathbf{g}_{\mathrm{A}}$ and $\mathbf{g}_{\mathrm{B}}$ respectively. Since the three subspaces $V_{\mathrm{R}}$, $V_{\mathrm{A}}$, and $V_{\mathrm{B}}$ are mutually orthogonal, the joint density of $(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{A}}, \mathbf{g}_{\mathrm{B}})$ is simply the product $p_{\mathrm{R}}(g_{\mathrm{R}})p_{\mathrm{A}}(g_{\mathrm{A}})p_{\mathrm{B}}(g_{\mathrm{B}})$.

The weight $\mathrm{S}_J(\boldsymbol{G})$, as defined by (23), is a function of $\boldsymbol{G}J$, which we decomposed in the proof of Lemma A.21 as a sum of $\boldsymbol{G}J'$ and $\boldsymbol{G}J''$. Note that $\boldsymbol{G}J'$ is a function of $\mathbf{g}_{\mathrm{R}}$, while $\boldsymbol{G}J''$ is a function of $\mathbf{g}_{\mathrm{P}}$ which in turn is a function of $(\mathbf{g}_{\mathrm{A}}, \mathbf{g}_{\mathrm{B}})$. Thus (23) can be rewritten as a function $\boldsymbol{S}_J$ of $(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{A}}, \mathbf{g}_{\mathrm{B}})$: explicitly,

$$\mathrm{S}_J(\boldsymbol{G}) = \prod_{a \leqslant M} U\bigg( \sum_{s \leqslant t} \frac{(J, \mathbf{r}^{(s)})}{N^{1/2}} (\mathbf{g}_{\mathrm{R}})_{a,s} + \frac{\|J''\|}{N^{1/2}} (\mathbf{g}_{\mathrm{P}})_a \bigg) \equiv \boldsymbol{S}_J(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{A}}, \mathbf{g}_{\mathrm{B}}) \,.$$

On the event R, the value of $\mathbf{g}_{\mathrm{R}}$ is fixed to a value $\bar{g}_{\mathrm{R}}$:

$$(\bar{g}_{\mathrm{R}})_{a,s} = (\boldsymbol{G}\mathbf{r}[t]^{\mathrm{t}})_{a,s} \overset{(43)}{=} \bigg( \frac{\boldsymbol{G}\mathbf{m}[t]^{\mathrm{t}}((\boldsymbol{\Lambda}_N)^{\mathrm{t}})^{-1}}{(Nq)^{1/2}} \bigg)_{a,s} \,,$$

where the right-hand side can be computed from (60). Likewise, on the event A, the value of $\mathbf{g}_{\mathrm{A}}$ is fixed to a value $\bar{g}_{\mathrm{A}}$. We then introduce a parameter $\tau \in \mathbb{R}^{t-1}$, and define

$$\mathrm{S}_{J,\tau}(\boldsymbol{G}) \equiv \boldsymbol{S}_{J,\tau}(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{A}}, \mathbf{g}_{\mathrm{B}}) \equiv \boldsymbol{S}_J(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{A}}, \mathbf{g}_{\mathrm{B}}) \exp\Big\{ N^{1/2}(\tau, \mathbf{g}_{\mathrm{A}}) \Big\} \,. \tag{69}$$

Then, for any $\tau \in \mathbb{R}^{t-1}$, we can rewrite (64) as

$$\begin{aligned} E_J &= \mathbb{E}\Big(\mathrm{S}_J(\boldsymbol{G}) \,\Big|\, \mathscr{H}'(t), \mathrm{R}, \mathrm{A}, (\boldsymbol{G}')_{\mathrm{RA}}\Big) = \mathbb{E}\bigg(\frac{\boldsymbol{S}_{J,\tau}(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{A}}, \mathbf{g}_{\mathrm{B}})}{\exp(N^{1/2}(\tau, \bar{g}_{\mathrm{A}}))} \,\bigg|\, (\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{A}}) = (\bar{g}_{\mathrm{R}}, \bar{g}_{\mathrm{A}})\bigg) \\ &= \frac{1}{\exp(N^{1/2}(\tau, \bar{g}_{\mathrm{A}}))} \int \boldsymbol{S}_{J,\tau}(\bar{g}_{\mathrm{R}}, \bar{g}_{\mathrm{A}}, g_{\mathrm{B}}) p_{\mathrm{B}}(g_{\mathrm{B}})\, dg_{\mathrm{B}}\,. \end{aligned} \tag{70}$$

By contrast, the expected value of $\mathrm{S}_{J,\tau}$ given only the row constraints is

$$\begin{aligned} \boldsymbol{E}_J(\tau \,|\, \bar{g}_{\mathrm{R}}) &\equiv \mathbb{E}\Big(\mathrm{S}_{J,\tau}(\boldsymbol{G}) \,\Big|\, \mathscr{H}'(t), \mathrm{R}, (\boldsymbol{G}')_{\mathrm{R}}\Big) = \mathbb{E}\Big(\boldsymbol{S}_{J,\tau}(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{A}}, \mathbf{g}_{\mathrm{B}}) \,\Big|\, \mathbf{g}_{\mathrm{R}} = \bar{g}_{\mathrm{R}}\Big) \\ &= \int p_{\mathrm{A}}(g_{\mathrm{A}}) \int \boldsymbol{S}_{J,\tau}(\bar{g}_{\mathrm{R}}, g_{\mathrm{A}}, g_{\mathrm{B}}) p_{\mathrm{B}}(g_{\mathrm{B}})\, dg_{\mathrm{B}}\, dg_{\mathrm{A}} = \exp(N \tilde{\mathcal{K}}_J(\tau))\,, \end{aligned} \tag{71}$$

which was computed in Lemma A.21 above. We then let $\mathbf{p}_{J,\tau}(\cdot \,|\, \bar{g}_{\mathrm{R}})$ be the probability density function of $g_{\mathrm{A}}$ under the measure that is biased by $\mathrm{S}_{J,\tau}(\boldsymbol{G})$, conditional on the event R, that is to say,

$$\begin{aligned} \mathbf{p}_{J,\tau}(g_{\mathrm{A}} \,|\, \bar{g}_{\mathrm{R}})\, dg_{\mathrm{A}} &\equiv \frac{\mathbb{E}(\mathrm{S}_{J,\tau}(\boldsymbol{G}) \mathbf{1}\{\mathbf{g}_{\mathrm{A}} \in dg_{\mathrm{A}}\} \,|\, \mathscr{H}'(t), \mathrm{R}, (\boldsymbol{G}')_{\mathrm{R}})}{\mathbb{E}(\mathrm{S}_{J,\tau}(\boldsymbol{G}) \,|\, \mathscr{H}'(t), \mathrm{R}, (\boldsymbol{G}')_{\mathrm{R}})} \\ &\equiv \frac{p_{\mathrm{A}}(g_{\mathrm{A}})}{\boldsymbol{E}_J(\tau \,|\, \bar{g}_{\mathrm{R}})} \bigg[\int \boldsymbol{S}_{J,\tau}(\bar{g}_{\mathrm{R}}, g_{\mathrm{A}}, g_{\mathrm{B}}) p_{\mathrm{B}}(g_{\mathrm{B}})\, dg_{\mathrm{B}}\bigg] dg_{\mathrm{A}}\,. \end{aligned} \tag{72}$$

Then, for any $\tau \in \mathbb{R}^{t-1}$, we can rewrite (70) as

$$E_J = \frac{\boldsymbol{E}_J(\tau \,|\, \bar{g}_{\mathrm{R}}) \cdot \mathbf{p}_{J,\tau}(\bar{g}_{\mathrm{A}} \,|\, \bar{g}_{\mathrm{R}})}{\exp\{N^{1/2}(\tau, \bar{g}_{\mathrm{A}})\} \cdot p_{\mathrm{A}}(\bar{g}_{\mathrm{A}})}\,. \tag{73}$$

We will show in Proposition E.13 (deferred to Section E) that there is a finite constant $\wp_{t,0}$ such that for any finite constant $\tau_{\max}$, we have the uniform bound

$$\max\bigg\{\Big\|\mathbf{p}_{J,\tau}(\cdot \,|\, \bar{g}_{\mathrm{R}})\Big\|_\infty : J \in \{-1,+1\}^N, \|\pi(J)\| \leqslant \frac{4}{5}, \|\tau\| \leqslant \tau_{\max}\bigg\} \leqslant \wp_{t,0} \tag{74}$$

with high probability. It therefore remains to estimate the other two terms on the right-hand side of (73). We then note that Definition A.18 implies that, on the event A, we have

$$\begin{aligned} \frac{\bar{g}_{\mathrm{A}}}{N^{1/2}} = \frac{\mathbf{g}_{\mathrm{A}}}{N^{1/2}} &\overset{(66)}{=} \frac{\mathbf{c}[t-1]\boldsymbol{G}\mathbf{v}}{N^{1/2}} \overset{(44)}{=} \frac{(\boldsymbol{\Gamma}_N)^{-1}\mathbf{n}[t-1]\boldsymbol{G}\mathbf{v}}{N\psi^{1/2}} \\ &\overset{(62)}{=} \frac{(\boldsymbol{\Gamma}_N)^{-1}\mathbf{H}[t-1]\mathbf{v}}{(N\psi)^{1/2}} \overset{(51)}{=} (\boldsymbol{\Gamma}_N)^{\mathrm{t}}\delta\,. \end{aligned} \tag{75}$$

Substituting (75) into the formula for $p_{\mathrm{A}}$ (similar to (68)) gives

$$p_{\mathrm{A}}(\bar{g}_{\mathrm{A}}) = \frac{1}{(2\pi)^{(t-1)/2}} \exp\bigg\{-\frac{N\|(\boldsymbol{\Gamma}_N)^{\mathrm{t}}\delta\|^2}{2}\bigg\}\,. \tag{76}$$

Meanwhile, it follows by combining (71) and (75) that

$$\frac{\boldsymbol{E}_J(\tau \,|\, \bar{g}_{\mathrm{R}})}{\exp\{N^{1/2}(\tau, \bar{g}_{\mathrm{A}})\}} = \exp\bigg\{N\Big[\tilde{\mathcal{K}}_J(\tau) - (\tau, (\boldsymbol{\Gamma}_N)^{\mathrm{t}}\delta)\Big]\bigg\}\,. \tag{77}$$

Substituting (74), (76), and (77) into (73) gives

$$\frac{E_J}{(2\pi)^{t/2}\cdot\wp_{t,0}} \leqslant \exp\left\{N\left[\tilde{\mathcal{K}}_J(\tau) - (\tau, (\mathbf{\Gamma}_N)^{\mathrm{t}}\delta) + \frac{\|(\mathbf{\Gamma}_N)^{\mathrm{t}}\delta\|^2}{2}\right]\right\}.$$

Recalling the calculation of $\tilde{\mathcal{K}}_J(\tau)$ from Lemma A.21 gives

$$\frac{E_J}{(2\pi)^{t/2}\cdot\wp_{t,0}} \leqslant \exp\left\{N\left[\frac{\|\tau-(\mathbf{\Gamma}_N)^{\mathrm{t}}\delta\|^2}{2} + \tilde{\mathcal{L}}_J(\tau)\right]\right\} \equiv \exp\left\{N\tilde{\mathcal{A}}_J(\tau)\right\}, \tag{78}$$

where $\tilde{\mathcal{A}}_J$ is defined by the last identity. To simplify the above expression, we will recenter $\tau$ around

$$\bar{\tau} \equiv \bar{\tau}(\acute{\pi}) \equiv -\frac{\psi^{1/2}(1-q)(\mathbf{\Gamma}_N)^{\mathrm{t}}\acute{\pi}}{q^{1/2}(1-\|\pi\|^2)^{1/2}} \overset{(54)}{=} -\frac{\dot{\varpi}}{(1-\|\pi\|^2)^{1/2}} + (\mathbf{\Gamma}_N)^{\mathrm{t}}\delta\,. \tag{79}$$

We then make a change of variables from $\tau$ to $\theta$, via the definition

$$\tau \equiv \bar{\tau} + \frac{\theta}{(1-\|\pi\|^2)^{1/2}}\,. \tag{80}$$

This change of variables results in the simplification

$$\tau - (\mathbf{\Gamma}_N)^{\mathrm{t}}\delta \overset{(80)}{=} \bar{\tau} + \frac{\theta}{(1-\|\pi\|^2)^{1/2}} - (\mathbf{\Gamma}_N)^{\mathrm{t}}\delta \overset{(79)}{=} \frac{\theta-\dot{\varpi}}{(1-\|\pi\|^2)^{1/2}}\,.$$

The computation of $\tilde{\boldsymbol{X}}_J$ from Lemma A.20 can also be rewritten as

$$\tilde{\boldsymbol{X}}_J \overset{(79)}{=} \mathbf{x}[t]^{\mathrm{t}}\dot{\pi} - N^{1/2}\Big(1-\|\pi\|^2\Big)^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\bar{\tau}\,. \tag{81}$$

As a result the function $\tilde{\mathcal{L}}_J$ from Lemma A.21 can be reparametrized as

$$\tilde{\mathcal{L}}_J\left(\bar{\tau} + \frac{\theta}{(1-\|\pi\|^2)^{1/2}}\right) \overset{(81)}{=} \frac{1}{N}\Big(\mathbf{1}, L_{\|\pi\|^2}\Big(\mathbf{x}[t]^{\mathrm{t}}\dot{\pi} + N^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\theta\Big)\Big)\,.$$

It follows by substituting the above calculations into (78) that

$$\tilde{\mathcal{A}}_J\left(\bar{\tau} + \frac{\theta}{(1-\|\pi\|^2)^{1/2}}\right) = \frac{\|\dot{\varpi}-\theta\|^2}{2(1-\|\pi\|^2)} + \frac{1}{N}\sum_{a\leqslant M} L_{\|\pi\|^2}\Big(\mathbf{x}[t]^{\mathrm{t}}\dot{\pi} + N^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\theta\Big)\,.$$

The claim follows by taking $\wp_{t,1} \equiv (\log\wp_{t,0} + t\log(2\pi))/2$. ■

The above completes the proof of Proposition A.13, modulo Proposition E.13 which is deferred to Section E.

### A.5. First moment for partition function

We now collect some of the preceding results to complete the proof of the main result of this section:
**Proof** [Proof of Theorem A.12] For any $J \in \{-1,+1\}^N$ we can calculate (abbreviating $\varpi \equiv \varpi(J)$)

$$\frac{(\mathbf{H}^{(t)}, J)}{N} = \frac{(\acute{e}_{t-1})^{\mathsf{t}}\mathbf{H}[t-1]J}{N} \overset{(38)}{=} \frac{\psi^{1/2}(\acute{e}_{t-1})^{\mathsf{t}}\mathbf{\Gamma}\mathbf{y}[t-1]J}{N} \overset{(49)}{=} (\psi^{1/2}\mathbf{\Gamma}^{\mathsf{t}}\acute{e}_{t-1}, \varpi) \overset{(56)}{=} \frac{(\varpi_*, \varpi)}{1-q}\,.$$

It follows by combining with Definition A.11 that

$$\begin{aligned}\frac{\mathbb{E}(\boldsymbol{Z}_\circ(\boldsymbol{G}') \mid \mathscr{F}'(t))}{\exp\{(\mathbf{1}, \log(2\,\mathrm{ch}(\mathbf{H}^{(t)})))\}} &= \sum_{J\in\mathbb{H}_\circ} \mathbf{Q}(J)\bigg(\frac{\mathbf{P}(J)}{\mathbf{Q}(J)\exp\{(\mathbf{1}, \log\mathrm{ch}(\mathbf{H}^{(t)}))\}}\bigg)\mathbb{E}\Big(\mathrm{S}_J(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big)\\ &= \sum_{J\in\mathbb{H}_\circ} \mathbf{Q}(J)\exp\bigg\{-\frac{N(\varpi_*, \varpi)}{1-q}\bigg\}\mathbb{E}\Big(\mathrm{S}_J(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big)\,. \qquad (82)\end{aligned}$$

Combining Proposition A.13 with Lemma A.10 gives, with high probability,

$$\mathbb{E}\Big(\mathrm{S}_J(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big) \leqslant \frac{\|\varpi-\theta\|^2}{2(1-\|\pi\|^2)} + \frac{1}{N}\sum_{a\leqslant M} L_{\|\pi\|^2}\Big(\mathbf{x}[t]^{\mathsf{t}}\pi + N^{1/2}\mathbf{c}[t-1]^{\mathsf{t}}\theta\Big) + \mathrm{ERR}_{t,3}\,,$$

uniformly over $\|\pi(J)\| \leqslant 4/5$ and $\|\theta\| \leqslant \theta_{\max}$. The claim follows by setting $\theta = \bar{\epsilon}(\varpi - \varpi_*)$. ■

Recall from (59) that $\boldsymbol{Z} = \boldsymbol{Z}_\circ + \boldsymbol{Z}_\bullet$ where $\boldsymbol{Z}_\circ$ is bounded by Theorem A.12. In the remainder of this section we show that the other quantity $\boldsymbol{Z}_\bullet$ can be bounded by *a priori* estimates. For this purpose we prove a rough estimate on $\pi(J)$ (Lemma A.22), followed by a more precise estimate on $\varpi(J)$ (Lemma A.23). In fact Lemma A.23 is more precise than what is needed to analyze $\boldsymbol{Z}_\bullet$, but it will be needed later (in Section C) in the analysis of $\boldsymbol{Z}_\circ$. We first state and prove the estimate for $\pi(J)$:

**Lemma A.22** *Recall $\pi(J)$ from Definition A.7 and $\dot{\pi}_*$ from (55). For $\mathbf{Q}$ as in Definition A.11, we have*

$$\mathbf{Q}\bigg(\bigg\{J \in \{-1,+1\}^N : \Big\|\pi(J) - \dot{\pi}_*\Big\| \geqslant d\bigg\}\bigg) \leqslant \bigg(\frac{66t}{q}\bigg)^{t/2}\exp\bigg\{-\frac{Nd^2(1-3q^{1/2})}{8}\bigg\}$$

*for all $|d| \geqslant 1/N^{1/2}$. (The bound is vacuous unless $Nd^2$ is large compared to $t\log t$.)*

**Proof** Under the measure $\mathbf{Q}$, the random vector $J - \mathbf{m}^{(t)}$ has independent entries of mean zero. We note also that

$$(\mathfrak{m}_i)^2 \equiv \max\bigg\{\Big|J_i - (\mathbf{m}^{(t)})_i\Big|^2 : J_i \in \{-1,+1\}\bigg\} \leqslant \Big(1 + |(\mathbf{m}^{(t)})_i|\Big)^2 \leqslant 1 + 3|(\mathbf{m}^{(t)})_i| \leqslant 4\,. \quad (83)$$

Thus for any $a \in \mathbb{R}^t$ we can bound

$$V_{\max}(a) \equiv \sum_{i\leqslant N}\bigg(\sum_{s\leqslant t} a_s(\mathbf{r}^{(s)})_i\bigg)^2(\mathfrak{m}_i)^2 \leqslant 4\bigg\|\sum_{s\leqslant t} a_s\mathbf{r}^{(s)}\bigg\|^2 = 4\|a\|^2\,.$$

It follows by the Azuma–Hoeffding bound that

$$\mathbf{Q}\bigg(\frac{1}{N^{1/2}}\bigg(\sum_{s\leqslant t} a_s \mathbf{r}^{(s)}, J-\mathbf{m}^{(t)}\bigg) \geqslant x\bigg) \leqslant \exp\bigg\{-\frac{Nx^2}{2V_{\max}(a)}\bigg\} \leqslant \exp\bigg\{-\frac{Nx^2}{8\|a\|^2}\bigg\}. \tag{84}$$

On the other hand, it follows from Definition A.7 and (55) that

$$\frac{1}{N^{1/2}}\bigg(\sum_{s\leqslant t} a_s \mathbf{r}^{(s)}, J-\mathbf{m}^{(t)}\bigg) = \Big(a, \pi(J)-\dot{\pi}_*\Big). \tag{85}$$

Given $d>0$ and $\epsilon \in (0,1/4]$, note there exists a $(d\epsilon)$-net of $[-4d,4d]^t$ of cardinality at most

$$\left\lceil \frac{8t^{1/2}}{\epsilon}\right\rceil^t \leqslant \bigg(\frac{8t^{1/2}}{\epsilon}+1\bigg)^t. \tag{86}$$

If $J$ is any element of $\{-1,+1\}^N$ with $d \leqslant \|\pi(J)-\dot{\pi}_*\| \leqslant 2d$, and $\pi_{\text{net}}$ is an element of the $(d\epsilon)$-net at minimal distance from $\pi(J)$, then $\|\pi_{\text{net}}-\dot{\pi}_*\| \geqslant d(1-\epsilon)$, and

$$\Big(\pi_{\text{net}}-\dot{\pi}_*, \pi(J)-\dot{\pi}_*\Big) \geqslant \Big\|\pi(J)-\dot{\pi}_*\Big\|^2 - \bigg|\Big(\pi_{\text{net}}-\pi(J), \pi(J)-\dot{\pi}_*\Big)\bigg| \geqslant d^2(1-2\epsilon).$$

Thus, by taking $a=\pi_{\text{net}}-\dot{\pi}_*$ and $\epsilon = q^{1/2}$ in (84) and (85), we obtain

$$\begin{aligned}\mathbf{Q}\Big(d \leqslant \Big\|\pi(J)-\dot{\pi}_*\Big\| \leqslant 2d\Big) &\leqslant \bigg(\frac{65t}{q}\bigg)^{t/2} \exp\bigg\{-\frac{Nd^4(1-2q^{1/2})^2}{8d^2(1-q^{1/2})^2}\bigg\} \\ &\leqslant \bigg(\frac{65t}{q}\bigg)^{t/2} \exp\bigg\{-\frac{Nd^2(1-3q^{1/2})}{8}\bigg\}.\end{aligned}$$

Since $4^k \geqslant 3k$ for all $k \geqslant 0$, as long as $Nd^2 \geqslant 1$ we can bound

$$\mathbf{Q}\Big(\Big\|\pi(J)-\dot{\pi}_*\Big\| \geqslant d\Big) \leqslant \sum_{k\geqslant 0} \frac{(65t/q)^{t/2}}{\exp\{N(2^k d)^2(1-3q^{1/2})/8\}} \leqslant \frac{2(65t/q)^{t/2}}{\exp\{Nd^2(1-3q^{1/2})/8\}}.$$

This proves the claim. ■

The result for $\varpi(J)$ is very similar, although slightly more involved since we require a more precise estimate:

**Lemma A.23** *Recall $\varpi(J)$ from Definition A.7, and $\dot{\varpi}_*$ from (56). For $\mathbf{Q}$ as in Definition A.11, we have*

$$\mathbf{Q}\bigg(\bigg\{J\in\{-1,+1\}^N : \Big\|\varpi(J)-\dot{\varpi}_*\Big\| \geqslant d\bigg\}\bigg) \leqslant \bigg(\frac{66t}{q}\bigg)^{t/2} \exp\bigg\{-\frac{Nd^2(1-8q^{1/2})}{2}\bigg\}$$

*for all $|d| \geqslant 1/N^{1/2}$. (The bound is vacuous unless $Nd^2$ is large compared to $t\log t$.)*

**Proof** Recall the definition of $\mathfrak{m}_i$ from the bound (83) in the proof of Lemma A.22. For $b \in \mathbb{R}^{t-1}$, denote

$$W_{\max}(b) \equiv \frac{1}{N}\sum_{i\leqslant N}\bigg(\sum_{\ell\leqslant t-1} b_\ell(\mathbf{y}^{(\ell)})_i\bigg)^2(\mathfrak{m}_i)^2 \leqslant W_0(b)+3W_1(b)\,.$$

Applying (83) gives $W_{\max} \leqslant W_0 + 3W_1$ where

$$W_0(b) \equiv \frac{1}{N}\bigg\|\sum_{\ell\leqslant t-1} b_\ell \mathbf{y}^{(\ell)}\bigg\|^2\,,$$

$$W_1(b) \equiv \frac{1}{N}\sum_{i\leqslant N}\bigg(\sum_{\ell\leqslant t-1} b_\ell(\mathbf{y}^{(\ell)})_i\bigg)^2|(\mathbf{m}^{(t)})_i|\,.$$

It follows from Lemma A.4 that $W_0(b) \to \|b\|^2$ in probability as $N \to \infty$. Lemma A.4 also implies

$$\frac{W_1(b)}{\|b\|^2} \overset{N\to\infty}{\longrightarrow} \mathbb{E}\bigg[\Big(\rho Z + (1-\rho^2)^{1/2}Z'\Big)^2\Big|\mathrm{th}(\psi^{1/2}Z)\Big|\bigg] \equiv w_1(\rho)\,.$$

in probability, where $\rho \in [-1,1]$ is a value that can depend on $b$. However we can crudely bound

$$w_1(\rho) \leqslant \Big(\mathbb{E}(Z^4)\mathbb{E}[\mathrm{th}(\psi^{1/2}Z)^2]\Big)^{1/2} \overset{(9)}{=} (3q)^{1/2}\,.$$

It follows by the Azuma–Hoeffding inequality that

$$\mathbf{Q}\bigg(\frac{1}{N}\bigg(\sum_{\ell\leqslant t-1} b_\ell\mathbf{y}^{(\ell)}, J-\mathbf{m}^{(t)}\bigg) \geqslant x\bigg) \leqslant \exp\bigg\{-\frac{Nx^2}{2W_{\max}(b)}\bigg\} \leqslant \exp\bigg\{-\frac{Nx^2}{2\|b\|^2(1+6q^{1/2})}\bigg\}\,. \tag{87}$$

On the other hand, it follows from Definition A.7 and (56) that

$$\frac{1}{N}\bigg(\sum_{\ell\leqslant t-1} b_\ell\mathbf{y}^{(\ell)}, J-\mathbf{m}^{(t)}\bigg) = \Big(b, \varpi(J)-\dot{\varpi}_*\Big)\,. \tag{88}$$

Given $d > 0$ and $\epsilon \in (0, 1/4]$, note there exists a $(d\epsilon)$-net of $[-4d, 4d]^{t-1}$ with cardinality upper bounded by (86). If $J$ is any element of $\{-1,+1\}^N$ with $d \leqslant \|\varpi(J)-\dot{\varpi}_*\| \leqslant 2d$, and $\varpi_{\mathrm{net}}$ is an element of the $(d\epsilon)$-net at minimal distance from $\varpi(J)$, then $\|\varpi_{\mathrm{net}}-\dot{\varpi}_*\| \geqslant d(1-\epsilon)$, and

$$\Big(\varpi_{\mathrm{net}}-\dot{\varpi}_*, \varpi(J)-\dot{\varpi}_*\Big) \geqslant \Big\|\varpi(J)-\dot{\varpi}_*\Big\|^2 - \Big|(\varpi_{\mathrm{net}}-\varpi(J), \varpi(J)-\dot{\varpi}_*)\Big| \geqslant d^2(1-2\epsilon)\,.$$

Thus, by taking $\epsilon = q^{1/2}$ and $b = \varpi_{\mathrm{net}} - \dot{\varpi}_*$ in (87) and (88), we obtain

$$\begin{aligned}\mathbf{Q}\Big(d \leqslant \Big\|\varpi(J)-\dot{\varpi}_*\Big\| \leqslant 2d\Big) &\leqslant \Big(\frac{65t}{q}\Big)^{t/2}\exp\bigg\{-\frac{Nd^4(1-2q^{1/2})^2}{2d^2(1-q^{1/2})^2(1+6q^{1/2})}\bigg\}\\ &\leqslant \Big(\frac{65t}{q}\Big)^{t/2}\exp\bigg\{-\frac{Nd^2(1-8q^{1/2})}{2}\bigg\}\,.\end{aligned}$$

Since $4^k \geqslant 3k$ for all $k \geqslant 0$, as long as $Nd^2 \geqslant 1$ we can bound

$$\mathbf{Q}\Big(\Big\|\varpi(J)-\dot{\varpi}_*\Big\| \geqslant d\Big) \leqslant \sum_{k\geqslant 0}\frac{(65t/q)^{t/2}}{\exp\{N(2^kd)^2(1-8q^{1/2})/2\}} \leqslant \frac{2(65t/q)^{t/2}}{\exp\{Nd^2(1-8q^{1/2})/2\}}\,.$$

The claim follows. ■

## Appendix B. Technical estimates

We now collect some technical results which will be used later in the proof. This section is organized as follows:

- In §B.1 we prove some basic consequences of Assumptions 1 and 2.
- In §B.2 we give the proof of Proposition A.1, which characterizes the replica symmetric fixed-point solution. As a consequence of this analysis we obtain a rough estimate (Corollary B.8) of the replica symmetric formula (29), which will be used in later sections. We also prove Proposition 1.8, showing that the replica symmetric formula for $U_\eta$ converges to the one for $U$ as $\eta \downarrow 0$.
- In §B.3 we prove Lemma B.11, which gives the Almeida–Thouless (AT) condition in our setting.
- In §B.4 we give the proof of Proposition 1.3, showing that Assumption 2 holds if $u \equiv \log U$ is either bounded or concave. We also give the proof of Proposition A.6 (convergence of the state evolution recursions), which amounts to checking that AT condition derived in Lemma B.11 holds for $0 < \alpha \leqslant \alpha(U)$. We conclude the section with some further consequences (Lemmas B.14 and B.15) of Assumption 2.

The following notation will be used throughout the paper:

**Definition B.1** *For $c > 0$ and $x \in \mathbb{R}$, let $\mu_{x,c}$ denote the probability measure on the real line whose density (with respect to the Lebesgue measure) is given by*

$$\frac{d\mu_{x,c}}{dz} = \chi_{x,c}(z) \equiv \frac{U(x+cz)\varphi(z)}{\mathbb{E}_\xi[U(x+c\xi)]}\,.$$

*We use $\mathbb{E}_{x,c}$, $\mathrm{Var}_{x,c}$, and $\mathrm{Cov}_{x,c}$ to denote expectation, variance, and covariance under $\mu_{x,c}$.*

### B.1. Preliminary bounds

In this subsection we prove some basic consequences of Assumptions 1 and 2. As before, $\xi$ denotes a standard gaussian random variable, and $\mathbb{E}_\xi$ denotes expectation over $\xi$.

**Lemma B.2** *Suppose $U$ satisfies Assumption 1, and let $q_{x,c}(z) \equiv U(x+cz)\varphi(z)$ as above. Then, given any $\epsilon > 0$ and any $L < \infty$, it is possible to choose $\eta'$ small enough such that we have the bound*

$$\int \Big| U(x+cz) - U(x'+c'z) \Big| \varphi(z)\, dz \leqslant \epsilon$$

*as long as $c, c' \in [1/3, 3]$, $x, x' \in [-L, L]$, and $\max\{|x-x'|, |c-c'|\} \leqslant \eta'$.*

**Proof** Given $\epsilon > 0$, we can clearly choose $L(\epsilon)$ large enough (depending only on $\epsilon$) such that $L(\epsilon) \geqslant L$, and

$$\int_{|z| \geqslant L(\epsilon)} \Big| U(x+cz) - U(x'+c'z) \Big| \varphi(z)\, dz \leqslant \int_{|z| \geqslant L(\epsilon)} \varphi(z)\, dz \leqslant \frac{\epsilon}{4}\,. \tag{89}$$

If $|z| \leqslant L(\epsilon)$, then the assumptions imply $|x + cz| \leqslant 4L(\epsilon)$ and $|x' + c'z| \leqslant 4L(\epsilon)$, so

$$\int_{|z|\leqslant L(\epsilon)} \Big|U(x+cz) - U(x'+c'z)\Big|\varphi(z)\,dz \leqslant \int \Big|\bar{u}(x+cz) - \bar{u}(x'+c'z)\Big|\varphi(z)\,dz$$

where $\bar{u}(x) \equiv U(x)\mathbf{1}\{|x| \leqslant 4L(\epsilon)\}$. Then, since $\bar{u} \in L^1$, it is well known that we can choose a function $\tilde{u}$ which is compactly supported and smooth, such that $\|\bar{u} - \tilde{u}\|_1 \leqslant \epsilon/4$ (see e.g. (Lieb and Loss, 2001, Lem. 2.19)). Therefore

$$\int \Big|\bar{u}(x+cz) - \tilde{u}(x+cz)\Big|\varphi(z)\,dz \leqslant \varphi(0)\int \Big|\bar{u}(x+cz) - \tilde{u}(x+cz)\Big|\,dz = \frac{\varphi(0)\|\bar{u}-\tilde{u}\|_1}{c} \leqslant \frac{\epsilon}{4},$$

where this estimate holds for all $x \in \mathbb{R}$ and all $c \geqslant 1/2$. We also have

$$\int \Big|\tilde{u}(x+cz) - \tilde{u}(x'+c'z)\Big|\varphi(z)\,dz \leqslant \|\tilde{u}'\|_\infty \int \Big(|x-x'| + |c-c'||z|\Big)\varphi(z)\,dz \leqslant 2\|\tilde{u}'\|_\infty \eta',$$

which can be made at most $\epsilon/4$ by taking $\eta' = \epsilon/(8\|\tilde{u}'\|_\infty)$. Combining the above estimates gives

$$\int_{|z|\leqslant L(\epsilon)} \Big|U(x+cz) - U(x'+c'z)\Big| \leqslant \frac{3\epsilon}{4},$$

and combining with the estimate (89) for $|z| \geqslant L(\epsilon)$ gives the conclusion. ■

**Lemma B.3** *Suppose $U$ satisfies Assumption 1 . There exists a finite constant $C_1(U)$, depending on $U$ only, such that*

$$\mathbb{E}_{x,c}(|Z|^p) = \frac{\mathbb{E}_\xi(|\xi|^p U(x+c\xi))}{\mathbb{E}_\xi U(x+c\xi)} \leqslant C_1(U) + \left(\frac{1.82\cdot|x|}{c}\right)^p$$

*for all $0 \leqslant p \leqslant 200$, $1/2 \leqslant c \leqslant 2$, and $x \in \mathbb{R}$. (We can assume, without loss, $C_1(U) \geqslant 10$.)*

**Proof** It follows from Assumption 1 that $\mathbb{E}_\xi U(c\xi) > 0$ for any $c > 0$. Lemma B.2 gives that $\mathbb{E}_\xi U(c\xi)$ is a continuous function of $1/2 \leqslant c \leqslant 2$, so by compactness considerations we must have

$$\bar{c}_1(U) \equiv \max\left\{2, \sup\left\{\frac{1}{\mathbb{E}_\xi U(c\xi)} : \frac{1}{2} \leqslant c \leqslant 2\right\}\right\} < \infty \tag{90}$$

(where we chose $\bar{c}_1(U) \geqslant 2$ for convenience). Next, for any $M > 0$, it holds for all $1/2 \leqslant c \leqslant 2$ that

$$\mathbb{E}_\xi\Big(U(c\xi); |c\xi| \geqslant M\Big) \leqslant \mathbb{P}\Big(|\xi| \geqslant \frac{M}{c}\Big) \leqslant \frac{\varphi(M/c)}{M/c}.$$

If we take $K \geqslant K_0(U) = (8\log \bar{c}_1(U))^{1/2} \geqslant 2$, then for all $1/2 \leqslant c \leqslant 2$ we have

$$\mathbb{E}_\xi\Big(U(c\xi); |c\xi| \leqslant K\Big) \geqslant \mathbb{E}_\xi U(c\xi) - \frac{\varphi(K/2)}{K/2} \geqslant \frac{1}{2\bar{c}_1(U)}.$$

In what follows let $K(x) \equiv \max\{K_0(U), |x|\}$. Then we can lower bound

$$\begin{aligned}\mathbb{E}_\xi U(x+c\xi) &= \int U(cz)\varphi\Big(z-\frac{x}{c}\Big)\,dz = \int U(cz)\exp\bigg\{-\frac{x^2}{2c^2}+\frac{xz}{c}\bigg\}\varphi(z)\,dz \\ &\geqslant \frac{\mathbb{E}(U(c\xi);|c\xi|\leqslant K(x))}{\exp\{(3/2)K(x)^2/c^2\}} \geqslant \frac{1/(2\bar{c}_1(U))}{\exp\{(3/2)K(x)^2/c^2\}}\,. \end{aligned} \tag{91}$$

Next we note that for any $M \geqslant 0$ and $\eta' = 1/10$ we have

$$\begin{aligned}\mathbb{E}_\xi(|\xi|^p;|\xi|\geqslant M) &= \int_{|z|\geqslant M}\frac{|z|^p}{(2\pi)^{1/2}}\exp\bigg\{-\frac{z^2}{2}\bigg\}\,dz \\ &= \int_{|z|\geqslant M/(1+\eta')^{1/2}}\frac{(1+\eta')^{(p+1)/2}|z|^p}{(2\pi)^{1/2}}\exp\bigg\{-\frac{(1+\eta')z^2}{2}\bigg\}\,dz \\ &\leqslant \sup\bigg\{\frac{1.05^{p+1}|z|^p}{\exp(z^2/20)}:z\in\mathbb{R}\bigg\}\mathbb{P}\bigg(|\xi|\geqslant\frac{M}{(1+\eta')^{1/2}}\bigg) \leqslant c_0\frac{\varphi(M/1.05)}{M/1.05}\,, \end{aligned} \tag{92}$$

where $c_0 \geqslant 5$ is an absolute constant since we restricted $0 \leqslant p \leqslant 200$. Combining (91) with (92) gives

$$\begin{aligned}\frac{\mathbb{E}_\xi(|\xi|^pU(x+c\xi))}{\mathbb{E}_\xi U(x+c\xi)} &\leqslant \bigg(\frac{1.82\cdot K(x)}{c}\bigg)^p + \frac{\mathbb{E}_\xi(|\xi|^p;|\xi|\geqslant 1.82\cdot K(x)/c)}{\mathbb{E}_\xi U(x+c\xi)} \\ &\leqslant \bigg(\frac{1.82\cdot K(x)}{c}\bigg)^p + c_0\cdot\frac{\varphi(1.82\cdot K(x)/(1.05\cdot c))}{1.82\cdot K(x)/(1.05\cdot c)}\cdot\frac{\exp\{(3/2)K(x)^2/c^2\}}{1/(2\bar{c}_1(U))}\,. \end{aligned}$$

(The first inequality above also uses that $U \leqslant 1$, from Assumption 1.) Recalling again the restrictions $1/2 \leqslant c \leqslant 2$ and $0 \leqslant p \leqslant 200$, we can simplify the above to obtain

$$\begin{aligned}\frac{\mathbb{E}_\xi(|\xi|^pU(x+c\xi))}{\mathbb{E}_\xi U(x+c\xi)} &\leqslant \bigg(\frac{1.82\cdot K(x)}{c}\bigg)^p + 2c_0\cdot\bar{c}_1(U)\cdot\varphi\bigg(\frac{1.82\cdot K(x)}{1.05\cdot c}\bigg)\exp\bigg\{\frac{3K(x)^2}{2c^2}\bigg\} \\ &\leqslant \bigg(\frac{1.82\cdot|x|}{c}\bigg)^p + \bigg\{\bigg(\frac{1.82\cdot K_0(U)}{1/2}\bigg)^{200} + \frac{2\cdot c_0\cdot\bar{c}_1(U)}{(2\pi)^{1/2}}\bigg\} \\ &\leqslant \bigg(\frac{1.82\cdot|x|}{c}\bigg)^p + \bigg\{\Big(4K_0(U)\Big)^{200} + c_0\cdot\bar{c}_1(U)\bigg\} \\ &\equiv \bigg(\frac{1.82\cdot|x|}{c}\bigg)^p + C_1(U)\,, \end{aligned} \tag{93}$$

where the last equality defines $C_1(U)$. The above choices guarantee $C_1(U) \geqslant c_0 \cdot \bar{c}_1(U) \geqslant 10$. We define $(C_1)^\wr(U)$ similarly, replacing $\bar{c}_1(U)$ with

$$(\bar{c}_1)^\wr(U) \equiv \max\bigg\{2,\sup\bigg\{\frac{1}{\mathbb{E}_\xi U(c\xi)}:\frac{2}{5}\leqslant c\leqslant\frac{7}{3}\bigg\}\bigg\} < \infty\,. \tag{94}$$

Note that a bound on $(\bar{c}_1)^\wr(U)$ implies a bound on $\bar{c}_1(U_\eta)$ for $\eta$ small enough; this will be spelled out below in the proof of Proposition 1.8. ■

**Remark** *The bound from Lemma B.3 is reasonably tight. To see this, consider the function*

$$U(x) = \mathbf{1}\left\{|x-a| \leqslant \frac{a}{2}\right\}$$

*for $a > 0$. If $U(x+\xi) = 1$, then $x+\xi \geqslant a/2$, so $\xi \geqslant a/2 - x$. In the case that $x \leqslant 0$, it implies $|\xi| \geqslant a/2 + |x|$. It follows that for any $x \leqslant 0$ we have*

$$\mathbb{E}_{x,c}(|Z|^p) = \frac{\mathbb{E}_\xi(|\xi|^p U(x+\xi))}{\mathbb{E}_\xi U(x+\xi)} \geqslant \left(\frac{a}{2} + |x|\right)^p \geqslant \left(\frac{a}{2}\right)^p + |x|^p\,,$$

*where $a > 0$ can be chosen to be arbitrarily large.*

Next we combine Assumption 2 (which bounds $\mathrm{Var}_{x,c}(Z)$) with the calculations of Lemma B.3 to obtain bounds on $\mathrm{Var}_{x,c}(Z^2)$ and $\mathrm{Cov}_{x,c}(Z,Z^2)$:

**Lemma B.4** *Suppose $U$ satisfies Assumptions 1 and 2, and let $C_1(U)$ be as in Lemma B.3. Then we have*

$$\mathrm{Var}_{x,c}(Z^2) \leqslant K_2(U)\cdot\left\{\left(\frac{1.82\cdot|x|}{c}\right)^2 + C_1(U)\right\}, \tag{95}$$

$$\mathrm{Cov}_{x,c}(Z,Z^2) \leqslant \frac{K_2(U)}{2^{1/2}}\cdot\left(\frac{1.82\cdot|x|}{c} + C_1(U)^{1/2}\right), \tag{96}$$

*for all $1/2 \leqslant c \leqslant 2$ and all $x \in \mathbb{R}$.*

**Proof** Let $K(x)$ be as in the proof of Lemma B.3. From the definition of $K_2(U)$ (see Assumption 2),

$$\begin{aligned}(\mathrm{I}) &\equiv \frac{\mathbb{E}_{\xi,\xi'}[(\xi-\xi')^2(\xi+\xi')^2 U(x+c\xi)U(x+c\xi'); |\xi+\xi'| \leqslant 2^{1/2}\cdot 1.82\cdot K(x)/c]}{\mathbb{E}_{\xi,\xi'}[U(x+c\xi)U(x+c\xi')]} \\ &\leqslant 2K_2(U)\cdot\left(\frac{1.82\cdot K(x)}{c}\right)^2.\end{aligned}$$

If $\xi$ and $\xi'$ are independent standard gaussian random variables, then $\xi-\xi'$ and $\xi+\xi'$ are independent gaussian random variables with mean zero and variance 2. It follows that

$$\mathbb{E}_{\xi,\xi'}\Big[(\xi-\xi')^2(\xi+\xi')^2; |\xi+\xi'| \geqslant \sqrt{2}M\Big] = 4\cdot\mathbb{E}_\xi\Big[|\xi|^2; |\xi| \geqslant M\Big] \overset{(92)}{\leqslant} 4\cdot c_0\frac{\varphi(M/1.05)}{M/1.05}\,. \tag{97}$$

Combining (97) with our earlier bound (91) gives

$$\begin{aligned}(\mathrm{II}) &\equiv \frac{\mathbb{E}_{\xi,\xi'}[(\xi-\xi')^2(\xi+\xi')^2 U(x+c\xi)U(x+c\xi'); |\xi+\xi'| \geqslant 2^{1/2}\cdot 1.82\cdot K(x)/c]}{\mathbb{E}_{\xi,\xi'}[U(x+c\xi)U(x+c\xi')]} \\ &\leqslant 4\cdot c_0\frac{\varphi(1.82\cdot K(x)/(1.05\cdot c))}{1.82\cdot K(x)/(1.05\cdot c)}\cdot\frac{\exp\{(3/2)K(x)^2/c^2\}}{1/(2\bar{c}_1(U))}\end{aligned}$$

(The first inequality above also uses that $U \leqslant 1$, from Assumption 1.) By combining the above bounds for the quantities (I) and (II), and recalling again that $1/2 \leqslant c \leqslant 2$, we obtain

$$\begin{aligned}\operatorname{Var}_{x,c}(Z^2) &= \frac{\mathbb{E}_{\xi,\xi'}[(\xi-\xi')^2(\xi+\xi')^2 U(x+c\xi)U(x+c\xi')]}{2\cdot\mathbb{E}_{\xi,\xi'}U(x+c\xi)U(x+c\xi')} \\ &\leqslant K_2(U)\cdot\left(\frac{1.82\cdot K(x)}{c}\right)^2 + \frac{4\cdot c_0\cdot\bar{c}_1(U)}{1.82/1.05}\cdot\varphi\left(\frac{1.82\cdot K(x)}{1.05\cdot c}\right)\exp\left\{\frac{3K(x)^2}{2c^2}\right\} \\ &\leqslant K_2(U)\cdot\left\{\left(\frac{1.82\cdot|x|}{c}\right)^2 + \left(\frac{1.82\cdot K_0(U)}{1/2}\right)^2\right\} + \frac{4\cdot c_0\cdot\bar{c}_1(U)}{(1.82/1.05)\cdot(2\pi)^{1/2}} \\ &\leqslant K_2(U)\cdot\left\{\left(\frac{1.82\cdot|x|}{c}\right)^2 + 14\cdot K_0(U)^2 + c_0\cdot\bar{c}_1(U)\right\} \\ &\leqslant K_2(U)\cdot\left\{\left(\frac{1.82\cdot|x|}{c}\right)^2 + C_1(U)\right\},\end{aligned}$$

where the second-to-last inequality uses that we took $K_2(U) \geqslant 1$ (see Assumption 2), and the last inequality uses the definition (93) of $C_1(U)$ from the proof of Lemma B.3. This proves (95). Combining with Assumption 2 and the Cauchy–Schwarz inequality gives

$$\begin{aligned}\operatorname{Cov}_{x,c}(Z,Z^2) &\leqslant \left\{\operatorname{Var}_{x,c}(Z)\operatorname{Var}_{x,c}(Z^2)\right\}^{1/2} \leqslant \frac{K_2(U)}{2^{1/2}}\left\{\left(\frac{1.82\cdot|x|}{c}\right)^2 + C_1(U)\right\}^{1/2} \\ &\leqslant \frac{K_2(U)}{2^{1/2}}\left(\frac{1.82\cdot|x|}{c} + C_1(U)^{1/2}\right),\end{aligned}$$

where the last inequality again uses that $K_2(U) \geqslant 1$. This proves (96). ■

**Remark B.5** *We include here an example of a function $U$ that satisfies Assumption 1 but does not satisfy the bound (95) (and hence, by Lemma B.4, must violate Assumption 2). For $k \geqslant 1$ let $b_k \equiv \exp(-100\cdot 4^k)$, and let*

$$A_k(x) \equiv \left(\mathbf{1}\left\{x\in[0,1]\right\} + \mathbf{1}\left\{x\in[2^k-1,2^k]\right\}\right)\frac{b_k}{\varphi(x)} \equiv \frac{b_k f_k(x)}{\varphi(x)}\,.$$

*Then clearly $A_k$ is a nonnegative measurable function supported on $[0,1]\cup[2^k-1,2^k]$, with*

$$\|A_k\|_\infty \leqslant \frac{b_k}{\varphi(2^k)} = b_k(2\pi)^{1/2}\exp\left(\frac{4^k}{2}\right) \leqslant \frac{(2\pi)^{1/2}}{\exp(99\cdot 4^k)}\,.$$

*Let $C$ be a large absolute constant, and define $x_k \equiv C2^k$ and*

$$U(x) \equiv \sum_{k\geqslant 1} A_k(x_k+x)\,.$$

*From the above bound on $\|A_k\|_\infty$ it is clear that $U$ satisfies Assumption 1. Next we note that*

$$\begin{aligned}\frac{\mathbb{E}_\xi[\xi^2 A_k(\xi)]}{b_k} &= \int z^2 f_k(z)\,dz = \frac{1}{3}\left((2^k)^3-(2^k-1)^3+1\right) = 2^{2k}\left(1+\frac{O(1)}{2^k}\right), \\ \frac{\mathbb{E}_\xi[\xi^4 A_k(\xi)]}{b_k} &= \int z^4 f_k(z)\,dz = \frac{1}{5}\left((2^k)^5-(2^k-1)^5+1\right) = 2^{4k}\left(1+\frac{O(1)}{2^k}\right).\end{aligned}$$

*For any $k \geqslant 1$, we have $\mathbb{E}_\xi U(-x_k+\xi) \geqslant \mathbb{E}_\xi A_k(\xi) = 2b_k$. For $\ell \geqslant k+1$ and $0 \leqslant p \leqslant 4$, we have*

$$\frac{\mathbb{E}_\xi[|\xi|^p A_\ell(-x_k+x_\ell+x)]}{b_k} \leqslant \frac{\|A_\ell\|_\infty \mathbb{E}_\xi(\xi^4)}{b_k} \leqslant \frac{3(2\pi)^{1/2}\exp(100\cdot 4^k)}{\exp(99\cdot 4^\ell)}$$
$$\leqslant \frac{3(2\pi)^{1/2}}{\exp(4^k[74\cdot 4^{\ell-k}+(25\cdot 4^{\ell-k}-100)])} \leqslant \frac{3(2\pi)^{1/2}}{\exp(74\cdot 4^\ell)} \leqslant \frac{1}{\exp(70\cdot 4^\ell)}\,.$$

*On the other hand, for $1 \leqslant \ell \leqslant k-1$ and $0 \leqslant p \leqslant 4$, we have (again taking $C$ large enough)*

$$\frac{\mathbb{E}_\xi[|\xi|^p A_\ell(-x_k+x_\ell+x)]}{b_k} \leqslant \frac{\|A_\ell\|_\infty \mathbb{E}_\xi[\xi^4;|\xi| \geqslant C2^k/4]}{b_k} \leqslant \frac{(2\pi)^{1/2}\exp(100\cdot 4^k)}{\exp(99\cdot 4^\ell + C^2 4^k/33)}$$
$$\leqslant \frac{(2\pi)^{1/2}\exp(100\cdot 4^k)}{\exp(99+C^2 4^k/33)} \leqslant \frac{(2\pi)^{1/2}}{\exp(99+C4^k)} \leqslant \frac{1}{\exp(70\cdot 4^k)}\,.$$

*(In the first inequality above, we used that the support of $A_\ell$ is contained in $[0,2^\ell]$.) Altogether we conclude*

$$\frac{\mathbb{E}_\xi[\xi^2 U(-x_k+\xi)]}{\mathbb{E}_\xi U(-x_k+\xi)} = \left(1+\frac{O(1)}{\exp(4^k)}\right)\frac{\mathbb{E}_\xi[\xi^2 A_k(\xi)]}{\mathbb{E}_\xi A_k(\xi)} = \left(1+\frac{O(1)}{\exp(4^k)}\right)\frac{2^{2k}}{2}\,,$$
$$\frac{\mathbb{E}_\xi[\xi^4 U(-x_k+\xi)]}{\mathbb{E}_\xi U(-x_k+\xi)} = \left(1+\frac{O(1)}{\exp(4^k)}\right)\frac{\mathbb{E}_\xi[\xi^4 A_k(\xi)]}{\mathbb{E}_\xi A_k(\xi)} = \left(1+\frac{O(1)}{\exp(4^k)}\right)\frac{2^{4k}}{2}\,.$$

*Recalling the notation of Definition B.1, we obtain*

$$\mathrm{Var}_{-x_k,1}(Z^2) = \left(1+\frac{O(1)}{\exp(4^k)}\right)\left\{\frac{2^{4k}}{2} - \left(\frac{2^{2k}}{2}\right)^2\right\} = \Theta(2^{4k})\,.$$

*Thus shows that $U$ does not satisfy the bound (95), as claimed.*

### B.2. Estimates of the replica symmetric solution

In this subsection we give the proof of Proposition A.1. As a consequence we obtain a rough estimate (Corollary B.8) of the replica symmetric formula which will be used later in our analysis.

**Lemma B.6** *Suppose $U$ satisfies Assumption 1. As in Proposition A.1, let $\bar{q}(\psi) \equiv \mathbb{E}[\mathrm{th}(\psi^{1/2}Z)^2]$. Then*

$$\max\left\{0, 1-4\psi\right\} \leqslant \frac{d\bar{q}}{d\psi} \leqslant 1$$

*for all $\psi \geqslant 0$.*

**Proof** It is clear that $\bar{q}$ is increasing with respect to $\psi \geqslant 0$: indeed,

$$\frac{d\bar{q}}{d\psi} = \mathbb{E}\left[\mathrm{th}(\psi^{1/2}Z)\,\mathrm{th}'(\psi^{1/2}Z)\frac{Z}{\psi^{1/2}}\right] > 0\,,$$

since $\mathrm{th}'(x) > 0$ for all $x \in \mathbb{R}$, and $x\,\mathrm{th}(x) \geqslant 0$ for all $x \in \mathbb{R}$. Integrating by parts gives

$$\frac{d\bar{q}}{d\psi} = \mathbb{E}\left[\left(\mathrm{th}'(\psi^{1/2}Z)\right)^2 + \mathrm{th}(\psi^{1/2}Z)\,\mathrm{th}''(\psi^{1/2}Z)\right]$$
$$= \mathbb{E}\left(1 - 4\,\mathrm{th}(\psi^{1/2}Z)^2 + 3\,\mathrm{th}(\psi^{1/2}Z)^4\right).$$

Note that $x = \operatorname{th}(\psi^{1/2}Z)^2 \in [0,1]$ almost surely, and $1 - 4x \leqslant 1 - 4x + 3x^2 \leqslant 1$ for all $x \in [0,1]$, so

$$1 \geqslant \frac{d\bar{q}}{d\psi} \geqslant \mathbb{E}\Big(1 - 4\operatorname{th}(\psi^{1/2}Z)^2\Big) \geqslant 1 - 4\psi \cdot \mathbb{E}(Z^2) = 1 - 4\psi\,,$$

for all $\psi \geqslant 0$. ■

**Lemma B.7** *Suppose $U$ satisfies Assumption 1. As in Proposition A.1, let $\bar{r}(q) \equiv \mathbb{E}[F_q(q^{1/2}Z)^2]$. Then*

$$\sup\left\{\left|\frac{d\bar{r}}{dq}\right| : 0 \leqslant q \leqslant \frac{1}{2}\right\} \leqslant c_1 \cdot C_1(U)^6\,,$$

*where $c_1 \geqslant 1$ is an absolute constant while $C_1(U)$ is the constant from Lemma B.3.*

**Proof** For convenience we shall rewrite (8) as

$$F_q(x) = \frac{\mathbb{E}_\xi U'(x + (1-q)^{1/2}\xi)}{\mathbb{E}_\xi U(x + (1-q)^{1/2}\xi)}\,. \tag{98}$$

Note that the above makes sense for any $U$ satisfying Assumption 1, without any smoothness assumption, since $U'$ can be interpreted as a distributional derivative (as in e.g. (Lieb and Loss, 2001, Ch. 6)). Similarly one can make sense of the distributional derivative $U^{(k)}$ for any integer $k \geqslant 1$. We can then calculate

$$\frac{d\bar{r}}{dq} = \mathbb{E}\left[2F_q(q^{1/2}Z)\frac{d[F_q(q^{1/2}Z)]}{dq}\right] = \text{(I)} - \text{(II)}$$

where, abbreviating $U^{(k)} \equiv U^{(k)}(q^{1/2}Z + (1-q)^{1/2}\xi)$, we have

$$\begin{aligned}
\text{(I)} &= \mathbb{E}\left[\frac{Z}{q^{1/2}}F_q(q^{1/2}Z)\cdot(F_q)'(q^{1/2}Z)\right] = \mathbb{E}\left[F_q(q^{1/2}Z)\cdot(F_q)''(q^{1/2}Z) + \Big((F_q)'(q^{1/2}Z)\Big)^2\right],\\
\text{(II)} &= \mathbb{E}\left[\frac{F_q(q^{1/2}Z)}{(1-q)^{1/2}}\left(\frac{\mathbb{E}_\xi(\xi U'')}{\mathbb{E}_\xi U} - \frac{(\mathbb{E}_\xi U')\mathbb{E}_\xi(\xi U')}{(\mathbb{E}_\xi U)^2}\right)\right].
\end{aligned}$$

It follows by repeated applications of the inequality $2ab \leqslant a^2 + b^2$ that

$$\left|\frac{d\bar{r}}{dq}\right| \leqslant C \sum_{0 \leqslant k,p \leqslant 3} \mathbb{E}\left(\frac{\mathbb{E}_\xi[|\xi|^k U(q^{1/2}Z + (1-q)^{1/2}\xi)]}{\mathbb{E}_\xi U(q^{1/2}Z + (1-q)^{1/2}\xi)}\right)^{2p}$$

for all $0 \leqslant q \leqslant 1/2$, where $C$ is an absolute constant. It then follows from Lemma B.3 that

$$\left|\frac{d\bar{r}}{dq}\right| \leqslant C \sum_{0 \leqslant k,p \leqslant 3} \mathbb{E}\left[\Big((4q^{1/2}|Z|)^k + C_1(U)\Big)^{2p}\right] \leqslant c_1 \cdot C_1(U)^6$$

for all $0 \leqslant q \leqslant 1/2$, where $c_1 \geqslant 1$ is an absolute constant. ■

**Proof** [Proof of Proposition A.1] We seek a value $q \in [0, 1/25]$ that satisfies the fixed-point equation (9), i.e., $q = \bar{q}(\alpha\bar{r}(q))$. This is the same as a root $q \in [0, 1/25]$ of the function

$$\bar{g}(q) = \frac{\bar{q}^{-1}(q)}{\alpha} - \bar{r}(q)\,. \tag{99}$$

Note that $\bar{q}(0) = 0$, and it follows from Lemma B.6 that $\bar{q}'(\psi) \in [4/5, 1]$ for all $\psi \leqslant 1/20$, so

$$\frac{4}{5}\psi \leqslant \bar{q}(\psi) \leqslant \psi$$

for all $\psi \leqslant 1/20$. Consequently, if $\bar{q}(\psi) \leqslant 1/25$ then we must have $\psi \leqslant 1/20$, that is to say,

$$\sup\left\{(\bar{q})^{-1}(q) : q \leqslant \frac{1}{25}\right\} \leqslant \frac{1}{20}\,.$$

It follows from Lemma B.6 that $(\bar{q}^{-1})'(q) \in [1, 5/4]$ for all $q \leqslant 1/25$. Combining with Lemma B.7 gives

$$\frac{1}{\alpha} - c_1 \cdot C_1(U)^6 \leqslant \frac{d\bar{g}}{dq} \leqslant \frac{5}{4\alpha} + c_1 \cdot C_1(U)^6\,,$$

where $c_1$ is the absolute constant from Lemma B.7. It follows that as long as $\alpha \leqslant \alpha(U)$ as defined by (27), then for all $0 \leqslant q \leqslant 1/25$ we will have

$$\frac{1}{2\alpha} \leqslant \frac{d\bar{g}}{dq} \leqslant \frac{2}{\alpha}\,.$$

At $q = 0$ we have $\bar{g}(0) = -\bar{r}(0)$, and it follows by Assumption 1 combined with Lemma B.3 that

$$\Big(\mathbb{E}_\xi[\xi U(\xi)]\Big)^2 \leqslant \bar{r}(0) = \left(\frac{\mathbb{E}_\xi U'(\xi)}{\mathbb{E}_\xi U(\xi)}\right)^2 = \left(\frac{\mathbb{E}_\xi[\xi U(\xi)]}{\mathbb{E}_\xi U(\xi)}\right)^2 \leqslant C_1(U)^2\,.$$

It follows that on the interval $0 \leqslant q \leqslant 1/25$, the function $\bar{g}$ has a unique root $q$, which must satisfy

$$\frac{(\mathbb{E}_\xi[\xi U(\xi)])^2}{2} \leqslant \frac{q}{\alpha} \leqslant 2C_1(U)^2\,.$$

It follows from the earlier bound on $\psi$ that

$$\frac{(\mathbb{E}_\xi[\xi U(\xi)])^2}{2} \leqslant \frac{q}{\alpha} \leqslant \frac{\psi}{\alpha} \leqslant \frac{5q}{4\alpha} \leqslant \frac{5C_1(U)^2}{2}\,,$$

so this concludes the proof. ■

**Corollary B.8** *If the function $U$ satisfies Assumptions 1 and 2, then for all $0 < \alpha \leqslant \alpha(U)$ we have*

$$\frac{\mathrm{RS}(\alpha; U)}{\alpha} \geqslant \frac{\mathrm{ann}(\alpha; U)}{\alpha} - 1.51 \cdot C_1(U)^2 \geqslant \frac{\log 2}{\alpha} - 1.53 \cdot C_1(U)^2\,,$$

*where $C_1(U)$ is the constant from Lemma B.3, and $\alpha(U)$ is given by (27).*

**Proof** Let $(q, \psi)$ be the solution from Proposition A.1, and recall from (29) that

$$\mathrm{RS}(\alpha; U) - \log 2 = -\frac{\psi(1-q)}{2} + \mathbb{E}\Big\{\log\mathrm{ch}(\psi^{1/2}Z) + \alpha L_q(q^{1/2}Z)\Big\}\,.$$

We hereafter abbreviate

$$\bar{\ell}(q) \equiv \mathbb{E}L_q(q^{1/2}Z) = \mathbb{E}\bigg[\log \mathbb{E}_\xi U\Big(q^{1/2}Z + (1-q)^{1/2}\xi\Big)\bigg].$$

Since $\operatorname{ch}(x) \geqslant 1$ for all $x \in \mathbb{R}$, we can lower bound

$$\mathrm{RS}(\alpha; U) - \log 2 \geqslant -\frac{\psi}{2} + \alpha\mathbb{E}L_q(q^{1/2}Z) \geqslant -\frac{\psi}{2} + \alpha\bigg\{\bar{\ell}(0) - q \sup_{0\leqslant q\leqslant 1/2}\bigg|\frac{d\bar{\ell}}{dq}\bigg|\bigg\}.$$

Similarly as in the proof of Lemma B.7, we can bound

$$\bigg|\frac{d\bar{\ell}}{dq}\bigg| \leqslant C \sum_{0\leqslant k,p\leqslant 2} \mathbb{E}\bigg[\bigg(\frac{\mathbb{E}_\xi[|\xi|^k U(q^{1/2}Z + (1-q)^{1/2}\xi)]}{\mathbb{E}_\xi U(q^{1/2}Z + (1-q)^{1/2}\xi)}\bigg)^p\bigg] \leqslant c_1 \cdot C_1(U)^2 \tag{100}$$

for all $0 \leqslant q \leqslant 1/2$, where $c_1$ is an absolute constant (and can be arranged to be the same as the $c_1$ from Lemma B.7). By combining the above bounds we conclude

$$\begin{aligned}\frac{\mathrm{RS}(\alpha; U) - (\log 2 + \alpha\bar{\ell}(0))}{\alpha} &\geqslant -\frac{\psi}{2\alpha} - q \sup_{0\leqslant q\leqslant 1/2}\bigg|\frac{d\bar{\ell}}{dq}\bigg| \overset{(100)}{\geqslant} -\frac{\psi}{2\alpha} - q\cdot c_1 \cdot C_1(U)^2 \\ &\overset{(28)}{\geqslant} -3C_1(U)^2\bigg(\frac{1}{2} + c_1\cdot C_1(U)^2\alpha\bigg) \\ &\overset{(27)}{\geqslant} -3C_1(U)^2\bigg(\frac{1}{2} + \frac{1}{e^{10}C_1(U)^4 K_2(U)^4}\bigg) \geqslant -1.51\cdot C_1(U)^2,\end{aligned}$$

where the last bound uses that we chose $C_1(U) \geqslant 10$ in the proof of Lemma B.3. Then, recalling (5), we have

$$\mathrm{ann}(\alpha; U) - \log 2 = \alpha\bar{\ell}(0) = -\alpha\log\frac{1}{\mathbb{E}U(Z)} \overset{(90)}{\geqslant} -\alpha\log\bar{c}_1(U) \geqslant -\alpha\bar{c}_1(U) \geqslant -\frac{\alpha C_1(U)^2}{50},$$

using that we also chose $C_1(U) \geqslant 5\cdot\bar{c}_1(U) \geqslant 10$ in the proof of Lemma B.3. The claim follows. ■

**Lemma B.9** *Suppose $U$ satisfies Assumptions 1 and 2, and let $U_\eta = U * \varphi_\eta$ as in (21). Then, using the notation of Assumption 2, we will have $K_2(U_\eta) \leqslant 4K_{2,\wr}(U)$ for all $\eta \leqslant 1$.*

**Proof** Let $\xi, \xi'$ be i.i.d. standard gaussian random variables. We need to bound the quantity

$$\frac{\mathbb{E}_{\xi,\xi'}[(\xi-\xi')^2 U_\eta(x+c\xi)U_\eta(x+c\xi')]}{\mathbb{E}_{\xi,\xi'}[U_\eta(x+c\xi)U_\eta(x+c\xi')]} \equiv \frac{N_\eta(x,c)}{D_\eta(x,c)}. \tag{101}$$

Let $\zeta, \zeta'$ be independent copies of $\xi, \xi'$, and note that

$$N_\eta(x,c) = \mathbb{E}_{\xi,\xi',\zeta,\zeta'}\bigg[(\xi-\xi')^2 U(x+c\xi+\eta\zeta)U(x+c\xi'+\eta\zeta')\bigg].$$

Taking an orthogonal transformation of $(\xi, \zeta)$ gives another pair of i.i.d. standard gaussians,

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \frac{1}{(c^2+\eta^2)^{1/2}}\begin{pmatrix} c & \eta \\ -\eta & c \end{pmatrix}\begin{pmatrix} \xi \\ \zeta \end{pmatrix}.$$

Likewise we like $(X', Y')$ be the pair obtained by the same transformation applied to $(\xi', \zeta')$. Then note that

$$(\xi - \xi')^2 = \left( \frac{c(X - X') - \eta(Y - Y')}{(c^2 + \eta^2)^{1/2}} \right)^2 \leqslant 2 \cdot \frac{c^2(X - X')^2 + \eta^2(Y - Y')^2}{c^2 + \eta^2} .$$

Rewriting $N_\eta(x, c)$ in terms of the random variables $X, X', Y, Y'$ gives

$$\begin{aligned} N_\eta(x, c) &\leqslant 2 \cdot \mathbb{E}_{X,X',Y,Y'} \Bigg[ \left( \frac{c^2(X - X')^2 + \eta^2(Y - Y')^2}{c^2 + \eta^2} \right) \\ &\qquad\qquad \times U(x + (c^2 + \eta^2)^{1/2} X) U(x + (c^2 + \eta^2)^{1/2} X') \Bigg] \\ &= \frac{2c^2}{c^2 + \eta^2} N_0(x, (c^2 + \eta^2)^{1/2}) + \frac{4\eta^2}{c^2 + \eta^2} D_0(x, (c^2 + \eta^2)^{1/2}) , \end{aligned}$$

where $N_0$ and $D_0$ are as in (101) but with $U$ in place of $U_\eta$. If $1/2 \leqslant c \leqslant 2$ and $\eta \leqslant 1$, then $1/2 \leqslant (c^2 + \eta^2)^{1/2} \leqslant 7/3$, so Assumption 2 will give

$$N_\eta(x, c) \leqslant \left( \frac{2c^2}{c^2 + \eta^2} K_{2,\wr}(U) + \frac{4\eta^2}{c^2 + \eta^2} \right) D_0(x, (c^2 + \eta^2)^{1/2}) \leqslant 4 K_{2,\wr}(U) D_\eta(x, c) .$$

The claim follows. ■

**Proof** [Proof of Proposition 1.8] Recall from Lemma B.3 the constants $C_1(U)$ and $(C_1)^\wr(U)$: they depend on the absolute constant $c_0$, as well as the constants $\bar{c}_1(U)$ and $(\bar{c}_1)^\wr(U)$ defined by (90) and (94). Let $\xi, \zeta$ be i.i.d. standard gaussians, and note

$$\mathbb{E}_\xi U_\eta(c\xi) = \mathbb{E}_{\xi,\zeta} U\Big(c\xi + \eta\zeta\Big) = \mathbb{E}_\xi U\Big((c^2 + \eta^2)^{1/2} \xi\Big) .$$

It follows from this that in the limit $\eta \downarrow 0$, we have $\bar{c}_1(U_\eta)$ asymptotically upper bounded by $(\bar{c}_1)^\wr(U)$. Next recall from Lemma B.9 that if $\eta \leqslant 1$ then we have $K_2(U_\eta) \leqslant 4K_{2,\wr}(U)$. Consequently, recalling (27) and (31), we have

$$\alpha(U_\eta) \overset{(27)}{\equiv} \frac{1}{e^{10} \cdot c_1 \cdot C_1(U_\eta)^6 \cdot K_2(U_\eta)^4} \geqslant \frac{1}{e^{16} \cdot c_1 \cdot (C_1)^\wr(U)^6 \cdot K_{2,\wr}(U)^4} \overset{(31)}{=} \alpha_\wr(U) . \tag{102}$$

This shows that for all $0 < \alpha \leqslant \alpha_\wr(U)$, we also have $\alpha \leqslant \alpha(U_\eta)$ for all $\eta$ small enough, which means that the results of Proposition A.1 apply for $U_\eta$ as well as for $U$. We see from the proof of Proposition A.1 that the replica symmetric fixed point $q_\eta$ for $U_\eta$ is a root $q_\eta \in [0, 1/25]$ of the function (cf. (99))

$$\bar{g}_\eta(q) = \frac{\bar{q}^{-1}(q)}{\alpha} - \bar{r}_\eta(q) ,$$

where $\bar{r}_\eta$ is defined as in (9) but with $U_\eta$ in place of $U$:

$$\bar{r}_\eta(q) = \frac{1}{(1 - q)} \mathbb{E}\left[ \left( \frac{\mathbb{E}_\xi[\xi U_\eta(Z + (1 - q)^{1/}\xi)]}{\mathbb{E}_\xi U_\eta(Z + (1 - q)^{1/}\xi)} \right)^2 \right] .$$

It is clear that $\bar{g}_\eta$ converges uniformly to $\bar{g}$ over $0 \leqslant q \leqslant 1/25$, so $q_\eta$ converges to $q$, and consequently $\psi_\eta$ converges to $\psi$. It is then straightforward to deduce from the formula (29) that $\mathrm{RS}(\alpha; U_\eta)$ converges to $\mathrm{RS}(\alpha; U)$ as $\eta \downarrow 0$. ■

### B.3. Almeida–Thouless condition

Recall from Definition A.2 the state evolution recursions.

**Lemma B.10** *Suppose $U$ satisfies Assumption 1. The recursions of Definition A.2 are well-defined: the recursions (33) lead to $|\rho_s| \leqslant 1$ and $|\mu_s| \leqslant 1$ for all $s \geqslant 1$, and the recursions (34) leads to $\Lambda_s \in [0,1)$ and $\Gamma_s \in [0,1)$ for all $s \geqslant 0$.*

**Proof** We abbreviate $F \equiv F_q$ throughout this proof. We have $\rho_1 \equiv \lambda_1$ and $\mu_1 \equiv \gamma_1$ as in (32), and it follows that

$$0 \leqslant (\rho_1)^2 = (\lambda_1)^2 \leqslant \frac{1}{q}\mathbb{E}\Big[\operatorname{th}(\psi^{1/2}Z)^2\Big] \overset{(9)}{=} 1\,,$$

and likewise $0 \leqslant (\mu_1)^2 = (\gamma_1)^2 \leqslant 1$. Then for $s \geqslant 1$ we have $\rho_{s+1}$ and $\mu_{s+1}$ defined by (33), and it follows by the Cauchy–Schwarz inequality that

$$|\rho_{s+1}| \leqslant \frac{\mathbb{E}[\operatorname{th}(\psi^{1/2}Z)^2]}{q} \overset{(9)}{=} 1\,, \quad |\mu_{s+1}| \leqslant \frac{\alpha\mathbb{E}[F(q^{1/2}Z)^2]}{\psi} \overset{(9)}{=} 1\,.$$

Thus $|\rho_s| \leqslant 1$ and $|\mu_s| \leqslant 1$ for all $s \geqslant 1$, which confirms that the recursions (33) are well-defined.

It remains to verify that the quantities $\Lambda_{s-1}$ and $\Gamma_{s-1}$ from (35) are *strictly* smaller than 1 for all $s \geqslant 1$. The claim holds trivially in the base case $s = 0$, since clearly $\Lambda_0 = \Gamma_0 = 0$. We therefore suppose inductively that we have $\Lambda_{s-1} < 1$ and $\Gamma_{s-1} < 1$. This means that the quantities $\lambda_s$ and $\gamma_s$ are well-defined by the recursions (34). Denote $M_1 \equiv q^{1/2}$ and $N_1 \equiv (\psi/\alpha)^{1/2}$. Next let $Y_i, X_j$ be a collection of i.i.d. standard gaussian random variables, and let

$$\begin{aligned} M_{i+1} &\equiv \operatorname{th}\bigg(\psi^{1/2}\Big\{\gamma_1 Y_1 + \ldots + \gamma_{i-1}Y_{i-1} + (1-\Gamma_{i-1})^{1/2}Y_i\Big\}\bigg) \\ N_{j+1} &\equiv F\bigg(q^{1/2}\Big\{\lambda_1 X_1 + \ldots + \lambda_{j-1}X_{j-1} + (1-\Lambda_{i-1})^{1/2}X_j\Big\}\bigg) \end{aligned}$$

(cf. (253) and (254)). This gives well-defined random variables $M_k, N_k$ for all $1 \leqslant k \leqslant s+1$, with $\mathbb{E}[(M_k)^2] = q$ and $\mathbb{E}[(N_k)^2] = \psi/\alpha$. If $2 \leqslant k < \ell \leqslant s+1$, then

$$\frac{\mathbb{E}(M_k M_\ell)}{q} = \rho\bigg((\gamma_1)^2 + \ldots + (\gamma_{k-2})^2 + \gamma_{k-1}(1-\Gamma_{k-2})^{1/2}\bigg) \overset{(34)}{=} \rho(\mu_{k-1}) \overset{(33)}{=} \rho_k\,, \tag{103}$$

$$\frac{\mathbb{E}(N_k N_\ell)}{\psi/\alpha} = \mu\bigg((\lambda_1)^2 + \ldots + (\lambda_{k-2})^2 + \lambda_{k-1}(1-\Lambda_{k-2})^{1/2}\bigg) \overset{(34)}{=} \mu(\rho_{k-1}) \overset{(33)}{=} \mu_k\,. \tag{104}$$

(cf. (41) and (42)). Now let $R_i, C_i$ ($i \geqslant 1$) be the Gram–Schmidt orthogonalization of the random variables $M_i, N_i$:

$$R_{i+1} = \frac{1}{r_{i+1}}\bigg\{M_{i+1} - \sum_{j\leqslant i}\mathbb{E}(M_{i+1}R_j)R_j\bigg\}\,, \tag{105}$$

$$C_{i+1} = \frac{1}{c_{i+1}}\bigg\{N_{i+1} - \sum_{j\leqslant i}\mathbb{E}(N_{i+1}C_j)C_j\bigg\} \tag{106}$$

where $r_{i+1}$ and $c_{i+1}$ are the normalizing constants such that $\mathbb{E}[(R_{i+1})^2] = 1$ and $\mathbb{E}[(C_{i+1})^2] = 1$. To see that $r_{s+1}$ is a well-defined positive number, we apply the inductive hypothesis $\Gamma_{s-1} < 1$:

then follows from the above definition (together with the fact that $\mathrm{th}$ is a non-constant function) that $M_{s+1}$ depends non-trivially on $Y_s$. On the other hand, the random variables $R_j$ for $j \leqslant s$ can depend only on $Y_1, \ldots, Y_{s-1}$. It follows that the random variable

$$M_{s+1} - \sum_{j \leqslant s} \mathbb{E}(M_{s+1} R_j) R_j$$

has strictly positive variance, so $r_{s+1}$ is well-defined and positive. Likewise, using the inductive hypothesis $\Lambda_{s-1} < 1$ together with the fact that $F$ is non-constant, we deduce that $c_{s+1}$ is also well-defined and positive. Next, since we see from above that the quantities $\mathbb{E}(M_k M_\ell)$ and $\mathbb{E}(N_k N_\ell)$ depend only on $\min\{k, \ell\}$, it follows that there is a value $l_j$ such that $\mathbb{E}(M_{i+1} R_j) = q^{1/2} l_j$ for all $i \geqslant j$, and likewise there is a value $y_j$ such that $\mathbb{E}(N_{i+1} C_j) = (\psi/\alpha)^{1/2} y_j$ for all $i \geqslant j$. As in (35), let us abbreviate

$$L_i \equiv \sum_{j \leqslant i} (l_j)^2 \,, \quad Y_i \equiv \sum_{j \leqslant i} (y_j)^2 \,.$$

It follows by the above calculations that

$$\begin{aligned} l_{i+1} &= \frac{\mathbb{E}(M_{i+2} R_{i+1})}{q^{1/2}} \overset{(105)}{=} \frac{q^{1/2}}{r_{i+1}} \left\{ \frac{\mathbb{E}(M_{i+2} M_{i+1})}{q} - \sum_{j \leqslant i} (l_j)^2 \right\} \overset{(103)}{=} \frac{\rho_{i+1} - L_i}{(1 - L_i)^{1/2}} \,, \\ y_{i+1} &= \frac{\mathbb{E}(N_{i+2} C_{i+1})}{(\psi/\alpha)^{1/2}} \overset{(106)}{=} \frac{(\psi/\alpha)^{1/2}}{r_{i+1}} \left\{ \frac{\mathbb{E}(N_{i+2} N_{i+1})}{\psi/\alpha} - \sum_{j \leqslant i} (y_j)^2 \right\} \overset{(104)}{=} \frac{\mu_{i+1} - Y_i}{(1 - Y_i)^{1/2}} \,. \end{aligned}$$

Recalling that $r_{i+1}$ and $c_{i+1}$ are positive for all $i \leqslant s$, we deduce

$$0 < \frac{r_{i+1}}{q^{1/2}} = \frac{1}{q^{1/2}} \mathbb{E}\left[ \left( M_{i+1} - \sum_{j \leqslant i} \mathbb{E}(M_{i+1} R_j) R_j \right)^2 \right]^{1/2} = (1 - L_i)^{1/2} \,,$$

and similarly $0 < (1 - Y_i)^{1/2}$, which implies $L_i, Y_i \in [0, 1)$. We see moreover that the sequences $l_i, m_i$ satisfy the same recursions (34) as the sequences $\lambda_i, \mu_i$, which implies $l_i = \lambda_i$ and $m_i = \mu_i$ for all $i \geqslant 1$. This proves that $\Lambda_i = L_i$ and $\Gamma_i = Y_i$ both lie in $[0, 1)$ for all $i \geqslant 1$. Therefore the recursions (34) give well-defined quantities $\lambda_s$ and $\gamma_s$ for all $s \geqslant 1$, as desired. ■

**Lemma B.11 (Almeida–Thouless condition)** *Suppose $U$ satisfies Assumption 1, and moreover that*

$$\mathrm{AT}(\alpha; U) \equiv \alpha \cdot \left\{ \mathbb{E}\Big( (F_q)'(q^{1/2} Z)^2 \Big) \right\} \left\{ \mathbb{E}\Big( \mathrm{th}'(\psi^{1/2} Z)^2 \Big) \right\} \leqslant 1 \,. \tag{107}$$

*In this case, the recursions of Definition A.2 lead to $\Gamma_s \to 1$ and $\Lambda_s \to 1$ as $s \to \infty$.*

**Proof** We begin with a general observation. Let $Z, \xi, \xi'$ be i.i.d. standard gaussians. Suppose $f : \mathbb{R} \to \mathbb{R}$ is any function with at most polynomial growth, and consider the function

$$r_f(t) \equiv \mathbb{E}\left[ f\Big( t^{1/2} Z + (1 - t)^{1/2} \xi \Big) f\Big( t^{1/2} Z + (1 - t)^{1/2} \xi' \Big) \right] ,$$

which is defined for $0 \leqslant t \leqslant 1$. Write $Z(t) \equiv t^{1/2} Z + (1-t)^{1/2}\xi$, and note that

$$r_f(t) = \mathbb{E}\bigg[\Big(\mathbb{E}_\xi f\Big(t^{1/2}Z + (1-t)^{1/2}\xi\Big)\Big)^2\bigg] = \mathbb{E}\bigg[\Big(\mathbb{E}_\xi f(Z(t))\Big)^2\bigg] \geqslant 0\,.$$

Next we differentiate with respect to $t$ and apply gaussian integration by parts to obtain

$$\begin{aligned}(r_f)'(t) &= \mathbb{E}\bigg\{\Big(\mathbb{E}_\xi f(Z(t))\Big)\mathbb{E}_\xi\bigg[f'(Z(t))\bigg(\frac{Z}{t^{1/2}} - \frac{\xi}{(1-t)^{1/2}}\bigg)\bigg]\bigg\}\\ &= \mathbb{E}\bigg[\Big(\mathbb{E}_\xi f'(Z(t))\Big)^2\bigg] = r_{f'}(t) \geqslant 0\,.\end{aligned}$$

It follows moreover that $(r_f)''(t) = (r_{f'})'(t) = r_{f''}(t) \geqslant 0$ for all $0 \leqslant t \leqslant 1$, so $r_f$ is convex.

Now, returning to the state evolution recursions from Definition A.2, we will consider $r_S$ and $r_T$ for

$$S(x) \equiv \left(\frac{\alpha}{\psi}\right)^{1/2} F(q^{1/2}x)\,, \quad T(x) \equiv \left(\frac{1}{q}\right)^{1/2} \operatorname{th}(\psi^{1/2}x)\,.$$

Denote $r_{ST} \equiv r_S \circ r_T$. Note that the fixed point equation (9) implies $r_S(1) = 1$ and $r_T(1) = 1$, so $r_{ST}(1) = 1$. We also have from (32) that $r_S(0) = \mu_1$, while $r_T(0) = \rho_1 = 0$; so if $\mu_1 = 0$ then $r_{ST}(0) = 0$. However, the condition (107) is equivalent to $(r_{ST})'(1) < 1$, which implies $(r_{ST})'(t) < 1$ for all $t \in [0,1]$, and consequently

$$1 - r_{ST}(0) = r_{ST}(1) - r_{ST}(0) = \int_0^1 (r_{ST})'(t)\,dt \leqslant (r_{ST})'(1) < 1\,.$$

This shows that if $(r_{ST})'(1) < 1$ then we must have $r_{ST}(0) = r_S(0) = (\mu_1)^2 > 0$.

Next we argue that $\rho_2 \neq 0$. To this end, for the function $T$ we can directly calculate that for all $0 \leqslant t \leqslant 1$,

$$(r_T)'(t) = r_{T'}(t) \geqslant r_{T'}(0) = \Big(\mathbb{E}T'(Z)\Big)^2 = \frac{\psi}{q}\Big(\mathbb{E}\operatorname{th}'(\psi^{1/2}Z)\Big)^2 \overset{(9)}{=} \frac{\psi(1-q)^2}{q} > 0\,,$$

so $r_T(t)$ is strictly increasing. Thus, in the case $\mu_1 > 0$ we obtain

$$\rho_2 \overset{(33)}{=} \rho(\mu_1) = r_T(\mu_1) > r_T(0) = 0\,.$$

Since $T$ is an odd function, in the case $\mu_1 < 0$ we obtain

$$\rho_2 \overset{(33)}{=} \rho(\mu_1) = -r_T(-\mu_1) < -r_T(0) = 0\,.$$

In both cases we obtain $\rho_2 \neq 0$ as claimed.

To conclude, note that Lemma B.10 implies that $\Lambda_s \uparrow \Lambda_\infty \leqslant 1$ and $\Gamma_s \uparrow \Gamma_\infty \leqslant 1$ as $s \to \infty$. If $(r_{ST})'(1) < 1$, the above considerations give $(\Gamma_\infty)^2 \geqslant (\gamma_1)^2 = (\mu_1)^2 > 0$, as well as

$$(\Lambda_\infty)^2 \geqslant (\lambda_2)^2 \overset{(34)}{=} \left(\frac{\rho_2 - \Lambda_1}{(1-\Lambda_1)^{1/2}}\right)^2 \overset{(32)}{=} (\rho_2)^2 > 0\,.$$

Clearly we must also have $\lambda_s \to 0$ and $\gamma_s \to 0$ as $s \to \infty$, so

$$\begin{pmatrix}\rho_s\\ \mu_s\end{pmatrix} \overset{(34)}{=} \begin{pmatrix}\Lambda_{s-1} + \lambda_s(1-\Lambda_{s-1})^{1/2}\\ \Gamma_{s-1} + \gamma_s(1-\Gamma_{s-1})^{1/2}\end{pmatrix} \xrightarrow{s\to\infty} \begin{pmatrix}\Lambda_\infty\\ \Gamma_\infty\end{pmatrix} > \begin{pmatrix}0\\ 0\end{pmatrix}.$$

Thus, for $s$ large enough, we can express

$$\mu_{s+1} \overset{(33)}{=} \mu(\rho_s) \overset{(33)}{=} \mu(\rho(\mu_{s-1}) = r_{ST}(\mu_{s-1}).$$

which shows that $\Gamma_\infty$ must be a fixed point of $r_{ST}$, and $\Lambda_\infty = r_T(\Gamma_\infty)$. Since we saw above that $r_{ST}(t)$ is convex on the interval $0 \leqslant t \leqslant 1$, if $(r_{ST})'(1) \leqslant 1$ then the only fixed point of $r_{ST}(t)$ on the interval $0 \leqslant t \leqslant 1$ occurs at $t = 1$, and thus we obtain $\Lambda_\infty = \Gamma_\infty = 1$. ■

### B.4. Logconcavity

In this subsection we review the proof of Proposition 1.3 which follows from well-known results on logconcave measures. We then state and prove Lemmas B.14 and B.15, which give some further consequences of Assumption 2. We also present the proof of Proposition A.6.

**Theorem B.12 ((Maurey, 1991))** *Suppose $U$ satisfies Assumption 1 and is logconcave. Recall that $\varphi$ denotes the standard gaussian density on $\mathbb{R}$, and let $\mu$ be the probability measure on $\mathbb{R}$ whose density (with respect to Lebesgue measure) is*

$$\frac{d\mu}{dz} = \frac{U(z)\varphi(z)}{\mathbb{E}_\xi U(\xi)}.$$

*Then for any measurable subset $B \subseteq \mathbb{R}$ we have the concentration bound*

$$\int \exp\left(\frac{d(z,B)^2}{4}\right) d\mu(z) \leqslant \frac{1}{\mu(B)},$$

*where $d(z, B)$ denotes the minimum distance from $z$ to $B$.*

Theorem B.12 is obtained as a consequence of the Prékopa–Leindler inequality (or functional Brunn–Minkowski inequality) (Prékopa, 1971, 1973; Leindler, 1972) from convex geometry; see also Bobkov and Ledoux (2000) and Talagrand (2011a, Thm. 3.1.4). In this paper we use Theorem B.12 only in the proof of Proposition 1.3, which is not needed for the main result Theorem 1.1. See §1.2.2 for a discussion of results on the positive spherical perceptron which use convex geometry in more essential ways. By well-known arguments, Theorem B.12 can be used to deduce the following:

**Theorem B.13 (see e.g. (Talagrand, 2011a, Thm. 3.1.4))** *In the same setting as Theorem B.12, if $f : \mathbb{R} \to \mathbb{R}$ is Lipschitz, then*

$$\int \frac{(f(y) - f(z))^{2k}}{(16k)^k} d\mu(y)\, d\mu(z) \leqslant \int \exp\left\{\frac{(f(y) - f(z))^2}{16}\right\} d\mu(y)\, d\mu(z) \leqslant 4$$

*for any integer $k \geqslant 1$.*

Note that the concentration bounds from Theorems B.12 and B.13 rely on the strong logconcavity of the gaussian density $\varphi(x)$, and the bounds hold uniformly over all logconcave functions $U$. As a consequence we obtain:

**Proof** [Proof of Proposition 1.3] Suppose $U$ satisfies Assumption 1. If $U$ is bounded away from zero or compactly supported, then Assumption 2 holds by trivial calculations. In the case that $U$ is logconcave, Assumption 2 follows from the above result Theorem B.13. ■

**Lemma B.14** *If $U$ satisfies Assumption 1 and 2, then the function $F_q$ of (8) satisfies*

$$\|(F_q)'\|_\infty \leqslant \frac{1}{1-q}\left(\frac{K_2(U)}{2}+1\right).$$

*Therefore $F_q$ is Lipschitz for any $q \in [0,1)$.*

**Proof** From (8) and (98) we calculate

$$(F_q)'(x) = \frac{\mathbb{E}_\xi U''(x+(1-q)^{1/2}\xi)}{\mathbb{E}_\xi U(x+(1-q)^{1/2}\xi)} - \left(\frac{\mathbb{E}_\xi U'(x+(1-q)^{1/2}\xi)}{\mathbb{E}_\xi U(x+(1-q)^{1/2}\xi)}\right)^2. \tag{108}$$

Applying gaussian integration by parts gives

$$\begin{aligned}(F_q)'(x) &= \frac{1}{1-q}\left\{\frac{\mathbb{E}_\xi[(\xi^2-1)U(x+(1-q)^{1/2}\xi)]}{\mathbb{E}_\xi U(x+(1-q)^{1/2}\xi)} - \left(\frac{\mathbb{E}_\xi[\xi U(x+(1-q)^{1/2}\xi)]}{\mathbb{E}_\xi U(x+(1-q)^{1/2}\xi)}\right)\right\}\\ &= \frac{1}{1-q}\left\{\frac{1}{2}\frac{\mathbb{E}_{\xi,\xi'}[(\xi-\xi')^2U(x+c\xi)U(x+c\xi')]}{\mathbb{E}_{\xi,\xi'}[U(x+c\xi)U(x+c\xi')]} - 1\right\}.\end{aligned}$$

The result follows from Assumption 2. ■

**Proof** [Proof of Proposition A.6] In view of Lemma B.11, it suffices to check that the condition (107) holds for $0 < \alpha \leqslant \alpha(U)$. By Lemma B.14 and the fact that $\mathrm{th}'(x) \in (0,1)$ for all $x \in \mathbb{R}$, we can bound

$$\begin{aligned}\mathrm{AT}(\alpha;U) &\leqslant \frac{\alpha}{(1-q)^2}\left(\frac{K_2(U)}{2}+1\right)^2 \leqslant \frac{(3/2)^2\cdot K_2(U)^2\cdot\alpha}{(1-q)^2} \overset{(28)}{\leqslant} 3\cdot K_2(U)^2\cdot\alpha\\ &\overset{(27)}{\leqslant} \frac{3}{e^{10}C_1(U)^6K_2(U)^2} < 1,\end{aligned}$$

having used that $C_1(U) \geqslant 10$ and $K_2(U) \geqslant 1$. ■

**Lemma B.15** *Suppose $U$ satisfies Assumption 1 and 2. Let $\mathscr{F}'(t)$ be as in (25). Then*

$$\max\left\{\|\mathbf{h}^{(\ell)}\|_\infty, \|\mathbf{n}^{(\ell)}\|_\infty, \|\mathbf{H}^{(s)}\|_\infty, \|\mathbf{m}^{(s)}\|_\infty : s \leqslant t, \ell \leqslant t-1\right\} \leqslant N^{0.01}$$

*with probability* $1 - o_N(1)$.

**Proof** Note that Lemma A.4 implies, for all $1 \leqslant \ell \leqslant t-1$ and all $1 \leqslant s \leqslant t$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{i \leqslant N} \left( \frac{(\mathbf{H}^{(s)})_i}{\psi^{1/2}} \right)^{101} = \lim_{N\to\infty} \frac{1}{M} \sum_{a \leqslant M} \left( \frac{(\mathbf{h}^{(\ell)})_a}{q^{1/2}} \right)^{101} = \mathbb{E}(Z^{101}) \,,$$

where the convergence holds in probability. It follows that the event

$$\mathbf{\Omega} \equiv \left\{ \max \left\{ \frac{1}{N} \sum_{i \leqslant N} \left( \frac{(\mathbf{H}^{(s)})_i}{\psi^{1/2}} \right)^{101}, \frac{1}{M} \sum_{a \leqslant M} \left( \frac{(\mathbf{h}^{(\ell)})_a}{q^{1/2}} \right)^{101} : s \leqslant t, \ell \leqslant t-1 \right\} \leqslant 2\mathbb{E}(Z^{101}) \right\}$$

occurs with probability $1 - o_N(1)$. We claim that $\mathbf{\Omega}$ implies the desired bounds. Indeed, $\mathbf{\Omega}$ clearly implies

$$\max \left\{ \|\mathbf{m}^{(s)}\|_\infty : s \leqslant t \right\} \leqslant \max \left\{ \|\mathbf{H}^{(s)}\|_\infty : s \leqslant t \right\} \leqslant \psi^{1/2} \Big( 2N\mathbb{E}(Z^{101}) \Big)^{1/101} \leqslant N^{1/100} \,.$$

In the above, the first inequality uses that $\mathbf{m}^{(s)} = \operatorname{th}(\mathbf{H}^{(s)})$ and $|\operatorname{th}(x)| \leqslant |x|$; and the last bound holds for $N$ large enough (depending on $\psi$). Similarly, $\mathbf{\Omega}$ implies

$$\max \left\{ \|\mathbf{h}^{(\ell)}\|_\infty : \ell \leqslant t-1 \right\} \leqslant q^{1/2} \Big( N\alpha\mathbb{E}(Z^{101}) \Big)^{1/101} \leqslant N^{1/100} \,,$$

where the last bound holds for $N$ large enough (depending on $\alpha$, $q$). Finally, it follows using Lemma B.3 that

$$\left| (\mathbf{n}^{(\ell)})_a \right| = \left| F((\mathbf{h}^{(\ell)})_a) \right| \overset{(8)}{=} \left| \frac{1}{(1-q)^{1/2}} \frac{\mathbb{E}_\xi[\xi U((\mathbf{h}^{(\ell)})_a + (1-q)^{1/2}\xi)]}{\mathbb{E}_\xi U((\mathbf{h}^{(\ell)})_a + (1-q)^{1/2}\xi)} \right| \leqslant \frac{C_1(U) + 4|(\mathbf{h}^{(\ell)})_a|}{(1-q)^{1/2}} \,,$$

and combining with the previous bound on $\|\mathbf{h}^{(\ell)}\|_\infty$ gives

$$\begin{aligned} \max \left\{ \|\mathbf{n}^{(\ell)}\|_\infty : \ell \leqslant t-1 \right\} &= \max \left\{ \|F(\mathbf{h}^{(\ell)})\|_\infty : \ell \leqslant t-1 \right\} \\ &\leqslant \frac{C_1(U) + 4q^{1/2}(N\alpha\mathbb{E}(Z^{101}))^{1/101}}{(1-q)^{1/2}} \leqslant N^{1/100} \,, \end{aligned}$$

where the last bound holds for $N$ large enough. This proves the claim. ■

## Appendix C. Analysis of first moment

In this section we finish analyzing the conditional first moment bound (Theorem A.12) obtained in Section A. This leads to the proof of Theorem 1.4, our main result on the conditional first moment. From this we can deduce the upper bound in Theorem 1.1, as presented at the end of this section. For the reader's convenience, we begin by reviewing some important notations. Recall from (55) that

$$\pi_* \equiv q^{1/2} \mathbf{\Lambda}^{\mathsf{t}} \hat{e}_t = q^{1/2} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_{t-1} \\ (1 - \Lambda_{t-1})^{1/2}) \end{pmatrix} \in \mathbb{R}^t \,. \tag{109}$$

Recall also from (56) that we defined

$$\varpi_* \equiv (1-q)\psi^{1/2}\mathbf{\Gamma}^{\mathsf{t}}\acute{e}_{t-1} \equiv (1-q)\psi^{1/2}\begin{pmatrix}\gamma_1\\ \vdots\\ \gamma_{t-2}\\ (1-\Gamma_{t-2})^{1/2})\end{pmatrix} \in \mathbb{R}^{t-1}\,. \tag{110}$$

Given $\pi \in \mathbb{R}^t$ with $\|\pi\|^2 \leqslant 1$, we denote $c(\pi) \equiv (1-\|\pi\|^2)^{1/2}$. Next, as in the statement of Theorem A.12, given a parameter $\bar{\epsilon} \in \mathbb{R}$ (see (114) below), we let

$$\boldsymbol{X}(\pi,\varpi) \equiv \mathbf{x}[t]^{\mathsf{t}}\pi_* + \Big\{\mathbf{x}[t]^{\mathsf{t}}(\pi-\pi_*) + N^{1/2}\bar{\epsilon}\mathbf{c}[t-1]^{\mathsf{t}}(\varpi-\varpi_*)\Big\} \in \mathbb{R}^M\,. \tag{111}$$

We then recall the function $L$ from (26), and use it to define

$$\mathcal{L}(\pi,\varpi) \equiv \frac{1}{N}\sum_{a\leqslant M} L_{\|\pi\|^2}(\boldsymbol{X}_a(\pi,\varpi)) \equiv \frac{1}{N}\sum_{a\leqslant M}\log \mathbb{E}_\xi U(\boldsymbol{Y}_a(\pi,\varpi))\,. \tag{112}$$

(Note the last identity above serves as the definition of $\boldsymbol{Y} \equiv \boldsymbol{Y}(\pi,\varpi)$.) The bound in Theorem A.12 is expressed in terms of the function

$$\Psi(\pi,\varpi) \equiv \frac{\|\varpi-\bar{\epsilon}(\varpi-\varpi_*)\|^2}{2c(\pi)^2} - \frac{(\varpi_*,\varpi)}{1-q} + \mathcal{L}(\pi,\varpi)\,. \tag{113}$$

Recall (59) that we decomposed $\boldsymbol{Z}(\boldsymbol{G}') = \boldsymbol{Z}_\circ(\boldsymbol{G}') + \boldsymbol{Z}_\bullet(\boldsymbol{G}')$. The rest of this section is organized as follows:

- In §C.1 we use Lemmas A.22 and A.23 to prove Corollary C.1, which gives a bound on $\boldsymbol{Z}_\bullet(\boldsymbol{G}')$. This takes care of the case $(\pi,\varpi) \notin \boldsymbol{N}_\circ$ (see (57)), so in the rest of the section we restrict to $(\pi,\varpi) \in \boldsymbol{N}_\circ$.

- In §C.2 we prove Lemmas C.2 and C.3, which show that the point $(\pi_*,\varpi_*)$, as defined by (109) and (110), is approximately a stationary point of the function $\Psi$ of (113).

- In §C.3 we prove Proposition C.4, which bounds Hess $\Psi$ for $(\pi,\varpi) \in \boldsymbol{N}_\circ$.

- In §C.4 we combine the results described above to conclude the proof of Theorem 1.4. We then use this to conclude the proof of the upper bound in Theorem 1.1.

Lastly, we now fix the parameter

$$\bar{\epsilon} = e^5 C_1(U)\alpha^{1/2} \overset{(27)}{\leqslant} \frac{1}{C_1(U)^2 K_2(U)}\,. \tag{114}$$

However, this choice of $\bar{\epsilon}$ will not become important until Lemma C.10 below.

## C.1. Azuma–Hoeffding bounds

**Corollary C.1** *If $U$ satisifes Assumptions 1 and 2, then with high probability we have*

$$\mathbb{E}\Big(\boldsymbol{Z}_{\bullet}(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big) \leqslant \exp\Big\{N\Big(\mathrm{RS}(\alpha;U) - C_1(U)^2\alpha\Big)\Big\}$$

*for $\boldsymbol{Z}_{\bullet}(\boldsymbol{G}')$ as defined by (59).*

**Proof** Recall from Corollary B.8 that for $\alpha \leqslant \alpha(U)$ we have

$$\frac{\mathrm{RS}(\alpha;U) - \log 2}{\alpha} \geqslant -1.53 \cdot C_1(U)^2\,,$$

where $C_1(U) \geqslant 10$ is the constant from Lemma B.3. Recalling (59), we will first bound the case where $\|\varpi(J) - \varpi_*\|$ is large. To this end, denote

$$\boldsymbol{Z}_d(\boldsymbol{G}') \equiv \sum_J \mathbf{1}\Big\{d \leqslant \|\varpi(J) - \varpi_*\| \leqslant 2d\Big\}\mathrm{S}_J(\boldsymbol{G}')\,.$$

Thanks to Assumption 1, in Proposition A.13 we also have the trivial bound $\mathbb{E}(\mathrm{S}_J(\boldsymbol{G}')\,|\,\mathscr{F}'(t)) \leqslant 1$. Substituting this into the calculation (82) from the proof of Theorem A.12 gives

$$\frac{\mathbb{E}(\boldsymbol{Z}_d(\boldsymbol{G}')\,|\,\mathscr{F}'(t))}{\exp\{(\mathbf{1}, \log(2\operatorname{ch}(\mathbf{H}^{(t)})))\}} \leqslant \sum_{J: d \leqslant \|\varpi(J) - \varpi_*\| \leqslant 2d} \mathbf{Q}(J)\exp\bigg\{-\frac{N(\varpi_*, \varpi(J))}{1-q}\bigg\}\,.$$

By Lemma A.4 combined with Jensen's inequality, we have

$$\begin{aligned}\lim_{N\to\infty}\frac{(\mathbf{1}, \log\operatorname{ch}(\mathbf{H}^{(t)}))}{N} &= \mathbb{E}\log\operatorname{ch}(\psi^{1/2}Z) \leqslant \log\mathbb{E}\operatorname{ch}(\psi^{1/2}Z)\\ &= \log\mathbb{E}\exp(\psi^{1/2}Z) = \frac{\psi}{2} \overset{(28)}{\leqslant} \frac{3C_1(U)^2\alpha}{2}\,,\end{aligned} \tag{115}$$

where the convergence holds in probability as $N \to \infty$. It follows that, with high probability,

$$\frac{\exp\{(\mathbf{1}, \log(2\operatorname{ch}(\mathbf{H}^{(t)})))\}}{\exp\{N\mathrm{RS}(\alpha;U)\}} \leqslant \exp\Big\{N\Big(1.53 + 1.51\Big)C_1(U)^2\alpha\Big\} \leqslant \exp\Big\{3.05 \cdot NC_1(U)^2\alpha\Big\}\,.$$

Next, it follows from (36) and (56) that

$$\|\varpi_*\| \overset{(56)}{=} \psi^{1/2}(1-q)\|\boldsymbol{\Gamma}^{\mathrm{t}}\acute{e}_{t-1}\| \overset{(36)}{=} \psi^{1/2}(1-q)\bigg(\sum_{\ell \leqslant t-2}(\gamma_\ell)^2 + 1 - \Gamma_{t-2}\bigg)^{1/2} = \psi^{1/2}(1-q)\,.$$

Note also that if $d \leqslant \|\varpi(J) - \varpi_*\| \leqslant 2d$ then

$$-\frac{(\varpi_*, \varpi(J))}{1-q} = -\frac{\|\varpi_*\|^2 + (\varpi_*, \varpi(J) - \varpi_*)}{1-q} \leqslant \frac{\|\varpi_*\|\|\varpi(J) - \varpi_*\|}{1-q} \leqslant \frac{2d\|\varpi_*\|}{1-q} = 2\psi^{1/2}d\,.$$

Combining the above bounds gives, with high probability,

$$\begin{aligned}\frac{\mathbb{E}(\boldsymbol{Z}_d(\boldsymbol{G}') \,|\, \mathscr{F}'(t))}{\exp\{N\mathrm{RS}(\alpha;U)\}} &\leqslant \exp\bigg\{N\Big(3.05\cdot C_1(U)^2\alpha + 2\psi^{1/2}d\Big)\bigg\}\mathbf{Q}\Big(d \leqslant \Big\|\varpi(J)-\varpi_*\Big\| \leqslant 2d\Big)\\ &\leqslant \exp\bigg\{-N\Big(\frac{d^2}{2.01} - 2\psi^{1/2}d - 3.05\cdot C_1(U)^2\alpha + o_N(1)\Big)\bigg\}\,,\end{aligned}$$

where the last inequality is by Lemma A.23. If we take $d \geqslant d_0 \equiv 8\cdot C_1(U)\alpha^{1/2}$, then we obtain

$$\begin{aligned}\frac{\mathbb{E}(\boldsymbol{Z}_d(\boldsymbol{G}') \,|\, \mathscr{F}'(t))}{\exp\{N\mathrm{RS}(\alpha;U)\}} &\leqslant \exp\bigg\{-NC_1(U)^2\alpha\Big(\frac{8^2}{2.01} - 2\cdot 3^{1/2}\cdot 8 - 3.05 - o_N(1)\Big)\bigg\}\\ &\leqslant \exp\bigg\{-1.1\cdot NC_1(U)^2\alpha\bigg\}\,.\end{aligned}$$

This concludes our analysis of the case where $\|\varpi(J)-\varpi_*\|$ is large, so we next turn to the case that $\|\pi(J)-\pi_*\|$ is large. To this end, let us denote

$$\boldsymbol{Z}'(\boldsymbol{G}') \equiv \sum_J \mathbf{1}\bigg\{\frac{\|\varpi(J)-\varpi_*\|}{C_1(U)\alpha^{1/2}} \leqslant 8, \frac{\|\pi(J)-\pi_*(J)\|}{C_1(U)\alpha^{1/2}} \geqslant 16\bigg\}\mathrm{S}_J(\boldsymbol{G}')\,.$$

It follows from the previous bounds that

$$\begin{aligned}\frac{\mathbb{E}(\boldsymbol{Z}'(\boldsymbol{G}') \,|\, \mathscr{F}'(t))}{\exp\{N\mathrm{RS}(\alpha;U)\}} &\leqslant \exp\bigg\{N\Big(3.05\cdot C_1(U)^2\alpha + 2\psi^{1/2}\cdot 8\cdot C_1(U)\alpha^{1/2}\Big)\bigg\}\\ &\qquad\times\mathbf{Q}\bigg(\frac{\|\pi(J)-\pi_*(J)\|}{C_1(U)\alpha^{1/2}} \geqslant 16\bigg)\\ &\leqslant \exp\bigg\{NC_1(U)^2\alpha\Big(3.05 + 2\cdot 3^{1/2}\cdot 8 - \frac{16^2}{8.01} + o_N(1)\Big)\bigg\}\\ &\leqslant \exp\bigg\{-1.2\cdot NC_1(U)^2\alpha\bigg\}\,,\end{aligned}$$

where the second-to-last inequality is by Lemma A.22. Recalling the definition (59) of $\boldsymbol{Z}_\circ(\boldsymbol{G}')$, we have

$$\boldsymbol{Z}_\bullet(\boldsymbol{G}') \leqslant \boldsymbol{Z}'(\boldsymbol{G}') + \sum_{k\geqslant 0}\boldsymbol{Z}_{2^k d_0}(\boldsymbol{G}')\,,$$

where $d_0 = 8\cdot C_1(U)\alpha^{1/2}$ as above. It follows by combining the above bounds that

$$\frac{\mathbb{E}(\boldsymbol{Z}_\bullet(\boldsymbol{G}') \,|\, \mathscr{F}'(t))}{\exp\{N\mathrm{RS}(\alpha;U)\}} \leqslant \exp\bigg\{-NC_1(U)^2\alpha\bigg\}$$

with high probability, which proves the claim. ■

### C.2. Stationarity at replica symmetric value

In this subsection we show that the function $\Psi(\pi,\varpi)$ from (113) is approximately stationary at the point $(\pi_*,\varpi_*)$.

**Lemma C.2** *Suppose $U$ satisfies Assumption 1 and 2. Then for all $1 \leqslant s \leqslant t$ we have*

$$\frac{\partial\Psi}{\partial\pi_s}(\pi_*,\varpi_*) \simeq 0\,,$$

*where $\simeq$ indicates convergence in probability as $N \to \infty$.*

**Proof** Recalling (8), (98), and (108), we can rewrite

$$(F_q)'(x) = \frac{\mathbb{E}_\xi U''(x+(1-q)^{1/2}\xi)}{\mathbb{E}_\xi U(x+(1-q)^{1/2}\xi)} - (F_q(x))^2\,. \tag{116}$$

Recall from (112) the definition of $\boldsymbol{Y} \equiv \boldsymbol{Y}(\pi,\varpi)$. We then calculate

$$\begin{aligned}
\frac{\partial\mathcal{L}}{\partial\pi_s} &\overset{(112)}{=} \frac{1}{N}\sum_{a\leqslant M}\left\{\frac{\partial\boldsymbol{X}_a}{\partial\pi_s}\frac{\mathbb{E}_\xi U'(\boldsymbol{Y}_a)}{\mathbb{E}_\xi U(\boldsymbol{Y}_a)} + \frac{\partial c}{\partial\pi_s}\frac{\mathbb{E}_\xi[\xi U'(\boldsymbol{Y}_a)]}{\mathbb{E}_\xi U(\boldsymbol{Y}_a)}\right\} \\
&\overset{(98)}{=} \frac{1}{N}\sum_{a\leqslant M}\left\{(\mathbf{x}^{(s)})_a F_{\|\pi\|^2}(\boldsymbol{X}_a) - \pi_s\frac{\mathbb{E}_\xi U''(\boldsymbol{Y}_a)}{\mathbb{E}_\xi U(\boldsymbol{Y}_a)}\right\} \\
&\overset{(116)}{=} \frac{1}{N}\left\{(\mathbf{x}^{(s)}, F_{\|\pi\|^2}(\boldsymbol{X}_a)) - \pi_s(\mathbf{1},(F_{\|\pi\|^2})'(\boldsymbol{X})) - \pi_s\|F_{\|\pi\|^2}(\boldsymbol{X})\|^2\right\}.
\end{aligned}$$

It follows from (109) that $\|\pi_*\|^2 = q$, and $c_* \equiv c(\pi_*) = (1-q)^{1/2}$. We also note that

$$\mathbf{h}^{(t+1)} = \mathbf{h}[t]^{\mathrm{t}}\hat{e}_t \overset{(39)}{=} q^{1/2}\mathbf{x}[t]^{\mathrm{t}}\boldsymbol{\Lambda}^{\mathrm{t}}\hat{e}_t \overset{(109)}{=} \mathbf{x}[t]^{\mathrm{t}}\pi_* \overset{(111)}{=} \boldsymbol{X}(\pi_*,\varpi_*) \equiv \boldsymbol{X}_*\,.$$

It follows using (39) and Lemma A.4 that at $(\pi_*,\varpi_*)$ we have

$$\frac{(\mathbf{x}^{(s)}, F_{\|\pi_*\|^2}(\boldsymbol{X}_*))}{N} \simeq \alpha\Lambda_{t,s}\mathbb{E}ZF_q(q^{1/2}Z) \overset{(109)}{=} \pi_{*,s}\alpha\mathbb{E}(F_q)'(q^{1/2}Z)\,,$$

having again used gaussian integration by parts at the last step. As a consequence

$$\frac{\partial\mathcal{L}}{\partial\pi_s}(\pi_*,\varpi_*) \simeq -\pi_{*,s}\alpha\mathbb{E}\Big[F_q(q^{1/2}Z)^2\Big] \overset{(9)}{=} -\pi_{*,s}\psi\,.$$

Substituting this into (113) gives

$$\frac{\partial\Psi}{\partial\pi_s}(\pi_*,\varpi_*) \simeq \frac{\|\varpi_*\|^2\pi_{*,s}}{(1-\|\pi_*\|^2)^2} - \pi_{*,s}\psi \overset{(110)}{=} 0\,,$$

as claimed. ■

**Lemma C.3** *Suppose $U$ satisfies Assumption 1 and 2, and $0 \leqslant \alpha \leqslant \alpha(U)$. Then for all $1 \leqslant \ell \leqslant t-2$ we have*

$$\frac{\partial \Psi}{\partial \varpi_\ell}(\pi_*, \varpi_*) \simeq 0\,,$$

*where $\simeq$ indicates convergence in probability as $N \to \infty$. For $\ell = t-1$ we have*

$$\frac{\partial \Psi}{\partial \varpi_\ell}(\pi_*, \varpi_*) \simeq \bar{\epsilon}\psi^{1/2}\Big(\gamma_{t-1} - (1-\Gamma_{t-2})^{1/2}\Big)\,,$$

*where the right-hand side is $o_t(1)$ by Proposition A.6.*

**Proof** Similarly to the proof of Lemma C.2, we calculate

$$\frac{\partial \mathcal{L}}{\partial \varpi_\ell} \overset{(112)}{=} \frac{1}{N}\sum_{a \leqslant M} \frac{\partial \boldsymbol{X}_a}{\partial \varpi_\ell} \frac{\mathbb{E}_\xi U'(\boldsymbol{Y}_a)}{\mathbb{E}_\xi U(\boldsymbol{Y}_a)} = \frac{\bar{\epsilon}(\mathbf{c}^{(\ell)}, F_{\|\pi\|^2}(\boldsymbol{X}))}{N^{1/2}}\,.$$

It follows by recalling Lemma A.4 that

$$\frac{\partial \mathcal{L}}{\partial \varpi_\ell}(\pi_*, \varpi_*) = \frac{\bar{\epsilon}(\mathbf{c}^{(\ell)}, \mathbf{n}^{(t+1)})}{N^{1/2}} \simeq \bar{\epsilon}\psi^{1/2}\gamma_\ell\,.$$

Substituting this into (113) gives

$$\frac{\partial \Psi}{\partial \varpi_\ell}(\pi_*, \varpi_*) \simeq \bar{\epsilon}\bigg\{ -\frac{\varpi_{*,\ell}}{1-q} + \psi^{1/2}\gamma_\ell \bigg\}\,,$$

and combining with (110) gives the claim. ■

## C.3. Hessian calculation

If $A$ and $B$ are symmetric matrices, we write $A \preccurlyeq B$ to indicate that $B - A$ is positive semidefinite. In this subsection we analyze the Hessian of the function $\Psi$ from (113) to prove:

**Proposition C.4** *If $U$ satisfies Assumptions 1 and 2, then the function $\mathcal{L}$ of (112) satisfies*

$$\operatorname{Hess}\Psi(\pi,\varpi) = \begin{pmatrix} \Psi_{\pi,\pi} & \Psi_{\pi,\varpi} \\ \Psi_{\pi,\varpi} & \Psi_{\varpi,\varpi} \end{pmatrix}\bigg|_{(\pi,\varpi)} \preccurlyeq \begin{pmatrix} e^7 C_1(U)^2 K_2(U)\alpha I & 0 \\ 0 & 1-1.9\bar{\epsilon} \end{pmatrix}$$

*for all $(\pi,\varpi) \in \boldsymbol{N}_\circ$ (as defined by (57)), for $0 \leqslant \alpha \leqslant \alpha(U)$ as defined by (27), and $\bar{\epsilon} = \bar{\epsilon}(\alpha; U)$ as in (114).*

The proof of Proposition C.4 is given at the end of this subsection. We divide the analysis into several steps. Define

$$A_c(x) = \frac{\mathbb{E}_\xi U''(x+c\xi)}{\mathbb{E}_\xi U(x+c\xi)} - \bigg(\frac{\mathbb{E}_\xi U'(x+c\xi)}{\mathbb{E}_\xi U(x+c\xi)}\bigg)^2 = (F_{1-c^2})'(x)\,, \tag{117}$$

$$B_c(x) \equiv \frac{\mathbb{E}_\xi[\xi U''(x+c\xi)]}{\mathbb{E}_\xi U(x+c\xi)} - \frac{\mathbb{E}_\xi[\xi U'(x+c\xi)]}{\mathbb{E}_\xi U(x+c\xi)}\frac{\mathbb{E}_\xi U'(x+c\xi)}{\mathbb{E}_\xi U(x+c\xi)}\,. \tag{118}$$

Define the $M$-dimensional vectors $\mathbf{A} \equiv A_{c(\pi)}(\boldsymbol{X})$ and $\mathbf{B} \equiv B_{c(\pi)}(\boldsymbol{X})$. Next let

$$a_c(x) \equiv \frac{\mathbb{E}_\xi[\xi U'(x+c\xi)]}{\mathbb{E}_\xi U(x+c\xi)}\,, \tag{119}$$

$$b_c(x) \equiv \frac{\mathbb{E}_\xi[\xi^2 U''(x+c\xi)]}{\mathbb{E}_\xi U(x+c\xi)} - \left(\frac{\mathbb{E}_\xi[\xi U'(x+c\xi)]}{\mathbb{E}_\xi U(x+c\xi)}\right)^2, \tag{120}$$

and define the scalars $\bar{a} \equiv (\mathbf{1}, a_{c(\pi)}(\boldsymbol{X}))$ and $\bar{b} \equiv (\mathbf{1}, b_{c(\pi)}(\boldsymbol{X}))$.

**Lemma C.5** *For the function $\mathcal{L}$ defined by (112) we have*

$$\begin{aligned}\mathcal{L}_{\pi,\pi} &= \frac{1}{N}\left\{\mathbf{x}[t](\operatorname{diag}\mathbf{A})\mathbf{x}[t]^{\mathrm{t}} + \left(\mathbf{x}[t]\mathbf{B}(\nabla c)^{\mathrm{t}} + (\nabla c)(\mathbf{x}[t]\mathbf{B})^{\mathrm{t}}\right)\right\} \\ &\quad + \frac{1}{N}\left\{\bar{a}\cdot \operatorname{Hess} c + \bar{b}\cdot(\nabla c)(\nabla c)^{\mathrm{t}}\right\}, \end{aligned}\tag{121}$$

$$\mathcal{L}_{\pi,\varpi} = \frac{\bar{\epsilon}}{N^{1/2}}\left\{\mathbf{x}[t](\operatorname{diag}\mathbf{A})\mathbf{c}[t-1]^{\mathrm{t}} + (\nabla c)\mathbf{c}[t-1]\mathbf{B}\right\}, \tag{122}$$

$$\mathcal{L}_{\varpi,\varpi} = \bar{\epsilon}^2\left\{\mathbf{c}[t-1](\operatorname{diag}\mathbf{A})\mathbf{c}[t-1]^{\mathrm{t}}\right\} \tag{123}$$

*for $\mathbf{A}$, $\mathbf{B}$, $\bar{a}$, and $\bar{b}$ as defined above.*

**Proof** Again recall from (112) the definition of $\boldsymbol{Y} \equiv \boldsymbol{Y}(\pi, \varpi)$. Note that $\boldsymbol{Y}$ is linear in $\varpi$, with first derivative

$$\frac{\partial \boldsymbol{Y}_a}{\partial \varpi_\ell} = \frac{\partial \boldsymbol{X}_a}{\partial \varpi_\ell} = N^{1/2}\bar{\epsilon}(\mathbf{c}^{(\ell)})_a\,.$$

It follows by differentiating (112) twice that

$$\begin{aligned}\frac{\partial \mathcal{L}^2}{\partial\varpi_k\partial\varpi_\ell} &= \frac{1}{N}\sum_{a\leqslant M}\left\{\frac{\mathbb{E}_\xi[U''(\boldsymbol{Y}_a)\frac{\partial \boldsymbol{Y}_a}{\partial\varpi_k}\frac{\partial \boldsymbol{Y}_a}{\partial\varpi_\ell}]}{\mathbb{E}_\xi U(\boldsymbol{Y}_a)} - \left(\frac{\mathbb{E}_\xi[U'(\boldsymbol{Y}_a)\frac{\partial \boldsymbol{Y}_a}{\partial\varpi_k}]}{\mathbb{E}_\xi U(\boldsymbol{Y}_a)}\right)\left(\frac{\mathbb{E}_\xi[U'(\boldsymbol{Y}_a)\frac{\partial \boldsymbol{Y}_a}{\partial\varpi_\ell}]}{\mathbb{E}_\xi U(\boldsymbol{Y}_a)}\right)\right\} \\ &= \frac{1}{N}\sum_{a\leqslant M}\mathbf{A}_a\frac{\partial \boldsymbol{X}_a}{\partial\varpi_k}\frac{\partial \boldsymbol{X}_a}{\partial\varpi_\ell} = \bar{\epsilon}^2\left\{\mathbf{c}[t-1](\operatorname{diag}\mathbf{A})\mathbf{c}[t-1]^{\mathrm{t}}\right\}_{k,\ell},\end{aligned}$$

which verifies (123). On the other hand we note that $\boldsymbol{Y}$ depends on $\pi$ both through $\boldsymbol{X}$ and through $c(\pi)$, and

$$\frac{\partial \boldsymbol{Y}_a}{\partial \pi_s} = \frac{\partial \boldsymbol{X}_a}{\partial \pi_s} + \frac{\partial c}{\partial \pi_s}\xi \overset{(111)}{=} \mathbf{x}[t]_s + \frac{\partial c}{\partial \pi_s}\xi\,.$$

We use this to calculate the mixed partial

$$\begin{aligned}\frac{\partial \mathcal{L}^2}{\partial\pi_s\partial\varpi_\ell} &= \frac{1}{N}\left\{\sum_{a\leqslant M}\mathbf{A}_a\frac{\partial \boldsymbol{X}_a}{\partial\pi_s}\frac{\partial \boldsymbol{X}_a}{\partial\varpi_\ell} + \frac{\partial c}{\partial\pi_s}\sum_{a\leqslant M}\mathbf{B}_a\frac{\partial \boldsymbol{X}_a}{\partial\varpi_\ell}\right\} \\ &= \frac{\bar{\epsilon}}{N^{1/2}}\left(\mathbf{x}[t](\operatorname{diag}\mathbf{A})\mathbf{c}[t-1]^{\mathrm{t}} + (\nabla c)\mathbf{c}[t-1]\mathbf{B}\right)_{s,\ell},\end{aligned}$$

which verifies (122). Finally, a similar calculation gives

$$\frac{\partial \mathcal{L}^2}{\partial \pi_r \partial \pi_s} = \frac{1}{N}\left\{ \sum_{a\leqslant M} \mathbf{A}_a \frac{\partial \boldsymbol{X}_a}{\partial \pi_s}\frac{\partial \boldsymbol{X}_a}{\partial \varpi_\ell} + \frac{\partial c}{\partial \pi_s}\sum_{a\leqslant M} \mathbf{B}_a \frac{\partial \boldsymbol{X}_a}{\partial \varpi_\ell} + \bar{a}\frac{\partial^2 c}{\partial \pi_r \partial \pi_s} + \bar{b}\frac{\partial c}{\partial \pi_r}\frac{\partial c}{\partial \pi_s}\right\},$$

which implies (121). ■

We now proceed to bound the quantities defined above.

**Lemma C.6** *Suppose $U$ satisfies Assumptions 1 and 2. With the notation from (118), we have*

$$\frac{\|\mathbf{B}\|}{M^{1/2}} = \frac{\|B_{c(\pi)}(\boldsymbol{X})\|}{M^{1/2}} \leqslant K_2(U)\bigg(2.5\cdot C_1(U) + 5.8\cdot \frac{\|\boldsymbol{X}\|}{M^{1/2}}\bigg).$$

*for all* $0.95 \leqslant c \leqslant 1$.

**Proof** Recalling the notation of Definition B.1, we first use gaussian integration by parts to rewrite (118) as

$$B_c(x) = \frac{1}{c^2}\bigg\{\operatorname{Cov}_{x,c}(Z^2, Z) - 2\cdot \mathbb{E}_{x,c}(Z)\bigg\}.$$

It follows by combining Lemmas B.3 and B.4 that for all $0.95 \leqslant c \leqslant 1$,

$$|B_c(x)| \leqslant \frac{1}{c^2}\bigg\{2\bigg(C_1(U) + \frac{1.82\cdot|x|}{0.95}\bigg) + \frac{K_2(U)}{2^{1/2}}\bigg(\frac{1.82\cdot|x|}{0.95} + C_1(U)^{1/2}\bigg)\bigg\}.$$

Recall that we assumed (without loss) $C_1(U) \geqslant 10$ and $K_2(U) \geqslant 1$, so for instance we can trivially bound $(C_1(U))^{1/2} \leqslant C_1(U)/10^{1/2}$. This leads to the simplified bound

$$\begin{aligned}|B_c(x)| &\leqslant \frac{K_2(U)}{0.95^2}\bigg\{\bigg(2 + \frac{1}{(2\cdot 10)^{1/2}}\bigg)C_1(U) + \bigg(2 + \frac{1}{2^{1/2}}\bigg)\frac{1.82\cdot|x|}{0.95}\bigg\} \\ &\leqslant K_2(U)\bigg(2.5\cdot C_1(U) + 5.8\cdot|x|\bigg).\end{aligned}$$

where the last bound again uses that $C_1(U) \geqslant 10$. The claim follows. ■

**Lemma C.7** *Suppose $U$ satisfies Assumption 1. With the notation from (119), we have*

$$\frac{|\bar{a}|}{M} = \frac{|(\mathbf{1}, a_{c(\pi)}(\boldsymbol{X}))|}{M} \leqslant 1.1\cdot C_1(U) + 3.7\cdot\frac{\|\boldsymbol{X}\|^2}{M}$$

*for all* $0.95 \leqslant c \leqslant 1$.

**Proof** We use gaussian integration by parts to rewrite (119) as

$$a_c(x) = \frac{\mathbb{E}_\xi[\xi^2 U(x + c\xi)]}{\mathbb{E}_\xi U(x+c\xi)} - 1\,.$$

It follows by Lemma B.3 (which uses only Assumption 1) that for all $0.95 \leqslant c \leqslant 1$,

$$|a_c(x)| \leqslant 1 + \bigg(C_1(U) + \bigg(\frac{1.82\cdot x}{0.95}\bigg)^2\bigg) \leqslant 1.1\cdot C_1(U) + 3.7\cdot x^2\,,$$

where the last bound uses that we took $C_1(U) \geqslant 10$. ■

**Lemma C.8** *Suppose $U$ satisfies Assumptions 1 and 2. With the notation from (120), we have*

$$\frac{|\bar{b}|}{M} = \frac{|(\mathbf{1}, b_{c(\pi)}(\boldsymbol{X}))|}{M} \leqslant K_2(U)\bigg(4.6 \cdot C_1(U) + 17 \cdot \frac{\|\boldsymbol{X}\|^2}{M}\bigg)$$

*for all* $0.95 \leqslant c \leqslant 1$.

**Proof** We use gaussian integration by parts to rewrite (120) as

$$\begin{aligned} b_c(x) &= \frac{1}{c^2}\bigg\{\frac{\mathbb{E}_\xi[(\xi^4 - 5\xi^2 + 2)U(x + c\xi)]}{\mathbb{E}_\xi U(x + c\xi)} - \bigg(\frac{\mathbb{E}_\xi[\xi^2 U(x + c\xi)]}{\mathbb{E}_\xi U(x + c\xi)} - 1\bigg)^2\bigg\} \\ &= \frac{1}{c^2}\bigg\{\operatorname{Var}_{x,c}(Z^2) - 3 \cdot \mathbb{E}_{x,c}(Z^2) + 1\bigg\}. \end{aligned}$$

It follows by combining Lemmas B.3 and B.4 that for all $0.95 \leqslant c \leqslant 1$,

$$\begin{aligned} |b_c(x)| &\leqslant \frac{1}{c^2}\bigg\{K_2(U)\bigg\{\bigg(\frac{1.82 \cdot x}{c}\bigg)^2 + C_1(U)\bigg\} + 3\bigg(C_1(U) + \bigg(\frac{1.82 \cdot x}{0.95}\bigg)^2\bigg) + 1\bigg\} \\ &\leqslant \frac{K_2(U)}{0.95^2}\bigg\{\bigg(4 + \frac{1}{10}\bigg)C_1(U) + 4 \cdot \bigg(\frac{1.82 \cdot x}{0.95}\bigg)^2\bigg\}, \end{aligned}$$

where the last bound uses that we took $C_1(U) \geqslant 10$ and $K_2(U) \geqslant 1$. The claim follows. ■

**Corollary C.9** *If $U$ satisfies Assumptions 1 and 2, then the function $\mathcal{L}$ of (112) satisfies*

$$\operatorname{Hess}\mathcal{L}(\pi, \varpi) = \begin{pmatrix} \mathcal{L}_{\pi,\pi} & \mathcal{L}_{\pi,\varpi} \\ \mathcal{L}_{\pi,\varpi} & \mathcal{L}_{\varpi,\varpi} \end{pmatrix}\bigg|_{(\pi,\varpi)} \preccurlyeq K_2(U)\begin{pmatrix} C_1(U)^2\alpha I & 0 \\ 0 & 5 \cdot \bar{\epsilon}^2 I \end{pmatrix}$$

*for all $(\pi, \varpi) \in \boldsymbol{N}_\circ$ (as defined by (57)), for $0 \leqslant \alpha \leqslant \alpha(U)$ as defined by (27), and $\bar{\epsilon} = \bar{\epsilon}(\alpha; U)$ as in (27).*

**Proof** We will bound each of the terms computed in Lemma C.5. Let $u$ denote any vector in $\mathbb{R}^t$ and let $v$ denote any vector in $\mathbb{R}^{t-1}$. It follows from Lemma A.4 that, with high probability,

$$\sup\bigg\{\frac{\|\mathbf{x}[t]^{\mathsf{t}}u\|^2}{M} = \frac{1}{M}\bigg\|\sum_{s \leqslant t} u_s \mathbf{x}^{(s)}\bigg\|^2 : u \in \mathbb{R}^{t-1}, \|u\| = 1\bigg\} \leqslant 2\,. \tag{124}$$

Next, it follows from (109) that $\|\pi_*\| = q^{1/2}$, so the restriction $(\pi, \varpi) \in \boldsymbol{N}_\circ$ (see (57)) implies

$$\begin{aligned} \frac{\|\nabla c\|}{2} &\leqslant \|\pi\| \leqslant q^{1/2} + 16 \cdot C_1(U)\alpha^{1/2} \overset{(28)}{\leqslant} 18 \cdot C_1(U)\alpha^{1/2} \\ &\overset{(27)}{\leqslant} \frac{18}{e^5 \cdot C_1(U)^2 K_2(U)^2} \leqslant \frac{1}{e^6 \cdot K_2(U)^2}\,, \end{aligned} \tag{125}$$

where the last bound uses that we assumed (without loss) $C_1(U) \geqslant 10$ and $K_2(U) \geqslant 1$. Therefore we certainly have $c(\pi) = (1 - \|\pi\|^2)^{1/2} \geqslant 0.95$. It follows from (117) and Lemma B.14 (which uses Assumption 2) that

$$\|\mathbf{A}\|_\infty \leqslant \|A_{c(\pi)}\|_\infty = \|(F_{\|\pi\|})'\|_\infty \leqslant \frac{1}{c(\pi)^2}\bigg\{\frac{K_2(U)}{2} + 1\bigg\} \leqslant \frac{K_2(U)/2 + 1}{0.95^2} \leqslant 1.7 \cdot K_2(U)\,. \tag{126}$$

It follows that, with high probability, it holds for all unit vectors $u, v$ that

$$u^{\mathrm{t}}\bigg(\frac{1}{N}\mathbf{x}[t](\operatorname{diag}\mathbf{A})\mathbf{x}[t]^{\mathrm{t}}\bigg)u \leqslant \frac{\|\mathbf{A}\|_\infty}{N}\cdot\Big\|\mathbf{x}[t]^{\mathrm{t}}u\Big\|^2 \leqslant 3.4\cdot K_2(U)\alpha\,, \tag{127}$$

$$u^{\mathrm{t}}\bigg(\frac{1}{N^{1/2}}\mathbf{x}[t](\operatorname{diag}\mathbf{A})\mathbf{c}[t-1]^{\mathrm{t}}\bigg)v \leqslant \frac{\|\mathbf{A}\|_\infty}{N^{1/2}}\cdot\Big\|\mathbf{x}[t]^{\mathrm{t}}u\Big\|\cdot\Big\|\mathbf{c}[t-1]^{\mathrm{t}}v\Big\| \leqslant 2.5\cdot K_2(U)\alpha^{1/2}\,, \tag{128}$$

$$v^{\mathrm{t}}\bigg(\mathbf{c}[t-1](\operatorname{diag}\mathbf{A})\mathbf{c}[t-1]^{\mathrm{t}}\bigg)v \leqslant \|\mathbf{A}\|_\infty\cdot\Big\|\mathbf{c}[t-1]^{\mathrm{t}}v\Big\|^2 \leqslant 1.7\cdot K_2(U)\,. \tag{129}$$

Next, recalling (111), for all $(\pi,\varpi)\in\boldsymbol{N}_\circ$ we have

$$\frac{\|\boldsymbol{X}(\pi,\varpi)\|}{M^{1/2}} \overset{(124)}{\leqslant} 2^{1/2}\|\pi\| + \frac{\bar{\epsilon}\|\varpi-\varpi_*\|}{\alpha^{1/2}} \overset{(57)}{\leqslant} 2^{1/2}\|\pi\| + 16\cdot\bar{\epsilon}C_1(U) \overset{(125)}{\leqslant} 0.33\cdot C_1(U)\,, \tag{130}$$

having used that $C_1(U)\geqslant 10$ and $|\bar{\epsilon}|\leqslant 1/50$. Combining (130) with Lemma C.6 gives

$$\frac{\|\mathbf{B}\|}{M^{1/2}} \leqslant K_2(U)\bigg(2.5\cdot C_1(U) + 5.8\cdot\frac{\|\boldsymbol{X}\|}{M^{1/2}}\bigg) \leqslant 4.5\cdot C_1(U)K_2(U)\,.$$

Combining the above with (124) and (125) gives that with high probability, for all unit vectors $u, v$ we have

$$\begin{aligned}
u^{\mathrm{t}}\bigg(\frac{1}{N}\mathbf{x}[t]\mathbf{B}(\nabla c)^{\mathrm{t}}\bigg)u &\leqslant \frac{\|\mathbf{x}[t]^{\mathrm{t}}u\|\|\mathbf{B}\|\|\nabla c\|}{N}\\
&\leqslant \frac{(2M)^{1/2}}{N}\Big(4.5\cdot C_1(U)K_2(U)M^{1/2}\Big)\Big(36\cdot C_1(U)\alpha^{1/2}\Big)\\
&\overset{(27)}{\leqslant} \frac{2^{1/2}\cdot 4.5\cdot 36}{e^5\cdot C_1(U)}\cdot\alpha \leqslant 0.16\cdot\alpha\,,
\end{aligned} \tag{131}$$

again using that $C_1(U)\geqslant 10$. Similarly, with high probability, it holds for all unit vectors $u, v$ that

$$\begin{aligned}
u^{\mathrm{t}}\bigg(\frac{1}{N^{1/2}}(\nabla c)\mathbf{c}[t-1]\mathbf{B}\bigg)v \leqslant \frac{\|\mathbf{B}\|\|\nabla c\|}{N^{1/2}} &\leqslant \Big(4.5\cdot C_1(U)K_2(U)\alpha^{1/2}\Big)\Big(36\cdot C_1(U)\alpha^{1/2}\Big)\\
&\overset{(27)}{\leqslant} \frac{4.5\cdot 36}{e^5\cdot C_1(U)}\cdot\alpha^{1/2} \leqslant 0.11\cdot\alpha^{1/2}\,.
\end{aligned} \tag{132}$$

Next, combining (130) with Lemma C.8 gives

$$\frac{|\bar{b}|}{M} \leqslant K_2(U)\bigg(4.6\cdot C_1(U) + 17\cdot\Big(0.33\cdot C_1(U)\Big)^2\bigg) \leqslant 2.4\cdot C_1(U)^2K_2(U)\,.$$

Combining the above with (125) gives, for any unit vector $u$,

$$\begin{aligned}
u^{\mathrm{t}}\bigg(\frac{1}{N}\bar{b}(\nabla c)(\nabla c)^{\mathrm{t}}\bigg)u &\leqslant \frac{|\bar{b}|\|\nabla c\|^2}{N}\\
&\leqslant \Big(2.4\cdot C_1(U)^2K_2(U)\Big)\cdot\bigg(\frac{18}{e^5\cdot C_1(U)^2K_2(U)^2}\bigg)^2\alpha \leqslant \frac{\alpha}{e^7}\,.
\end{aligned} \tag{133}$$

Finally, we note that the Hessian of $c(\pi) = (1 - \|\pi\|^2)^{1/2}$ can be calculated as

$$\operatorname{Hess} c(\pi) = -\frac{1}{c(\pi)}\left\{ I + \frac{\pi\pi^{\mathrm{t}}}{c(\pi)^2} \right\}.$$

We can bound the above in operator norm by

$$\|\operatorname{Hess} c(\pi)\| \leqslant \frac{1}{0.95}\left(1 + \frac{\|\pi\|^2}{0.95^2}\right) \overset{(125)}{\leqslant} \frac{1}{0.95}\left(1 + \frac{(1/e^6)^2}{0.95^2}\right) \leqslant 1.1\,.$$

Combining (130) with Lemma C.7 gives

$$\frac{|\bar{a}|}{M} \leqslant 1.1 \cdot C_1(U) + 3.7 \cdot \Big(0.33 \cdot C_1(U)\Big)^2 \leqslant 0.6 \cdot C_1(U)^2\,,$$

so altogether we obtain, for any unit vector $u$,

$$u^{\mathrm{t}}\left(\frac{1}{N}\bar{a} \cdot \operatorname{Hess} c\right)u \leqslant 1.1 \cdot 0.6 \cdot C_1(U)^2\alpha \leqslant 0.7 \cdot C_1(U)^2\alpha\,. \tag{134}$$

To conclude, we note that substituting (129) into (123) implies

$$\frac{\|\mathcal{L}_{\varpi,\varpi}\|}{\bar{\epsilon}^2} \leqslant 1.7 \cdot K_2(U)\,.$$

Substituting (128) and (132) into (122) implies

$$\frac{\|\mathcal{L}_{\pi,\varpi}\|}{\alpha^{1/2}\bar{\epsilon}} \leqslant 2.5 \cdot K_2(U) + 0.11 \leqslant 2.7 \cdot K_2(U)\,.$$

Finally, substituting (127), (131), (133), and (134) into (121) gives

$$\frac{\|\mathcal{L}_{\pi,\pi}\|}{\alpha} \leqslant 3.4 \cdot K_2(U) + 2 \cdot 0.16 + \frac{1}{e^7} + 0.7 \cdot C_1(U)^2 \leqslant 0.8 \cdot C_1(U)^2 K_2(U)\,.$$

Consequently, for any vector $x \equiv (\dot{x}, \ddot{x})$ where $\dot{x} \in \mathbb{R}^t$ and $\ddot{x} \in \mathbb{R}^{t-1}$, we have

$$\begin{aligned}\frac{|x^{\mathrm{t}}(\operatorname{Hess}\mathcal{L})x|}{K_2(U)} &\leqslant 0.8 \cdot C_1(U)^2\alpha\|\dot{x}\|^2 + 1.7 \cdot \bar{\epsilon}^2\|\ddot{x}\|^2 + 2 \cdot 2.7 \cdot \alpha^{1/2}\bar{\epsilon}\|\dot{x}\|\|\ddot{x}\| \\ &\leqslant \Big(0.8 \cdot C_1(U)^2 + 2.7\Big)\alpha\|\dot{x}\|^2 + \Big(1.7 + 2.7\Big)\bar{\epsilon}^2\|\ddot{x}\|^2\,.\end{aligned}$$

The claim follows. ■

Recalling (113), let us now denote

$$\mathcal{P}(\pi, \varpi) \equiv \frac{\|\varpi - \bar{\epsilon}(\varpi - \varpi_*)\|^2}{2c(\pi)^2} - \frac{(\varpi_*, \varpi)}{1 - q}\,, \tag{135}$$

so that $\Psi = \mathcal{P} + \mathcal{L}$.

**Lemma C.10** *If $U$ satisfies Assumptions 1 and 2, then the function $\mathcal{P}$ of (135) satisfies*

$$\operatorname{Hess}\mathcal{P}(\pi,\varpi)=\begin{pmatrix}\mathcal{P}_{\pi,\pi} & \mathcal{P}_{\pi,\varpi}\\ \mathcal{P}_{\pi,\varpi} & \mathcal{P}_{\varpi,\varpi}\end{pmatrix}\Bigg|_{(\pi,\varpi)} \preccurlyeq \begin{pmatrix}1080\cdot C_1(U)^2\alpha I & 0\\ 0 & (1-1.95\cdot\bar\epsilon)I\end{pmatrix}$$

*for all $(\pi,\varpi)\in\boldsymbol{N}_\circ$ (as defined by (57)), for $0\leqslant\alpha\leqslant\alpha(U)$ as defined by (27), and $\bar\epsilon=\bar\epsilon(\alpha;U)$ as in (114).*

**Proof** We first calculate the mixed partial derivatives

$$\begin{aligned}\mathcal{P}_{\pi,\pi}&=\frac{\|\varpi-\bar\epsilon(\varpi-\varpi_*)\|^2}{c(\pi)^4}\left\{I+\frac{4\pi\pi^{\mathrm{t}}}{c(\pi)^2}\right\},\\ \mathcal{P}_{\pi,\varpi}&=\frac{2(1-\bar\epsilon)}{c(\pi)^4}\pi\Big(\varpi-\bar\epsilon(\varpi-\varpi_*)\Big)^{\mathrm{t}},\\ \mathcal{P}_{\varpi,\varpi}&=\frac{(1-\bar\epsilon)^2}{c(\pi)^2}I=\frac{(1-\bar\epsilon)^2}{1-\|\pi\|^2}I\,.\end{aligned}$$

We have from (110) that $\|\varpi_*\|=(1-q)\psi^{1/2}\leqslant\psi^{1/2}$. Then, for $(\pi,\varpi)\in\boldsymbol{N}_\circ$ (as defined by (57)) we must have

$$\|\varpi\|\leqslant\psi^{1/2}+16\cdot C_1(U)\alpha^{1/2}\overset{(28)}{\leqslant}18\cdot C_1(U)\alpha^{1/2}\overset{(27)}{\leqslant}\frac{18}{e^5\cdot C_1(U)^2}\leqslant\frac{1}{e^6}\tag{136}$$

(very similarly to (125)). It follows using (125) and (136) that

$$\begin{aligned}\|\mathcal{P}_{\pi,\pi}\|&\leqslant\frac{(18\cdot C_1(U))^2\alpha}{0.95^4}\left(1+\frac{4\cdot(1/e^6)^2}{0.95^2}\right)\leqslant e^6\cdot C_1(U)^2\alpha\,,\\ \|\mathcal{P}_{\pi,\varpi}\|&\leqslant\frac{2(18\cdot C_1(U))^2\alpha}{0.95^4}\leqslant720\cdot C_1(U)^2\alpha\overset{(114)}{\leqslant}\frac{\bar\epsilon^2}{e^3}\,,\\ \|\mathcal{P}_{\varpi,\varpi}\|&\leqslant\frac{(1-\bar\epsilon)^2}{1-(18\cdot C_1(U))^2\alpha}\leqslant(1-\bar\epsilon)^2+2\cdot(18\cdot C_1(U))^2\alpha\overset{(114)}{\leqslant}1-2\bar\epsilon+1.03\cdot\bar\epsilon^2\,.\end{aligned}$$

Consequently, for any vector $x\equiv(\dot x,\ddot x)$ where $\dot x\in\mathbb{R}^t$ and $\ddot x\in\mathbb{R}^{t-1}$, we have

$$\begin{aligned}|x^{\mathrm{t}}(\operatorname{Hess}\mathcal{P})x|&\leqslant360\cdot C_1(U)^2\alpha\|\dot x\|^2+2\cdot720\cdot C_1(U)^2\alpha\|\dot x\|\|\ddot x\|+\Big(1-2\bar\epsilon+1.03\cdot\bar\epsilon^2\Big)\|\ddot x\|^2\\ &\leqslant C_1(U)^2\Big(360+720\Big)\alpha\|\dot x\|^2+\left(1-2\bar\epsilon+1.03\cdot\bar\epsilon^2+\frac{\bar\epsilon^2}{e^3}\right)\|\ddot x\|^2\,.\end{aligned}$$

The claim follows. ■

**Proof** [Proof of Proposition C.4] It follows by combining Corollary C.9 and Lemma C.10 that

$$\operatorname{Hess}\Psi=\operatorname{Hess}\mathcal{P}+\operatorname{Hess}\mathcal{L}\preccurlyeq\begin{pmatrix}C_1(U)^2(K_2(U)+1080)\alpha I & 0\\ 0 & (1-1.95\cdot\bar\epsilon+5\cdot K_2(U)\bar\epsilon^2)I\end{pmatrix}.$$

We use the choice of $\bar\epsilon$ from (114) to bound

$$5\cdot K_2(U)\bar\epsilon^2\overset{(114)}{\leqslant}\frac{5\bar\epsilon}{C_1(U)^2}\leqslant0.05\cdot\bar\epsilon\,,$$

and the claim follows. ■

### C.4. Replica symmetric upper bound

In this subsection we give the proof of Theorem 1.4. We then use this to conclude the proof of the upper bound in Theorem 1.1.

**Proof** [Proof of Theorem 1.4] Recall from (59) that we decomposed $\boldsymbol{Z}(\boldsymbol{G}') = \boldsymbol{Z}_\circ(\boldsymbol{G}') + \boldsymbol{Z}_\bullet(\boldsymbol{G}')$. For $\boldsymbol{Z}_\circ(\boldsymbol{G}')$, we will analyze the bound from Theorem A.12. Note that Lemma A.4 implies

$$\frac{(\mathbf{1}, \log(2\operatorname{ch}(\mathbf{H}^{(t)})))}{N} \overset{N\to\infty}{\longrightarrow} \log 2 + \mathbb{E}\log\operatorname{ch}(\psi^{1/2}Z) \tag{137}$$

in probability. Recalling (109), (110), and (113), and applying Lemma A.4 again, we have

$$\Psi(\pi_*, \varpi_*) = -\frac{\|\varpi_*\|^2}{2(1-q)} + \mathcal{L}(\pi_*, \varpi_*) \overset{N\to\infty}{\longrightarrow} -\frac{\psi(1-q)}{2} + \alpha\mathbb{E}L_q(q^{1/2}Z) \tag{138}$$

in probability, for $L$ as in (26). It follows by comparing (137) and (138) with (29) that

$$\frac{(\mathbf{1}, \log(2\operatorname{ch}(\mathbf{H}^{(t)})))}{N} + \Psi(\pi_*, \varpi_*) \overset{N\to\infty}{\longrightarrow} \mathrm{RS}(\alpha; U) \tag{139}$$

in probability. Next, it follows by combining Lemmas A.22 and A.23 with Hölder's inequality that

$$\begin{aligned} &\mathbf{Q}\bigg(\bigg\{J \in \{-1,+1\}^N : \Big\|\pi(J) - \pi_*\Big\| \geqslant d_1 \text{ and } \Big\|\varpi(J) - \varpi_*\Big\| \geqslant d_2\bigg\}\bigg) \\ &\qquad \leqslant \exp\bigg\{-N\bigg[\vartheta\frac{(1-3q^{1/2})}{8}(d_1)^2 + (1-\vartheta)\frac{(1-8q^{1/2})}{2}(d_2)^2 + o_N(1)\bigg]\bigg\} \end{aligned} \tag{140}$$

for any $\vartheta \in [0,1]$ (having used also that $\pi_* \simeq \dot{\pi}_*$ and $\varpi_* \simeq \dot{\varpi}_*$, which follows from (55) and (56)). On the other hand, if $(\pi, \varpi) \in \boldsymbol{N}_\circ$ (as defined by (57)) with $\|\pi - \pi_*\| \leqslant d_1$ and $\|\varpi - \varpi_*\| \leqslant d_2$, then it follows by combining Lemmas C.2 and C.3 with Proposition C.4 that

$$\begin{aligned} \Psi(\pi, \varpi) - \Psi(\pi_*, \varpi_*) &\leqslant \nabla\Psi(\pi_*, \varpi_*)\begin{pmatrix}\pi - \pi_* \\ \varpi - \varpi_*\end{pmatrix} + \frac{e^7 C_1(U)^2 K_2(U)\alpha}{2}(d_1)^2 + \frac{(1-1.9\bar{\epsilon})}{2}(d_2)^2 \\ &\leqslant o_N(1) + o_t(1) + \frac{e^7 C_1(U)^2 K_2(U)\alpha}{2}(d_1)^2 + \frac{(1-1.9\bar{\epsilon})}{2}(d_2)^2\,. \end{aligned} \tag{141}$$

Let us take $\vartheta = 4\alpha^{1/2}$. Then, for $d_1 \leqslant \|\pi - \pi_*\| \leqslant (1+\alpha)^{1/2}d_1$, combining the $\|\pi - \pi_*\|^2$ terms in (140) and (141) results in

$$-\frac{4\alpha^{1/2}(1-3q^{1/2})}{8} + \frac{e^7 C_1(U)^2 K_2(U)\alpha(1+\alpha)}{2} \overset{(27)}{\leqslant} \bigg(-1 + 3q^{1/2} + \frac{e^7(1+\alpha)}{e^5 C_1(U)}\bigg)\frac{\alpha^{1/2}}{2} \leqslant -\frac{\alpha^{1/2}}{10}\,.$$

For $d_2 \leqslant \|\varpi - \varpi_*\| \leqslant (1+\alpha)^{1/2}d_2$, combining the $\|\varpi - \varpi_*\|^2$ terms in (140) and (141) results in

$$\begin{aligned} &-\frac{(1-4\alpha^{1/2})(1-8q^{1/2})}{2} + \frac{(1+\alpha)(1-1.9\bar{\epsilon})}{2} \overset{(28)}{\leqslant} \Big(2 + 4\cdot 3^{1/2}C_1(U) + \alpha^{1/2}\Big)\alpha^{1/2} - \frac{1.9\cdot\bar{\epsilon}}{2} \\ &\qquad \leqslant 8C_1(U)\alpha^{1/2} - \frac{1.9\cdot\bar{\epsilon}}{2} \overset{(114)}{\leqslant} \bigg(8 - \frac{1.9\cdot e^5}{2}\bigg)C_1(U)\alpha^{1/2} \leqslant -1000\cdot\alpha^{1/2}\,. \end{aligned}$$

Substituting the above bounds into the result of Theorem A.12 gives, with high probability,

$$\frac{\mathbb{E}(\boldsymbol{Z}_\circ(\boldsymbol{G}') \mid \mathscr{F}'(t))}{\exp\{N(\mathrm{RS}(\alpha;U)+o_t(1))\}} \leqslant \sum_{k_1,k_2\geqslant 0} \exp\bigg\{-\frac{N\alpha^{1/2}}{10}\sum_{i=1}^{2}(d_i)^2(1+\alpha)^{k_i}\bigg\} \leqslant O(1)\,.$$

The result follows by combining with the bound on $\boldsymbol{Z}_\bullet(\boldsymbol{G}')$ from Corollary C.1. ■

**Proof** [Proof of Theorem 1.1 upper bound] It follows from Theorem 1.4 and Markov's inequality that for any $\epsilon > 0$,

$$\mathbb{P}\bigg(\frac{1}{N}\log \boldsymbol{Z}(\boldsymbol{G}') \geqslant \mathrm{RS}(\alpha;U)+\epsilon \,\bigg|\, \mathscr{F}'(t)\bigg) \leqslant \frac{\exp(No_t(1))}{\exp(N\epsilon)}\,,$$

with high probability over the randomness of $\mathscr{F}'(t)$. It follows that

$$\mathbb{P}\bigg(\frac{1}{N}\log \boldsymbol{Z}(\boldsymbol{G}') \geqslant \mathrm{RS}(\alpha;U)+\epsilon\bigg) \leqslant o_N(1) + \frac{\exp(No_t(1))}{\exp(N\epsilon)}\,.$$

The left-hand side does not depend on $t$, so it follows that

$$\limsup_{N\to\infty} \frac{1}{N}\log \boldsymbol{Z} \leqslant \mathrm{RS}(\alpha;U)$$

in probability, which gives the upper bound in Theorem 1.1. ■

## Appendix D. Second moment conditional on AMP

In this section we give the proof of Theorem 1.5, our main result on the conditional second moment. From this we will deduce the lower bound in Theorem 1.1 in the bounded case, as explained at the end of this section. The lower bound in the general case will be treated in Section F. Recalling (57), we now restrict further to

$$\boldsymbol{N}_* \equiv \bigg\{(\pi,\varpi) : \max\Big\{\|\pi(J)-\pi_*\|, \|\varpi(J)-\varpi_*\|\Big\} \leqslant o_N(1)\bigg\}\,,$$

so $\boldsymbol{N}_* \subseteq \boldsymbol{N}_\circ$. Then, analogously to (58), we let

$$\mathbb{H}_* \equiv \Big\{J \in \{-1,+1\}^N : (\pi(J),\varpi(J)) \in \boldsymbol{N}_*\Big\}\,, \tag{142}$$

so $\mathbb{H}_* \subseteq \mathbb{H}_\circ$. Analogously to (59), we let

$$\boldsymbol{Z}_*(\boldsymbol{G}) \equiv \sum_{J\in\mathbb{H}_*} \mathrm{S}_J(\boldsymbol{G}) \leqslant \boldsymbol{Z}_\circ(\boldsymbol{G}) \leqslant \boldsymbol{Z}(\boldsymbol{G})\,. \tag{143}$$

We will prove Theorem 1.5 for the random variable

$$\bar{\boldsymbol{Z}}(\boldsymbol{G}) \equiv \sum_{J\in\mathbb{H}_*} \mathrm{S}_J(\boldsymbol{G})\mathbf{1}\bigg\{\frac{\|\boldsymbol{G}\mathbf{v}_J\|^2}{M} \leqslant 5C_1(U)^2\bigg\} \leqslant \boldsymbol{Z}_*(\boldsymbol{G})\,, \tag{144}$$

where $\mathbf{v}_J = J''/\|J''\|$ as in Definition A.8, and $C_1(U)$ is the constant from Lemma B.3. The remainder of this section is organized as follows:

- In §D.1 we prove the first moment lower bound (17), which gives the first assertion of Theorem 1.5.

- In §D.2 we introduce a parameter $\lambda = \lambda(J, K)$ (Definition D.3) which captures the correlation of a pair of configurations $J, K \in \{-1, +1\}^N$. We then prove Theorem D.9 which gives a preliminary bound on the second moment contribution from pairs with small $\lambda$ (see (170)). We also prove Corollary D.10 which bounds the second moment contribution from pairs with larger $\lambda$.

- In §D.3 we further analyze the bound obtained in Theorem D.9. We show in Proposition D.11 that the bound is approximately stationary at $\lambda = 0$, and then in Corollary C.9 we control the second derivative of the bound with respect to $\lambda$.

- In §D.4 we combine the results of the preceding sections to conclude the proof of Theorem 1.5. From this we deduce the lower bound of Theorem 1.1 in the case $\|u\| < \infty$.

The calculation of this section follows a similar outline as that of Sections A and C, so we will point out the parallels throughout. As before, we let $\boldsymbol{G}$ be an independent copy of $\boldsymbol{G}'$.

### D.1. First moment lower bound

In this subsection we prove (17), the first assertion of Theorem 1.5. To this end, we begin with the following result which essentially says that the upper bound of Theorem A.12 is tight in the case $(\pi, \varpi) = (\pi_*, \varpi_*)$.

**Proposition D.1** *Suppose $U$ satisfies Assumptions 1 and 2. Let $\mathscr{F}'(t)$ be as in (25). For $\boldsymbol{Z}_*$ as in (143) we have*

$$\mathbb{E}\Big(\boldsymbol{Z}_*(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big) \geqslant \exp\Big\{N\Big(\mathrm{RS}(\alpha; U) - o_t(1)\Big)\Big\}$$

*with high probability.*

**Proof** Recall from the proof of Proposition A.13 that

$$E_J \equiv \mathbb{E}\Big(\mathrm{S}_J(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big) \overset{(73)}{=} \frac{\boldsymbol{E}_J(\tau\,|\,\bar{g}_{\mathrm{R}}) \cdot \mathbf{p}_{J,\tau}(\bar{g}_{\mathrm{A}}\,|\,\bar{g}_{\mathrm{R}})}{\exp\{N^{1/2}(\tau, \bar{g}_{\mathrm{A}})\} \cdot p_{\mathrm{A}}(\bar{g}_{\mathrm{A}})}\,. \tag{145}$$

If $J \in \mathbb{H}_*$, then it follows from Lemma A.10 that $\acute{\pi}(J) \simeq \acute{\pi}_* \equiv q^{1/2}\acute{e}_{t-1}$, and

$$\frac{\bar{g}_{\mathrm{A}}}{N^{1/2}} \overset{(75)}{=} (\boldsymbol{\Gamma}_N)^{\mathrm{t}}\delta(J) \simeq \frac{1}{(1-q)^{1/2}}\bigg\{\varpi_* - \frac{\psi^{1/2}}{q^{1/2}}(1-q)\boldsymbol{\Gamma}^{\mathrm{t}}\acute{\pi}_*\bigg\} \overset{(56)}{=} \mathbf{0} \in \mathbb{R}^{t-1}\,. \tag{146}$$

Substituting this into the result of Proposition E.13 gives

$$\begin{aligned}\frac{\mathbf{p}_{J,\bar{\tau}}(\bar{g}_{\mathrm{A}}\,|\,\bar{g}_{\mathrm{R}})}{\psi^{1/2}|\det \boldsymbol{\Gamma}_N|} &\simeq \frac{\mathbf{g}_{J,\bar{\tau}}(\bar{g}_{\mathrm{A}})}{\psi^{1/2}|\det \boldsymbol{\Gamma}_N|} \\ &\overset{(204)}{=} g_{J,\bar{\tau}}\bigg(-(N\psi)^{1/2}\bigg[\boldsymbol{\Gamma}_N\bar{\tau} + c(\pi)\frac{\mathbf{n}[t-1]F_{\|\pi\|^2}(\boldsymbol{X}_{J,\bar{\tau}})}{N\psi^{1/2}} + o_N(1)\bigg]\bigg)\,,\end{aligned} \tag{147}$$

for $\boldsymbol{X}_{J,\bar{\tau}}$ as defined by (181). To evaluate the right-hand side above, note that $J \in \mathbb{H}_*$ implies

$$\frac{\boldsymbol{\Gamma}_N \bar{\tau}}{\psi^{1/2}(1-q)^{1/2}} \equiv \frac{\boldsymbol{\Gamma}_N \bar{\tau}(J)}{\psi^{1/2}(1-q)^{1/2}} \overset{(79)}{\simeq} -\frac{\boldsymbol{\Gamma}\varpi_*}{\psi^{1/2}(1-q)} \overset{(56)}{=} -\boldsymbol{\Gamma}\boldsymbol{\Gamma}^{\mathrm{t}} \acute{e}_{t-1} = -\begin{pmatrix} \mu_1 \\ \vdots \\ \mu_{t-2} \\ 1 \end{pmatrix},$$

where the last identity uses (40) and (40). It also implies $\boldsymbol{X}_{J,\bar{\tau}} \simeq \mathbf{h}^{(t+1)}$, and consequently

$$c(\pi)\frac{\mathbf{n}[t-1]F_{\|\pi\|^2}(\boldsymbol{X}_{J,\bar{\tau}})}{N\psi(1-q)^{1/2}} \simeq \frac{\mathbf{n}[t-1]F_q(\mathbf{h}^{(t+1)})}{N\psi} \overset{(42)}{\simeq} \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_{t-2} \\ \mu_{t-1} \end{pmatrix}.$$

Note moreover that Proposition A.6 and Lemma B.11 together imply $\mu_{t-1} = 1 - o_t(1)$. Substituting these calculations into (147) gives (cf. (74))

$$\mathbf{p}_{J,\bar{\tau}}(\bar{g}_{\mathrm{A}} \mid \bar{g}_{\mathrm{R}}) \simeq \psi^{1/2} |\det \boldsymbol{\Gamma}_N| g_{J,\bar{\tau}} \left( (N\psi)^{1/2} \begin{pmatrix} o_N(1) \\ \vdots \\ o_N(1) \\ o_t(1) \end{pmatrix} \right) = \exp\{N o_t(1)\}\,. \tag{148}$$

Substituting (76), (77), and (148) into (145) gives (cf. (78))

$$E_J = \exp\left\{ N\Big[ \tilde{A}_J(\bar{\tau}) + o_t(1) \Big] \right\}.$$

It then follows from the proof of Theorem A.12 that (cf. (82))

$$\frac{\mathbb{E}(\boldsymbol{Z}_*(\boldsymbol{G}') \mid \mathscr{F}'(t))}{\exp\{(\mathbf{1}, \log(2\,\mathrm{ch}(\mathbf{H}^{(t)})))\}} = \mathbf{Q}(\mathbb{H}_*) \exp\left\{ N\Big[ \Psi(\pi_*, \varpi_*) + o_t(1) \Big] \right\}. \tag{149}$$

We have $\mathbf{Q}(\mathbb{H}_*) \simeq 1$ by the law of large numbers, so the claim follows by recalling (139). ■

To finish the proof of (17), it remains only to account for the restriction on $\|\boldsymbol{G}\mathbf{v}\|$ in (144):
**Proof** [Proof of first moment lower bound (17)] We begin with an easy large deviations calculation. If $\zeta$ is a standard gaussian random variable, then it is well known that $\zeta^2/2$ is a gamma random variable with shape parameter $1/2$, and moment-generating function

$$\mathbb{E}\exp\left(\frac{\theta\zeta^2}{2}\right) = \int_0^\infty \frac{e^{-(1-\theta)x}}{2\pi^{1/2}x^{1/2}}\,dx = \frac{1}{(1-\theta)^{1/2}},$$

for any $\theta < 1$. If $\boldsymbol{\zeta}$ is a standard gaussian random vector in $\mathbb{R}^M$, then for any $L > 1$ we have

$$\begin{aligned} \mathbb{P}\left( \frac{\|\boldsymbol{\zeta}\|^2}{M} \geqslant L \right) &\leqslant \exp\left\{ -\frac{M}{2} \sup\left\{ \log(1-\theta) + L\theta : \theta \in [0,1) \right\} \right\} \\ &\leqslant \exp\left\{ -\frac{M}{2}\Big[ L - \log L - 1 \Big] \right\}. \end{aligned} \tag{150}$$

Now, recalling (143) and (144), let us take $L \equiv L_1(U) \equiv 5C_1(U)^2 \geqslant 500$ and define

$$\boldsymbol{Z}''(\boldsymbol{G}') \equiv \boldsymbol{Z}_*(\boldsymbol{G}') - \bar{\boldsymbol{Z}}(\boldsymbol{G}') \equiv \sum_J \mathrm{S}_J(\boldsymbol{G}')\mathbf{1}\bigg\{\frac{\|\boldsymbol{G}'\mathbf{v}_J\|^2}{M} > L\bigg\}. \tag{151}$$

It follows from Lemmas A.16 and A.19 that

$$\begin{aligned}\mathbb{E}\Big(\boldsymbol{Z}''(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big) &= \mathbb{E}\Big(\boldsymbol{Z}''(\boldsymbol{G})\,\Big|\,\mathscr{H}'(t), \mathrm{R}, \mathrm{A}, (\boldsymbol{G}')_{\mathrm{RA}}\Big)\\ &\leqslant \sum_J \mathbb{P}\bigg(\frac{\|\boldsymbol{G}\mathbf{v}_J\|^2}{M} > L\,\bigg|\,\mathscr{H}'(t), \mathrm{R}, \mathrm{A}, (\boldsymbol{G}')_{\mathrm{RA}}\bigg).\end{aligned}$$

Recall from Definition A.14 that $V_{\mathrm{C}}$ denotes the span of the vectors $\mathbf{c}^{(\ell)}$ for $\ell \leqslant t-1$. Let us decompose $\boldsymbol{G}\mathbf{v}_J \in \mathbb{R}^M$ as $(\boldsymbol{G}\mathbf{v}_J)^{\|} + (\boldsymbol{G}\mathbf{v}_J)^{\perp}$ where $(\boldsymbol{G}\mathbf{v}_J)^{\|}$ is the orthogonal projection of $\boldsymbol{G}\mathbf{v}_J$ onto $V_{\mathrm{C}}$. Conditional on the events R and A, $(\boldsymbol{G}\mathbf{v}_J)^{\|}$ is fixed by the admissibility condition (see (51), (62), and (75)), while $(\boldsymbol{G}\mathbf{v}_J)^{\perp}$ behaves as an independent standard gaussian random vector in the orthogonal complement of $V_{\mathrm{C}}$. It follows that, conditional on R and A, $\|\boldsymbol{G}\mathbf{v}_J\|^2/M$ is equidistributed as

$$\frac{N\|(\boldsymbol{\Gamma}_N)^{\mathrm{t}}\delta\|}{M} + \frac{\|\boldsymbol{\zeta}'\|^2}{M} = o_N(1) + \frac{\|\boldsymbol{\zeta}'\|^2}{M},$$

where $\boldsymbol{\zeta}'$ is a standard gaussian random vector in $\mathbb{R}^{M-\ell-1}$. It follows by applying (150) that

$$\begin{aligned}\mathbb{E}\Big(\boldsymbol{Z}''(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big) &\leqslant 2^N \mathbb{P}\bigg(\frac{\|\boldsymbol{\zeta}\|^2}{M} + o_N(1) \geqslant L\bigg) \leqslant \exp\bigg\{N\bigg[\log 2 - \frac{5\alpha C_1(U)^2}{3}\bigg]\bigg\}\\ &\leqslant \exp\bigg\{N\bigg[\mathrm{RS}(\alpha; U) - \frac{\alpha C_1(U)^2}{10}\bigg]\bigg\},\end{aligned}$$

where the last bound uses the result of Corollary B.8. Combining with the result of Proposition D.1 gives

$$\begin{aligned}\mathbb{E}\Big(\bar{\boldsymbol{Z}}(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big) &\geqslant \mathbb{E}\Big(\boldsymbol{Z}_*(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big) - \mathbb{E}\Big(\boldsymbol{Z}''(\boldsymbol{G}')\,\Big|\,\mathscr{F}'(t)\Big)\\ &\geqslant \exp\Big\{N\Big(\mathrm{RS}(\alpha; U) - o_t(1)\Big)\Big\},\end{aligned}$$

with high probability. ■

### D.2. Expected weight of a correlated pair

**Definition D.2** *Recall the function $\boldsymbol{S}_J(\mathrm{g_R}, \mathrm{g_A}, \mathrm{g_B})$ from (69). Moreover recall that by (66) and (67) combined, the pair $(\mathrm{g_A}, \mathrm{g_B})$ is equivalent to $\mathrm{g_P} \equiv \boldsymbol{G}\mathbf{v}$. We let $\mathbb{Q}_J(\cdot)$ denote the measure on $\mathbb{R}^M$ such that*

$$\mathbb{Q}_J(B) = \frac{\mathbb{E}(\mathrm{S}_J(\boldsymbol{G})\mathbf{1}\{\boldsymbol{G}\mathbf{v} \in B\} \mid \mathscr{H}'(t), \mathrm{R}, \mathrm{A})}{\mathbb{E}(\mathrm{S}_J(\boldsymbol{G}) \mid \mathscr{H}'(t), \mathrm{R}, \mathrm{A})} = \frac{\mathbb{E}(\boldsymbol{S}_J(\bar{g}_\mathrm{R}, \bar{g}_\mathrm{A}, \mathrm{g_B})\mathbf{1}\{(\bar{g}_\mathrm{A}, \mathrm{g_B}) \in B\})}{\mathbb{E}(\boldsymbol{S}_J \mid \bar{g}_\mathrm{R}, \bar{g}_\mathrm{A}, \mathrm{g_B}))}.$$

*Note that $\mathbb{Q}_J$ depends on $\bar{g}_\mathrm{R}$ and $\bar{g}_\mathrm{A}$, where $\bar{g}_\mathrm{R}$ does not depend on $J$, but $\bar{g}_\mathrm{A}$ does.*

**Definition D.3 (analogous to Definition A.7)** *Let $J, K \in \{-1,+1\}^N$. Recall from Definition A.7 that we decompose $J = J' + J''$ where $J'$ is the orthogonal projection of $J$ onto the span of the vectors $\mathbf{m}^{(s)}$, $1 \leqslant s \leqslant t$. Analogously decompose $K = K' + K''$. Recall that $\mathbf{v} \equiv J''/\|J''\|$, and define analogously $\mathbf{v}_K \equiv K''/\|K''\|$. Then let*

$$\lambda(J,K) \equiv \left( \frac{J''}{\|J''\|}, \frac{K''}{\|K''\|} \right) = (\mathbf{v}, \mathbf{v}_K)\,,$$

*so clearly we have $-1 \leqslant \lambda(J,K) \leqslant 1$. We further denote*

$$\mathbf{w} \equiv \frac{K'' - (K'', \mathbf{v})\mathbf{v}}{\|K'' - (K'',\mathbf{v})\mathbf{v}\|} \simeq \frac{\mathbf{v}_K - \lambda \mathbf{v}}{(1-\lambda^2)^{1/2}}\,, \tag{152}$$

*so $\mathbf{w}$ is a unit vector in $\mathbb{R}^N$ orthogonal to $\mathbf{v}$.*

**Definition D.4 (analogous to Definition A.17)** *Given $\mathscr{F}'(t)$ as in (25), and $J, K \in \{-1,+1\}^N$, recall from Definition D.3 that we decompose $J = J' + J''$ and $K = K' + K''$, and define corresponding unit vectors $\mathbf{v}$ and $\mathbf{w}$. Let*

$$V_{\mathrm{P}(K)} \equiv \operatorname{span}\left\{ \mathbf{e}_a \mathbf{w}^{\mathrm{t}} : 1 \leqslant a \leqslant M \right\},$$
$$V_{\mathrm{A}(K)} \equiv \operatorname{span}\left\{ \mathbf{n}^{(\ell)} \mathbf{w}^{\mathrm{t}} : 1 \leqslant \ell \leqslant t-1 \right\}.$$

*Note $V_{\mathrm{A}(K)}$ is a subspace of $V_{\mathrm{P}(K)}$, and is also a subspace of the space $V_{\mathrm{C}}$ from Definition A.14. Let $\operatorname{proj}_{\mathrm{A}(K)}$ denote the orthogonal projection onto $V_{\mathrm{A}(K)}$, and note that $(\boldsymbol{G}')_{\mathrm{A}(K)} \equiv \operatorname{proj}_{\mathrm{A}(K)}(\boldsymbol{G}')$ is measurable with respect to $\mathscr{F}'(t)$.*

**Definition D.5 (analogous to Definition A.18)** *As before, let $\boldsymbol{G}$ be an independent copy of $\boldsymbol{G}'$. Let*

$$\mathrm{A}(K) \equiv \left\{ \operatorname{proj}_{\mathrm{A}(K)}(\boldsymbol{G}) = (\boldsymbol{G}')_{\mathrm{A}(K)} \right\} \overset{(61)}{=} \left\{ \frac{\mathbf{n}[t-1]\boldsymbol{G}\mathbf{w}}{N\psi^{1/2}} = \frac{\mathbf{H}[t-1]\mathbf{w}}{(N\psi)^{1/2}} \right\}, \tag{153}$$

*where the last identity holds assuming that the event $\mathrm{C}$ from (61) occurs.*

**Definition D.6 (extension of Definition A.11)** *We now let $\mathbf{P}$ denote the uniform probability measure over pairs $(J,K) \in (\{-1,+1\}^N)^2$, and let $\mathbf{Q}$ be the probability measure on the same space which is given by*

$$\frac{d\mathbf{Q}}{d\mathbf{P}} = \frac{\exp\{(\mathbf{H}^{(t)}, J+K)\}}{\exp\{2\cdot(\mathbf{1}, \log\operatorname{ch}\mathbf{H}^{(t)})\}}\,.$$

*Note that $J$ and $K$ are independent under $\mathbf{Q}$, and each has mean $\mathbf{m}^{(t)}$.*

**Proposition D.7 (analogous to Proposition A.13)** *For $\boldsymbol{\zeta} \in \mathbb{R}^M$ define*

$$\mathcal{A}_2(\lambda\,|\,\boldsymbol{\zeta}) \equiv \frac{\psi(1-q)}{2(1-\lambda^2)} + \frac{1}{N}\left( \mathbf{1}, L_{q+\lambda^2(1-q)}\left( \mathbf{h}^{(t+1)} + (1-q)^{1/2}\lambda\boldsymbol{\zeta} \right) \right).$$

*Then, for $J, K \in \mathbb{H}_*$, we have*

$$\frac{\mathbb{E}(\mathrm{S}_J(\boldsymbol{G}')\mathrm{S}_K(\boldsymbol{G}')\mathbf{1}\{\|\boldsymbol{G}'\mathbf{v}\|^2/M \leqslant L\}\,|\,\mathscr{F}'(t))}{\mathbb{E}(\mathrm{S}_J(\boldsymbol{G}')\,|\,\mathscr{F}'(t))} \leqslant \int \mathbf{1}\left\{ \frac{\|\boldsymbol{\zeta}\|^2}{M} \leqslant L \right\} \exp\{N\mathcal{A}_2(\lambda\,|\,\boldsymbol{\zeta})\}\,\mathbb{Q}_J(d\boldsymbol{\zeta})$$

*with $\mathbb{Q}_J$ as in Definition D.2, and $\lambda = \lambda(J,K)$ as in Definition D.3.*

In preparation for the proof of Proposition D.7, we record the following calculation:

**Lemma D.8 (analogous to Lemma A.21)** *For spin configurations $J, K \in \{-1,+1\}^N$ and a vector $\boldsymbol{\zeta} \in \mathbb{R}^M$, define the cumulant-generating function*

$$\tilde{\mathcal{K}}_{K|J}(\tau\,|\,\boldsymbol{\zeta}) \equiv \frac{1}{N}\log\mathbb{E}\bigg(\mathrm{S}_K(\boldsymbol{G})\exp\Big\{N^{1/2}\tau^{\mathrm{t}}\mathbf{c}[t-1]\boldsymbol{G}\mathbf{w}\Big\}\,\bigg|\,\mathscr{H}'(t),\mathrm{R},(\boldsymbol{G}')_{\mathrm{R}},\boldsymbol{G}\mathbf{v}=\boldsymbol{\zeta}\bigg)$$

*for $\tau \in \mathbb{R}^{t-1}$. Next, with $L$ as in (26) and with $\tilde{\boldsymbol{X}}_K$ as defined by Lemma A.20, define*

$$\tilde{\mathcal{L}}_{K|J}(\tau\,|\,\boldsymbol{\zeta}) \equiv \frac{1}{N}\bigg(\mathbf{1}, L_{\|\pi(K)\|^2(1-\lambda^2)+\lambda^2}\bigg(\tilde{\boldsymbol{X}}_K + c(\pi(K))\Big[\lambda\boldsymbol{\zeta} + (1-\lambda^2)^{1/2}N^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\tau\Big]\bigg)\bigg)\,, \tag{154}$$

*where $c(\pi(K)) \equiv (1-\|\pi(K)\|^2)^{1/2}$. Then the function $\tilde{\mathcal{K}}_{K|J}$ satisfies*

$$\tilde{\mathcal{K}}_{K|J}(\tau\,|\,\boldsymbol{\zeta}) = \frac{\|\tau\|^2}{2} + \tilde{\mathcal{L}}_{K|J}(\tau\,|\,\boldsymbol{\zeta})\,.$$

**Proof** Conditional on the event R, it follows from Lemma A.20 that $\boldsymbol{G}K'/N^{1/2} = \tilde{\boldsymbol{X}}_K \equiv \tilde{\boldsymbol{X}}$. We also have

$$\frac{\boldsymbol{G}K''}{N^{1/2}} = \frac{\|K''\|}{N^{1/2}}\boldsymbol{G}\mathbf{v}_K = c(\pi(K))\Big(\lambda\boldsymbol{\zeta} + (1-\lambda^2)^{1/2}\boldsymbol{\xi}\Big)\,, \tag{155}$$

where $\boldsymbol{\xi} = \boldsymbol{G}\mathbf{w}$ is distributed as an independent gaussian vector in $\mathbb{R}^N$. Thus

$$\tilde{\mathcal{K}}_{K|J}(\tau\,|\,\boldsymbol{\zeta}) = \frac{1}{N}\sum_{a\leqslant M}\log\mathbb{E}_\xi\bigg[\exp\Big\{N^{1/2}\sum_{\ell\leqslant t-1}\tau_\ell(\mathbf{c}^{(\ell)})_a\xi\Big\} \times U\Big(\tilde{\boldsymbol{X}}_a + c(\pi(K))\Big\{\lambda\boldsymbol{\zeta}_a + (1-\lambda^2)^{1/2}\xi\Big\}\Big)\bigg]\,,$$

where $\xi$ denotes a standard gaussian random variable. Making a change of variable gives

$$\tilde{\mathcal{K}}_{K|J}(\tau\,|\,\boldsymbol{\zeta}) = \frac{\|\tau\|^2}{2} + \frac{1}{N}\sum_{a\leqslant M}\log\mathbb{E}_\xi U\bigg(\tilde{\boldsymbol{X}}_a + c(\pi(K))\Big\{\lambda\boldsymbol{\zeta}_a + (1-\lambda^2)^{1/2}\Big[\xi + N^{1/2}\sum_{\ell\leqslant t-1}\tau_\ell(\mathbf{c}^{(\ell)})_a\Big]\Big\}\bigg)\,,$$

from which the result follows. ■

**Proof** [Proof of Proposition D.7] We follow a very similar outline as in the proof of Proposition A.13. As in (151) above, let us write $L = 5C_1(U)^2$. Given $\mathscr{F}'(t)$ as in (25) and $J, K \in \{-1,+1\}^N$, we abbreviate the quantity of interest as

$$E_{J,K} \equiv \mathbb{E}\bigg(\mathrm{S}_J(\boldsymbol{G}')\mathrm{S}_K(\boldsymbol{G}')\mathbf{1}\Big\{\frac{\|\boldsymbol{G}'\mathbf{v}\|^2}{M} \leqslant L\Big\}\,\bigg|\,\mathscr{F}'(t)\bigg)\,. \tag{156}$$

It follows by the obvious generalization of Lemma A.16 that

$$E_{J,K} = \mathbb{E}\left( \mathrm{S}_J(\boldsymbol{G})\mathrm{S}_K(\boldsymbol{G})\mathbf{1}\left\{ \frac{\|\boldsymbol{G}\mathbf{v}\|^2}{M} \leqslant L \right\} \,\middle|\, \mathscr{H}'(t), \mathrm{R}, \mathrm{C}, (\boldsymbol{G}')_{\mathrm{RC}} \right),$$

where $\boldsymbol{G}$ is an independent copy of $\boldsymbol{G}'$. Next, the obvious generalization of Lemma A.19 gives the simplification

$$E_{J,K} = \mathbb{E}\left( \mathrm{S}_J(\boldsymbol{G})\mathrm{S}_K(\boldsymbol{G})\mathbf{1}\left\{ \frac{\|\boldsymbol{G}\mathbf{v}\|^2}{M} \leqslant L \right\} \,\middle|\, \mathscr{H}'(t), \mathrm{R}, \mathrm{A}, \mathrm{A}(K), (\boldsymbol{G}')_{\mathrm{RAA}(K)} \right),$$

where A and $\mathrm{A}(K)$ are as in Definition A.18 and Definition D.5 respectively. By the law of iterated expectations,

$$\begin{aligned} E_{J,K} = \mathbb{E}\Bigg( &\mathrm{S}_J(\boldsymbol{G})\mathbf{1}\left\{ \frac{\|\boldsymbol{G}\mathbf{v}\|^2}{M} \leqslant L \right\} \\ &\times \mathbb{E}\Big[ \mathrm{S}_K(\boldsymbol{G}) \,\Big|\, \mathscr{H}'(t), \mathrm{R}, \boldsymbol{G}\mathbf{v}, \mathrm{A}(K), (\boldsymbol{G}')_{\mathrm{RAA}(K)} \Big] \,\Bigg|\, \mathscr{H}'(t), \mathrm{R}, \mathrm{A}, (\boldsymbol{G}')_{\mathrm{RA}} \Bigg). \end{aligned} \tag{157}$$

We therefore first consider the calculation of the inner term

$$E_{K|J}(\boldsymbol{\zeta}) \equiv \mathbb{E}\left( \mathrm{S}_K(\boldsymbol{G}) \,\middle|\, \mathscr{H}'(t), \mathrm{R}, \boldsymbol{G}\mathbf{v} = \boldsymbol{\zeta}, \mathrm{A}(K), (\boldsymbol{G}')_{\mathrm{RAA}(K)} \right) \tag{158}$$

(where we assume that $\boldsymbol{\zeta}$ satisfies the constraints imposed by A).

Towards the calculation of (158), recall the notation of Definition D.4, and let $V_{\mathrm{P}(K)\setminus\mathrm{A}(K)}$ be the orthogonal complement of $V_{\mathrm{A}(K)}$ inside $V_{\mathrm{P}(K)}$. Analogously to (65) and (66), define $\mathbf{g}_{\mathrm{P}(K)}$ and $\mathbf{g}_{\mathrm{A}(K)}$, for instance

$$\mathbf{g}_{\mathrm{A}(K)} \equiv \left( (\boldsymbol{G}, \mathbf{c}^{(\ell)}\mathbf{w}^{\mathrm{t}}) : 1 \leqslant \ell \leqslant t-1 \right) = \mathbf{c}[t-1]\boldsymbol{G}\mathbf{w} \in \mathbb{R}^{t-1}. \tag{159}$$

Choose an orthonormal basis for $V_{\mathrm{P}(K)\setminus\mathrm{A}(K)}$, and denote it $\boldsymbol{B}_j(K)$ for $1 \leqslant j \leqslant M-(t-1)$. Analogously to (67), let

$$\mathbf{g}_{\mathrm{B}(K)} \equiv \left( (\boldsymbol{G}, \boldsymbol{B}_j(K)) : 1 \leqslant j \leqslant M-(t-1) \right) \in \mathbb{R}^{M-t+1}.$$

Note that there is an orthogonal transformation of $\mathbb{R}^M$ which maps $\mathbf{g}_{\mathrm{P}(K)}$ to the pair $(\mathbf{g}_{\mathrm{A}(K)}, \mathbf{g}_{\mathrm{B}(K)})$.

The weight $\mathrm{S}_K(\boldsymbol{G})$, as defined by (23), is a function of $\boldsymbol{G}K$, which we decomposed in the proof of Lemma D.8 as a sum of $\boldsymbol{G}K'$ and $\boldsymbol{G}K''$. Recall that $\boldsymbol{G}K'$ is a function of $\mathbf{g}_{\mathrm{R}}$. Meanwhile (see e.g. (155)) $\boldsymbol{G}K''$ is a linear combination of $\mathbf{g}_{\mathrm{P}} = \boldsymbol{G}\mathbf{v} = \boldsymbol{\zeta}$ and $\mathbf{g}_{\mathrm{P}(K)} = \boldsymbol{G}\mathbf{w}$, where $\mathbf{g}_{\mathrm{P}(K)}$ is equivalent to the pair $(\mathbf{g}_{\mathrm{A}(K)}, \mathbf{g}_{\mathrm{B}(K)})$ as noted above. Thus $\mathrm{S}_K(\boldsymbol{G})$ can be rewritten as a function $\boldsymbol{S}_{K|J}$ of $(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{P}}, \mathbf{g}_{\mathrm{A}(K)}, \mathbf{g}_{\mathrm{B}(K)})$: explicitly,

$$\begin{aligned} \mathrm{S}_K(\boldsymbol{G}) &= \prod_{a \leqslant M} U\left( \sum_{s \leqslant t} \frac{(K, \mathbf{r}^{(s)})}{N^{1/2}} (\mathbf{g}_{\mathrm{R}})_{a,s} + \frac{\|K''\|}{N^{1/2}} \Big( \lambda(\mathbf{g}_{\mathrm{P}})_a + (1-\lambda^2)^{1/2} (\mathbf{g}_{\mathrm{P}(K)})_a \Big) \right) \\ &\equiv \boldsymbol{S}_{K|J}(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{P}}, \mathbf{g}_{\mathrm{A}(K)}, \mathbf{g}_{\mathrm{B}(K)}), \end{aligned}$$

with $\lambda \equiv \lambda(J,K)$ as given by Definition D.3. On the event $\mathrm{A}(K)$, the value of $\mathbf{g}_{\mathrm{A}(K)}$ is fixed to a value $\bar{g}_{\mathrm{A}(K)}$. We then introduce a parameter $\tau \in \mathbb{R}^{t-1}$, and define (analogously to (69))

$$\begin{aligned}\mathrm{S}_{K|J,\tau}(\boldsymbol{G}) &\equiv \boldsymbol{S}_{K|J,\tau}(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{P}}, \mathbf{g}_{\mathrm{A}(K)}, \mathbf{g}_{\mathrm{B}(K)}) \\ &\equiv \boldsymbol{S}_{K|J}(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{P}}, \mathbf{g}_{\mathrm{A}(K)}, \mathbf{g}_{\mathrm{B}(K)}) \exp\left\{ N^{1/2}(\tau, \mathbf{g}_{\mathrm{A}(K)}) \right\}.\end{aligned}$$

Then, analogously to (70), for any $\tau \in \mathbb{R}^{t-1}$ we can rewrite (158) as

$$\begin{aligned}E_{K|J}(\boldsymbol{\zeta}) &= \mathbb{E}\left( \frac{\boldsymbol{S}_{K|J,\tau}(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{P}}, \mathbf{g}_{\mathrm{A}(K)}, \mathbf{g}_{\mathrm{B}(K)})}{\exp\{N^{1/2}(\tau, \bar{g}_{\mathrm{A}(K)})\}} \,\middle|\, (\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{P}}, \mathbf{g}_{\mathrm{A}(K)}) = (\bar{g}_{\mathrm{R}}, \boldsymbol{\zeta}, \bar{g}_{\mathrm{A}(K)}) \right) \\ &= \frac{1}{\exp\{N^{1/2}(\tau, \bar{g}_{\mathrm{A}(K)})\}} \int \boldsymbol{S}_{K|J,\tau}(\bar{g}_{\mathrm{R}}, \boldsymbol{\zeta}, \bar{g}_{\mathrm{A}(K)}, g_{\mathrm{B}(K)}) p_{\mathrm{B}(K)}(g_{\mathrm{B}(K)})\, dg_{\mathrm{B}(K)}\,. \end{aligned} \tag{160}$$

By contrast, the expected value of $\mathrm{S}_{K|J,\tau}$ given only the row constraints is (cf. (71))

$$\begin{aligned}\boldsymbol{E}_{K|J}(\tau \,|\, \bar{g}_{\mathrm{R}}, \boldsymbol{\zeta}) &\equiv \mathbb{E}\left( \mathrm{S}_{K|J,\tau}(\boldsymbol{G}) \,\middle|\, \mathscr{H}'(t), \mathrm{R}, \boldsymbol{G}\mathbf{v} = \boldsymbol{\zeta}, (\boldsymbol{G}')_{\mathrm{R}} \right) \\ &= \mathbb{E}\left( \boldsymbol{S}_{K|J,\tau}(\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{P}}, \mathbf{g}_{\mathrm{A}(K)}, \mathbf{g}_{\mathrm{B}(K)}) \,\middle|\, (\mathbf{g}_{\mathrm{R}}, \mathbf{g}_{\mathrm{P}}) = (\bar{g}_{\mathrm{R}}, \boldsymbol{\zeta}) \right) \\ &= \int p_{\mathrm{A}(K)}(g_{\mathrm{A}(K)}) \int \boldsymbol{S}_{K|J,\tau}(\bar{g}_{\mathrm{R}}, \boldsymbol{\zeta}, g_{\mathrm{A}(K)}, g_{\mathrm{B}(K)}) p_{\mathrm{B}(K)}(g_{\mathrm{B}(K)})\, dg_{\mathrm{B}(K)}\, dg_{\mathrm{A}(K)} \\ &= \exp\left\{ N\tilde{\mathcal{K}}_{K|J}(\tau \,|\, \boldsymbol{\zeta}) \right\}. \end{aligned} \tag{161}$$

Then, analogously to (72), we define the probability density function

$$\begin{aligned}\mathbf{p}_{K|J,\tau}(g_{\mathrm{A}(K)} \,|\, \bar{g}_{\mathrm{R}}, \boldsymbol{\zeta})\, dg_{\mathrm{A}(K)} &\equiv \frac{\mathbb{E}(\mathrm{S}_{K|J,\tau}(\boldsymbol{G}) \mathbf{1}\{\mathbf{g}_{\mathrm{A}(K)} \in dg_{\mathrm{A}(K)}\} \,|\, \mathscr{H}'(t), \mathrm{R}, \boldsymbol{G}\mathbf{v} = \boldsymbol{\zeta}, (\boldsymbol{G}')_{\mathrm{R}})}{\mathbb{E}(\mathrm{S}_{K|J,\tau}(\boldsymbol{G}) \,|\, \mathscr{H}'(t), \mathrm{R}, \boldsymbol{G}\mathbf{v} = \boldsymbol{\zeta}, (\boldsymbol{G}')_{\mathrm{R}})} \\ &= \frac{p_{\mathrm{A}(K)}(g_{\mathrm{A}(K)})}{\boldsymbol{E}_{K|J}(\tau \,|\, \bar{g}_{\mathrm{R}}, \boldsymbol{\zeta})} \left[ \int \boldsymbol{S}_{K|J,\tau}(\bar{g}_{\mathrm{R}}, \boldsymbol{\zeta}, g_{\mathrm{A}(K)}, g_{\mathrm{B}(K)}) p_{\mathrm{B}(K)}(g_{\mathrm{B}(K)})\, dg_{\mathrm{B}(K)} \right] dg_{\mathrm{A}(K)}\,. \end{aligned} \tag{162}$$

Then it follows similarly to (73) that we can rewrite (160) as

$$E_{K|J}(\boldsymbol{\zeta}) = \frac{\boldsymbol{E}_{K|J}(\tau \,|\, \bar{g}_{\mathrm{R}}, \boldsymbol{\zeta}) \cdot \mathbf{p}_{K|J,\tau}(\bar{g}_{\mathrm{A}(K)} \,|\, \bar{g}_{\mathrm{R}}, \boldsymbol{\zeta})}{\exp\{N^{1/2}(\tau, \bar{g}_{\mathrm{A}(K)})\} \cdot p_{\mathrm{A}(K)}(\bar{g}_{\mathrm{A}(K)})}\,. \tag{163}$$

We will show in Proposition E.14 (deferred to Section E) that (cf. (74))

$$\max\left\{ \left\| \mathbf{p}_{K|J,\tau}(\cdot \,|\, \bar{g}_{\mathrm{R}}) \right\|_{\infty} : J \in \{-1,+1\}^N, \|\pi(J)\| \leqslant \frac{4}{5}, |\lambda| \leqslant \frac{4}{5}, \|\tau\| \leqslant \tau_{\max} \right\} \leqslant \wp_{t,2}\,. \tag{164}$$

It therefore remains to estimate the other two terms on the right-hand side of (163). We then note that Definition D.5 implies that, on the event $\mathrm{A}(K)$, we have (cf. (75))

$$\begin{aligned}\frac{\bar{g}_{\mathrm{A}(K)}}{N^{1/2}} &\overset{(159)}{=} \frac{\mathbf{c}[t-1]\boldsymbol{G}\mathbf{w}}{N^{1/2}} \overset{(44)}{=} \frac{(\boldsymbol{\Gamma}_N)^{-1}\mathbf{n}[t-1]\boldsymbol{G}\mathbf{w}}{N\psi^{1/2}} \overset{(153)}{=} \frac{(\boldsymbol{\Gamma}_N)^{-1}\mathbf{H}[t-1]\mathbf{w}}{(N\psi)^{1/2}} \\ &\overset{(152)}{=} \frac{(\boldsymbol{\Gamma}_N)^{-1}\mathbf{H}[t-1]}{(N\psi)^{1/2}} \left( \frac{\mathbf{v}_K - \lambda\mathbf{v}}{(1-\lambda^2)^{1/2}} \right) \overset{(51)}{=} \frac{(\boldsymbol{\Gamma}_N)^{\mathrm{t}}[\delta(K) - \lambda\delta(J)]}{(1-\lambda^2)^{1/2}} = o_N(1)\,, \end{aligned} \tag{165}$$

where the last estimate holds thanks to the restriction $J, K \in \mathbb{H}_*$ (see (146)). Substituting (165) into the formula for $p_{\mathrm{A}(K)}$ (similar to (76)) gives

$$p_{\mathrm{A}(K)}(\bar{g}_{\mathrm{A}(K)}) = \frac{1}{(2\pi)^{(t-1)/2}} \exp\bigg\{ -\frac{N}{2}\bigg\| \frac{(\boldsymbol{\Gamma}_N)^{\mathrm{t}}[\delta(K) - \lambda\delta(J)]}{(1-\lambda^2)^{1/2}} \bigg\|^2 \bigg\} = \exp\{N \cdot o_N(1)\}\,. \quad (166)$$

Meanwhile, it follows by combining (161) and (165) that (cf. (77))

$$\frac{\boldsymbol{E}_{K|J}(\tau\,|\,\bar{g}_{\mathrm{R}}, \boldsymbol{\zeta})}{\exp\{N^{1/2}(\tau, \bar{g}_{\mathrm{A}(K)})\}} \leqslant \exp\bigg\{ N\bigg[ \breve{\mathcal{K}}_{K|J}(\tau\,|\,\boldsymbol{\zeta}) - \bigg(\tau, \frac{(\boldsymbol{\Gamma}_N)^{\mathrm{t}}[\delta(K) - \lambda\delta(J)]}{(1-\lambda^2)^{1/2}}\bigg) + o_N(1) \bigg]\bigg\} \quad (167)$$

Substituting (164), (166), and (167) into (163), and combining with Lemma D.8, gives (cf. (78))

$$\frac{E_{K|J}(\boldsymbol{\zeta})}{\wp_{t,2}(2\pi)^{t/2}} \leqslant \exp\bigg\{ N\bigg[ \bigg( \frac{1}{2}\bigg\| \tau - \frac{(\boldsymbol{\Gamma}_N)^{\mathrm{t}}[\delta(K) - \lambda\delta(J)]}{(1-\lambda^2)^{1/2}} \bigg\|^2 + \tilde{\mathcal{L}}_{K|J}(\tau\,|\,\boldsymbol{\zeta}) \bigg) + o_N(1) \bigg]\bigg\}\,. \quad (168)$$

To simplify the above expression, we set $\tau = \bar{\tau}(\lambda)$ where

$$\bar{\tau}(\lambda) \equiv \frac{\varpi_*}{(1-q)^{1/2}(1-\lambda^2)^{1/2}} \overset{(110)}{=} -\frac{\psi^{1/2}(1-q)^{1/2}}{(1-\lambda^2)^{1/2}} \boldsymbol{\Gamma}^{\mathrm{t}} \acute{e}_{t-1}\,.$$

Substituting this into (154), and recalling the definition of $\tilde{\boldsymbol{X}}_K$ from Lemma A.20, we obtain

$$\tilde{\mathcal{L}}_{K|J}(\bar{\tau}(\lambda)\,|\,\boldsymbol{\zeta}) \simeq \frac{1}{N}\Big( \mathbf{1}, L_{q(1-\lambda^2)+\lambda^2}\Big( \mathbf{h}^{(t+1)} + (1-q)^{1/2}\lambda\boldsymbol{\zeta} \Big)\Big) + o_N(1) \equiv \mathcal{L}_2(\lambda\,|\,\boldsymbol{\zeta})\,, \quad (169)$$

where $\mathcal{L}_2$ is defined by the last identity. By substituting the above into (168), we see that the quantity from (158) can be upper bounded by

$$E_{K|J}(\boldsymbol{\zeta}) \leqslant \exp\bigg\{ N\bigg[ \frac{\psi(1-q)}{2(1-\lambda^2)} + \mathcal{L}_2(\lambda\,|\,\boldsymbol{\zeta}) + o_N(1) \bigg]\bigg\} = \exp\Big\{ N\Big[ \mathcal{A}_2(\lambda\,|\,\boldsymbol{\zeta}) + o_N(1) \Big]\Big\}\,,$$

for $\mathcal{A}_2(\lambda\,|\,\boldsymbol{\zeta})$ as in the statement of the proposition. By comparing (157) with (158), we see that

$$E_{J,K} = \mathbb{E}(\mathrm{S}_J\,|\,\mathrm{R}, \mathrm{A}) \int \mathbf{1}\bigg\{ \frac{\|\boldsymbol{\zeta}\|^2}{M} \leqslant L \bigg\} E_{K|J}(\boldsymbol{\zeta})\, \mathbb{Q}_J(d\boldsymbol{\zeta})\,,$$

so the claim follows. ■

Analogously to (58), we now define

$$(\mathbb{H}_*)^{2,\circ} \equiv \bigg\{ (J,K) \in (\mathbb{H}_*)^2 : \frac{|\lambda(J,K)|}{\alpha^{1/2}} \leqslant 10 \cdot C_1(U) \bigg\}\,,$$

so $(\mathbb{H}_*)^{2,\circ}$ is a subset of $(\mathbb{H}_*)^2$. Then decompose $\bar{\boldsymbol{Z}}^2(\boldsymbol{G}') \equiv \bar{\boldsymbol{Z}}^{2,\circ}(\boldsymbol{G}') + \bar{\boldsymbol{Z}}^{2,\bullet}(\boldsymbol{G}')$ where (cf. (59))

$$\bar{\boldsymbol{Z}}^{2,\circ}(\boldsymbol{G}') \equiv \sum_{(J,K) \in (\mathbb{H}_*)^{2,\circ}} \mathrm{S}_J(\boldsymbol{G}')\mathrm{S}_K(\boldsymbol{G}') \mathbf{1}\bigg\{ \frac{\|\boldsymbol{G}'\mathbf{v}_J\|^2}{M} \leqslant L, \frac{\|\boldsymbol{G}'\mathbf{v}_K\|^2}{M} \leqslant L \bigg\}\,. \quad (170)$$

We bound $\bar{\boldsymbol{Z}}^{2,\circ}(\boldsymbol{G}')$ as follows:

**Theorem D.9 (analogous to Theorem A.12)** *Suppose $U$ satisfies Assumptions 1 and 2, and let $\mathscr{F}'(t)$ be as in (25). Recalling Proposition D.7 and (169), let $\Psi_2(\lambda \,|\, \boldsymbol{\zeta})$ be defined by*

$$\Psi_2(\lambda \,|\, \boldsymbol{\zeta}) - \Psi(\pi_*, \varpi_*) \equiv -\psi(1-q) + \mathcal{A}_2(\lambda \,|\, \boldsymbol{\zeta}) = -\psi(1-q) + \frac{\psi(1-q)}{2(1-\lambda^2)} + \mathcal{L}_2(\lambda \,|\, \boldsymbol{\zeta}) .$$

*For $\bar{\boldsymbol{Z}}^{2,\circ}(\boldsymbol{G}')$ as defined by (170), we have*

$$\frac{\mathbb{E}(\bar{\boldsymbol{Z}}^{2,\circ}(\boldsymbol{G}') \,|\, \mathscr{F}'(t))}{\exp\{2 \cdot (\mathbf{1}, \log(2\operatorname{ch}(\mathbf{H}^{(t)})))\}} \leqslant \sum_{(J,K)\in(\mathbb{H}_*)^{2,\circ}} \mathbf{Q}(J,K) \int \exp\Big\{ N\Big[ \Psi_2(\lambda \,|\, \boldsymbol{\zeta}) + o_t(1) \Big] \Big\} \,\mathbb{Q}_J(d\boldsymbol{\zeta})$$

*for $\mathbb{Q}_J$ as in Definition D.2 and $\mathbf{Q}$ as in Definition D.6.*

**Proof** We follow the proof of Theorem A.12. Suppose $J, K \in \mathbb{H}_*$ with $\lambda = \lambda(J,K)$ as given by Definition D.3. Recalling Definition A.7, the restriction $J \in \mathbb{H}_*$ implies

$$\frac{\mathbf{H}[t-1]J}{N\psi^{1/2}} \overset{(38)}{=} \frac{\boldsymbol{\Gamma}\mathbf{y}[t-1]J}{N} \overset{(49)}{=} \boldsymbol{\Gamma}\varpi(J) \simeq \boldsymbol{\Gamma}\varpi_* \overset{(56)}{=} \psi^{1/2}(1-q)\boldsymbol{\Gamma}\boldsymbol{\Gamma}^{\mathrm{t}}\acute{e}_{t-1} .$$

It follows that, for all $J \in \mathbb{H}_*$,

$$\frac{(\mathbf{H}^{(t)}, J)}{N} \simeq \psi(1-q)(\boldsymbol{\Gamma}\boldsymbol{\Gamma}^{\mathrm{t}})_{t-1,t-1} \overset{(36)}{=} \psi(1-q) .$$

Since $(\mathbf{H}^{(t)}, \mathbf{H}^{(t+1)})/(N\psi) = 1 - o_t(1)$, we conclude that, for all $J \in \mathbb{H}_*$.

$$\frac{(\mathbf{H}^{(t+1)}, J)}{N} \simeq \psi(1-q) - o_t(1) .$$

Let $E_{J,K}$ be as in (156). Combining with Definition D.6 gives

$$\begin{aligned}\frac{\mathbb{E}(\bar{\boldsymbol{Z}}^{2,\circ}(\boldsymbol{G}') \,|\, \mathscr{F}'(t))}{\exp\{2 \cdot (\mathbf{1}, \log(2\operatorname{ch}(\mathbf{H}^{(t)})))\}} &\leqslant \sum_{(J,K)\in(\mathbb{H}_*)^{2,\circ}} \mathbf{Q}(J,K) \left( \frac{\mathbf{P}(J,K)/\mathbf{Q}(J,K)}{\exp\{2 \cdot (\mathbf{1}, \log\operatorname{ch}(\mathbf{H}^{(t)}))\}} \right) E_{J,K} \\ &\leqslant \sum_{(J,K)\in(\mathbb{H}_*)^{2,\circ}} \mathbf{Q}(J,K) \frac{E_J \cdot E_{J,K}/E_J}{\exp\{2N[\psi(1-q) - o_t(1)]\}} \\ &\leqslant \exp\Big\{ N\Psi(\pi_*, \varpi_*) \Big\} \sum_{(J,K)\in(\mathbb{H}_*)^{2,\circ}} \mathbf{Q}(J,K) \frac{E_{J,K}/E_J}{\exp\{N[\psi(1-q) - o_t(1)]\}} ,\end{aligned} \tag{171}$$

where the last bound is by the calculation (149) from the proof of Proposition D.1. Combining with Proposition D.7 gives the claim. ■

**Corollary D.10 (analogous to Corollary C.1)** *Suppose $U$ satisfies Assumptions 1 and 2, and let $\mathscr{F}'(t)$ be as in (25). We then have the bound*

$$\mathbb{E}\Big( \bar{\boldsymbol{Z}}^{2,\bullet}(\boldsymbol{G}') \,\Big|\, \mathscr{F}'(t) \Big) \leqslant \exp\Big\{ 2N\Big( \mathrm{RS}(\alpha; U) - 0.1 \cdot C_1(U)^2 \alpha \Big) \Big\}$$

*for $\bar{\boldsymbol{Z}}^{2,\bullet}(\boldsymbol{G}') = \bar{\boldsymbol{Z}}^{2}(\boldsymbol{G}') - \bar{\boldsymbol{Z}}^{2,\circ}(\boldsymbol{G}')$ as defined by (170).*

**Proof** For $E_{J,K}$ as in (156) we also have trivially $E_{J,K} \leqslant 1$, and combining this with the calculation (171) gives

$$\frac{\mathbb{E}(\bar{\boldsymbol{Z}}^{2,\bullet}(\boldsymbol{G}') \mid \mathscr{F}'(t))}{\exp\{2 \cdot (\mathbf{1}, \log(2\operatorname{ch}(\mathbf{H}^{(t)})))\}} \leqslant \sum_{(J,K)\in(\mathbb{H}_*)^{2,\bullet}} \frac{\mathbf{Q}(J,K)}{\exp\{2N[\psi(1-q) - o_t(1)]\}} .$$

Combining Proposition A.1 with Corollary B.8 and (115) gives, with high probability,

$$\begin{aligned}\frac{\mathbb{E}(\bar{\boldsymbol{Z}}^{2,\bullet}(\boldsymbol{G}') \mid \mathscr{F}'(t))}{\exp\{2N\mathrm{RS}(\alpha;U)\}} &\leqslant \mathbf{Q}\Big((\mathbb{H}_*)^{2,\bullet}\Big) \cdot \exp\left\{N \cdot 2\left[3 + 1.53 + \frac{3}{2} + o_t(1)\right] C_1(U)^2 \cdot \alpha\right\} \\ &\leqslant \mathbf{Q}\Big((\mathbb{H}_*)^{2,\bullet}\Big) \cdot \exp\left\{12.1 \cdot N \cdot C_1(U)^2\alpha\right\} .\end{aligned}$$

For any $J \in \{-1,+1\}^N$, it follows by the Azuma–Hoeffding inequality that

$$\mathbf{Q}\left(K \in \{-1,+1\}^N : \left|\frac{(J - \mathbf{m}^{(t)}, K - \mathbf{m}^{(t)})}{N}\right| \geqslant x\right) \leqslant 2\exp\left\{-\frac{Nx^2}{8}\right\}$$

for any $x \geqslant 0$. Recalling Definition D.3, it follows that for any $J \in \mathbb{H}_*$,

$$\mathbf{Q}\Big(K \in \mathbb{H}_* : |\lambda(J,K)| \geqslant l\Big) \leqslant 2\exp\left\{-\frac{N(1 - q + o_N(1))l^2}{8}\right\} \tag{172}$$

for any $l \geqslant 0$. Taking $l = 10 \cdot C_1(U)\alpha^{1/2}$ and summing over $J$ gives

$$\mathbf{Q}\Big((\mathbb{H}_*)^{2,\bullet}\Big) \leqslant \sum_{J\in\mathbb{H}_*} \mathbf{Q}\Big(K \in \mathbb{H}_* : |\lambda(J,K)| \geqslant 10 \cdot C_1(U)\alpha^{1/2}\Big) \leqslant \exp\left\{-12.4 \cdot N \cdot C_1(U)^2\alpha\right\} .$$

It follows by combining the above bounds that

$$\frac{\mathbb{E}(\bar{\boldsymbol{Z}}^{2,\bullet}(\boldsymbol{G}') \mid \mathscr{F}'(t))}{\exp\{2N\mathrm{RS}(\alpha;U)\}} \leqslant \exp\left\{-0.3 \cdot N \cdot C_1(U)^2\alpha\right\} ,$$

which concludes the proof. ■

### D.3. Analysis of second moment

In this subsection we analyze the bound from Theorem D.9.

**Proposition D.11 (analogous to Lemmas C.2 and C.3)** *For $\mathcal{A}_2(\lambda \mid \boldsymbol{\zeta})$ as in Proposition D.7, the derivative with respect to $\lambda$ at $\lambda = 0$ satisfies the estimate*

$$\left.\frac{d\mathcal{A}_2(\lambda \mid \boldsymbol{\zeta})}{d\lambda}\right|_{\lambda=0} = o_N(1) + o_t(1)\alpha L^{1/2}$$

*provided that $\boldsymbol{\zeta} = \boldsymbol{G}\mathbf{v}$ is compatible with the admissibility condition (62), and satisfies the bound $\|\boldsymbol{\zeta}\|^2 \leqslant ML$ where $L = L_1(U) = 5C_1(U)^2$ as defined above.*

**Proof** For $\mathcal{L}_2(\lambda \,|\, \boldsymbol{\zeta})$ as defined by (169), we have

$$\frac{d\mathcal{A}_2(\lambda \,|\, \boldsymbol{\zeta})}{d\lambda}\bigg|_{\lambda=0} = \frac{d\mathcal{L}_2(\lambda \,|\, \boldsymbol{\zeta})}{d\lambda}\bigg|_{\lambda=0} = \frac{(1-q)^{1/2}}{N} \sum_{a \leqslant M} \frac{\mathbb{E}_\xi U'((\mathbf{h}^{(t+1)})_a + (1-q)^{1/2}\xi)}{\mathbb{E}U((\mathbf{h}^{(t+1)})_a + (1-q)^{1/2}\xi)} \zeta_a$$
$$\overset{(98)}{=} \frac{(1-q)^{1/2}(F_q(\mathbf{h}^{(t+1)}), \boldsymbol{\zeta})}{N} = \frac{(1-q)^{1/2}(\mathbf{n}^{(t+1)}, \boldsymbol{\zeta})}{N}\,.$$

On the other hand, it follows from the admissibility condition that $\boldsymbol{\zeta} = \boldsymbol{G}\mathbf{v}$ must satisfy

$$\frac{\mathbf{c}[t-1]\boldsymbol{\zeta}}{N^{1/2}} \overset{(63)}{=} (\boldsymbol{\Gamma}_N)^{\mathrm{t}} \delta(J) = o_N(1)\,, \tag{173}$$

where the last step is by the restriction $J \in \mathbb{H}_*$. The span of the vectors $\mathbf{c}^{(\ell)}$ for $\ell \leqslant t-1$ — which is the same as the span of the vectors $\mathbf{n}^{(\ell)}$ for $\ell \leqslant t-1$ — does not contain $\mathbf{n}^{(t+1)}$, but recall from (42) that

$$\frac{(\mathbf{n}^{(t+1)}, \mathbf{n}^{(t-1)})}{N\psi} \overset{(42)}{=} \mu_{t-1}\,.$$

It follows from Proposition A.6 and Lemma B.11 that $\mu_{t-1} = 1 - o_t(1)$, so we can decompose

$$\frac{\mathbf{n}^{(t+1)}}{(N\psi)^{1/2}} = \mathbf{c}^{\|} + \mathbf{c}^{\perp}$$

where $\mathbf{c}^{\|}$ lies in the span of the vectors $\mathbf{c}^{(\ell)}$ and has norm $1 - o_t(1)$, while $\mathbf{c}^{\perp}$ is orthogonal to the vectors $\mathbf{c}^{(\ell)}$ and has norm $o_t(1)$. It follows that

$$\left|\left(\frac{\mathbf{n}^{(t+1)}}{N\psi^{1/2}}, \boldsymbol{\zeta}\right)\right| = \frac{|(\mathbf{c}^{\|} + \mathbf{c}^{\perp}, \boldsymbol{\zeta})|}{N^{1/2}} \overset{(173)}{\leqslant} o_N(1) + \frac{\|\mathbf{c}^{\perp}\| \|\boldsymbol{\zeta}\|}{N^{1/2}} \leqslant o_N(1) + o_t(1)(\alpha L)^{1/2}\,,$$

having used Cauchy–Schwarz together with the assumption $\|\boldsymbol{\zeta}\|^2 \leqslant ML$. In conclusion we find

$$\frac{d\mathcal{A}_2(\lambda \,|\, \boldsymbol{\zeta})}{d\lambda}\bigg|_{\lambda=0} = o_N(1) + o_t(1)\alpha L^{1/2}\,,$$

as claimed. ■

**Lemma D.12 (analogous to Corollary C.9)** *Suppose $U$ satisfies Assumptions 1 and 2. Recall $K_2(U)$ from Assumption 2, and $C_1(U)$ from Lemma B.3. For $\mathcal{L}_2(\lambda \,|\, \boldsymbol{\zeta})$ as defined by (169), we have the bound*

$$\left|\frac{d^2\mathcal{L}_2(\lambda \,|\, \boldsymbol{\zeta})}{d\lambda^2}\right| \leqslant 420 \cdot C_1(U)^2 K_2(U) \cdot \alpha$$

*as long as $|\lambda| \leqslant 4/5$ and $\|\boldsymbol{\zeta}\|^2/M \leqslant L = L_1(U) = 5C_1(U)^2$.*

**Proof** Let $e(\lambda) \equiv (1-q)^{1/2}(1-\lambda^2)^{1/2}$. Denote

$$\boldsymbol{Y} \equiv \boldsymbol{Y}(\lambda; \boldsymbol{\zeta}) = \left\{\mathbf{h}^{(t+1)} + (1-q)^{1/2}\lambda\boldsymbol{\zeta}\right\} + (1-q)^{1/2}(1-\lambda^2)^{1/2}\xi\mathbf{1} \equiv \boldsymbol{X}(\lambda; \boldsymbol{\zeta}) + e(\lambda)\xi\mathbf{1}\,.$$

Then the function $\mathcal{L}_2(\lambda\,|\,\boldsymbol{\zeta})$ from Proposition D.7 can be rewritten as

$$\mathcal{L}_2(\lambda\,|\,\boldsymbol{\zeta}) \equiv \frac{1}{N}\sum_{a\leqslant M} \log \mathbb{E}_\xi U(\boldsymbol{Y}_a(\lambda,\boldsymbol{\zeta}))\,.$$

Recalling the notation of (117), (118), (119), and (120), let us now define $\mathbf{A} \equiv A_c(\boldsymbol{X})$, $\mathbf{B} \equiv B_c(\boldsymbol{X})$, $\bar{a} \equiv (\mathbf{1}, a_c(\boldsymbol{X}))$, and $\bar{b} \equiv (\mathbf{1}, b_c(\boldsymbol{X}))$, for $c = e(\lambda)$ and $\boldsymbol{X} = \boldsymbol{X}(\lambda;\boldsymbol{\zeta})$. With this notation, we have

$$\frac{d^2\mathcal{L}_2(\lambda\,|\,\boldsymbol{\zeta})}{d\lambda^2} = \frac{1}{N}\sum_{a\leqslant M}\left\{\frac{\mathbb{E}_\xi U'(\boldsymbol{Y}_a)\frac{d^2\boldsymbol{Y}_a}{d\lambda^2} + \mathbb{E}_\xi U''(\boldsymbol{Y}_a)(\frac{d\boldsymbol{Y}_a}{d\lambda})^2}{\mathbb{E}_\xi U(\boldsymbol{Y}_a)} - \left(\frac{\mathbb{E}_\xi U'(\boldsymbol{Y}_a)\frac{d\boldsymbol{Y}_a}{d\lambda}}{\mathbb{E}_\xi U(\boldsymbol{Y}_a)}\right)^2\right\}.$$

We decompose the above as (I) + (II) + (III) + (IV) where (cf. Lemma C.5)

$$\begin{aligned}
(\mathrm{I}) &\equiv \frac{1}{N}(\boldsymbol{X}'(\lambda))^{\mathrm{t}}(\operatorname{diag}\mathbf{A})\boldsymbol{X}'(\lambda) = \frac{1-q}{N}\boldsymbol{\zeta}^{\mathrm{t}}(\operatorname{diag}\mathbf{A})\boldsymbol{\zeta}\,,\\
(\mathrm{II}) &\equiv \frac{2}{N}e'(\lambda)\mathbf{B}^{\mathrm{t}}\boldsymbol{X}'(\lambda) = -\frac{2(1-q)^{1/2}\lambda}{N(1-\lambda^2)^{1/2}}\mathbf{B}^{\mathrm{t}}\boldsymbol{\zeta}\,,\\
(\mathrm{III}) &\equiv \frac{1}{N}e''(\lambda)\bar{a} = -\frac{(1-q)^{1/2}}{N(1-\lambda^2)^{3/2}}\bar{a}\,,\\
(\mathrm{IV}) &\equiv \frac{1}{N}e'(\lambda)^2\bar{b} = \frac{(1-q)\lambda^2}{N(1-\lambda^2)}\bar{b}\,.
\end{aligned}$$

We bound each of the above terms, assuming $|\lambda| \leqslant 4/5$. Applying (126) gives

$$|(\mathrm{I})| \leqslant \frac{1}{N}\|\mathbf{A}\|_\infty\|\boldsymbol{\zeta}\|^2 \leqslant \frac{1}{N}1.7\cdot K_2(U)\|\boldsymbol{\zeta}\|^2 \leqslant 1.7\cdot K_2(U)\alpha L = 8.5\cdot C_1(U)^2K_2(U)\cdot\alpha\,.$$

It follows from the above definition of $\boldsymbol{X} \equiv \boldsymbol{X}(\lambda;\boldsymbol{\zeta})$ that

$$\frac{\|\boldsymbol{X}\|}{M^{1/2}} \leqslant \frac{\|\mathbf{h}^{(t+1)}\| + \|\boldsymbol{\zeta}\|}{M^{1/2}} \leqslant 2q^{1/2} + L^{1/2} \leqslant 2.5\cdot C_1(U)\,, \tag{174}$$

with high probability. Combining (174) with Lemma C.6 gives

$$\begin{aligned}
|(\mathrm{II})| &\leqslant \frac{8}{3N}\|\mathbf{B}\|\|\boldsymbol{\zeta}\| \leqslant \frac{8M^{1/2}\|\boldsymbol{\zeta}\|}{3N}K_2(U)\left(2.5\cdot C_1(U) + 5.8\cdot\frac{\|\boldsymbol{X}\|}{M^{1/2}}\right)\\
&\leqslant \frac{8\alpha L^{1/2}}{3}K_2(U)\Big(2.5\cdot C_1(U) + 5.8\cdot 2.5\cdot C_1(U)\Big) \leqslant 105\cdot C_1(U)^2K_2(U)\cdot\alpha\,.
\end{aligned}$$

Next, combining (174) with Lemma C.7 gives

$$\begin{aligned}
|(\mathrm{III})| &\leqslant \frac{4.7}{N}|\bar{a}| \leqslant \frac{4.7\cdot M}{N}\left\{1.1\cdot C_1(U) + 3.7\cdot\frac{\|\boldsymbol{X}\|^2}{M}\right\}\\
&\leqslant \frac{4.7\cdot M}{N}\left\{1.1\cdot C_1(U) + 3.7\cdot 2.5^2\cdot C_1(U)^2\right\} \leqslant 110\cdot C_1(U)^2\cdot\alpha\,.
\end{aligned}$$

Finally, combining (174) with Lemma C.8 gives

$$\begin{aligned}|(\mathrm{IV})| &\leqslant \frac{1.8}{N}|\bar{b}| \leqslant 1.8\cdot K_2(U)\bigg(4.6\cdot C_1(U)+17\cdot\frac{\|\boldsymbol{X}\|^2}{M}\bigg)\cdot\alpha\\ &\leqslant 1.8\cdot K_2(U)\bigg(4.6\cdot C_1(U)+17\cdot\Big(2.5\cdot C_1(U)\Big)^2\bigg)\cdot\alpha\leqslant 193\cdot C_1(U)^2K_2(U)\cdot\alpha\,.\end{aligned}$$

Combining the above bounds gives the claim. ■

**Corollary D.13 (analogous to Proposition C.4)** *Suppose $U$ satisfies Assumptions 1 and 2. For $\Psi_2(\lambda\,|\,\boldsymbol{\zeta})$ as in the statement of Theorem D.9, we have the bound*

$$\bigg|\frac{d^2\Psi_2(\lambda\,|\,\boldsymbol{\zeta})}{d\lambda^2}\bigg|\leqslant 610\cdot C_1(U)^2K_2(U)\cdot\alpha\,,$$

*as long as $|\lambda|\leqslant 4/5$ and $\|\boldsymbol{\zeta}\|^2/M\leqslant L_1(U)=5C_1(U)^2$.*

**Proof** It follows from the definition that

$$\bigg|\frac{d^2\Psi_2(\lambda\,|\,\boldsymbol{\zeta})}{d\lambda^2}\bigg|\leqslant\frac{\psi(1-q)(1+3\lambda^2)}{(1-\lambda^2)^3}+\bigg|\frac{d^2\mathcal{L}_2(\lambda\,|\,\boldsymbol{\zeta})}{d\lambda^2}\bigg|\leqslant 62.6\cdot\psi+\bigg|\frac{d^2\mathcal{L}_2(\lambda\,|\,\boldsymbol{\zeta})}{d\lambda^2}\bigg|\,.$$

Applying Proposition A.1 and Lemma D.12 gives

$$\bigg|\frac{d^2\mathcal{A}_2(\lambda\,|\,\boldsymbol{\zeta})}{d\lambda^2}\bigg|\leqslant\bigg\{62.6\cdot 3\cdot C_1(U)^2+420\cdot C_1(U)^2K_2(U)\bigg\}\cdot\alpha\,.$$

The claim follows. ■

### D.4. Conclusion of second moment

In this concluding subsection we finish the proof of Theorem 1.5, and use it to deduce the lower bound of Theorem 1.1 in the case $\|u\|_\infty<\infty$.

**Proof** [Proof of Theorem 1.5 (conclusion)] Recall that the proof of the first moment lower bound (17) was already given at the end of §D.1. It therefore remains to show the second moment upper bound (18), and for this we follow the proof of Theorem 1.4. Recall from (170) that we decomposed $\bar{\boldsymbol{Z}}^2(\boldsymbol{G}')$ as the sum of $\bar{\boldsymbol{Z}}^{2,\circ}(\boldsymbol{G}')$ and $\bar{\boldsymbol{Z}}^{2,\bullet}(\boldsymbol{G}')$. For $\bar{\boldsymbol{Z}}^{2,\circ}(\boldsymbol{G}')$, we will analyze the bound from Theorem D.9. We note that at $\lambda=0$ we have

$$\Psi_2(0\,|\,\boldsymbol{\zeta})-\Psi(\pi_*,\varpi_*)=-\frac{\psi(1-q)}{2}+\mathcal{L}_2(0\,|\,\boldsymbol{\zeta})\overset{(169)}{\simeq}-\frac{\psi(1-q)}{2}+\alpha\mathbb{E}L_q(q^{1/2}Z)\overset{(138)}{\simeq}\Psi(\pi_*,\varpi_*)\,.$$

It follows by combining with (137) that

$$(\mathbf{1},\log(2\,\mathrm{ch}(\mathbf{H}^{(t)})))+\frac{\Psi_2(0\,|\,\boldsymbol{\zeta})}{2}\overset{N\to\infty}{\longrightarrow}\mathrm{RS}(\alpha;U)\,.$$

Next, for $|\lambda| \leqslant 4/5$, it follows by combining Proposition D.11 and Corollary D.13 that

$$\Psi_2(\lambda \,|\, \boldsymbol{\zeta}) - \Psi_2(0 \,|\, \boldsymbol{\zeta}) \leqslant \frac{d\Psi_2(\lambda \,|\, \boldsymbol{\zeta})}{d\lambda}\bigg|_{\lambda=0} \cdot \lambda + \max\left\{\left|\frac{d^2\Psi_2(\lambda \,|\, \boldsymbol{\zeta})}{d\lambda^2}\right| : |\lambda| \leqslant \frac{4}{5}\right\} \cdot \frac{\lambda^2}{2}$$
$$\leqslant o_t(1)\lambda + 610 \cdot C_1(U)^2 K_2(U) \cdot \alpha \cdot \frac{\lambda^2}{2}\,.$$

Recalling that $\alpha \leqslant \alpha(U)$ as defined by (27), the above can be simplified as

$$\Psi_2(\lambda \,|\, \boldsymbol{\zeta}) - \Psi_2(0 \,|\, \boldsymbol{\zeta}) \overset{(27)}{\leqslant} o_t(1) + \frac{610 \cdot \lambda^2}{2e^{10} C_1(U)^4 K_2(U)^3} \leqslant o_t(1) + \frac{\lambda^2}{e^{13}}\,.$$

Substituting this into the bound from Theorem D.9 gives

$$\frac{\mathbb{E}(\bar{\boldsymbol{Z}}^{2,\circ}(\boldsymbol{G}') \,|\, \mathscr{F}'(t))}{\exp\{2N[\mathrm{RS}(\alpha; U) + o_t(1)]\}} \leqslant \sum_{(J,K) \in (\mathbb{H}_*)^{2,\circ}} \mathbf{Q}(J,K) \exp\left\{\frac{N\lambda^2}{e^{13}}\right\}.$$

It follows by combining with (172) that the right-hand side is bounded by a constant. Finally, we recall that $\mathbb{E}(\bar{\boldsymbol{Z}}^{2,\bullet}(\boldsymbol{G}')$ was bounded by Corollary D.10, so the claim follows. ■

**Proof** [Proof of Theorem 1.1 lower bound assuming $\|u\|_\infty < \infty$] It follows from the first bound from Theorem 1.5 that

$$\mathbb{E}\left(\bar{\boldsymbol{Z}}\mathbf{1}\left\{\bar{\boldsymbol{Z}} \geqslant \frac{\mathbb{E}(\bar{\boldsymbol{Z}} \,|\, \mathscr{F}(t))}{2}\right\} \,\middle|\, \mathscr{F}(t)\right) \geqslant \frac{\mathbb{E}(\bar{\boldsymbol{Z}} \,|\, \mathscr{F}(t))}{2} \overset{(17)}{\geqslant} \frac{\exp\{N(\mathrm{RS}(\alpha; U) - o_t(1))\}}{2}\,, \tag{175}$$

with high probability over the randomness of $\mathscr{F}(t)$. On the other hand, the Cauchy–Schwarz inequality gives

$$\mathbb{E}\left(\bar{\boldsymbol{Z}}\mathbf{1}\left\{\bar{\boldsymbol{Z}} \geqslant \frac{\mathbb{E}(\bar{\boldsymbol{Z}} \,|\, \mathscr{F}(t))}{2}\right\} \,\middle|\, \mathscr{F}(t)\right)^2 \leqslant \mathbb{E}(\bar{\boldsymbol{Z}}^2 \,|\, \mathscr{F}(t)) \cdot \mathbb{P}\left(\bar{\boldsymbol{Z}} \geqslant \frac{\mathbb{E}(\bar{\boldsymbol{Z}} \,|\, \mathscr{F}(t))}{2} \,\middle|\, \mathscr{F}(t)\right).$$

Combining the above with the second bound from Theorem 1.5 gives, again with high probability,

$$\mathbb{P}\left(\bar{\boldsymbol{Z}} \geqslant \frac{\exp\{N(\mathrm{RS}(\alpha; U) - o_t(1))\}}{2} \,\middle|\, \mathscr{F}(t)\right) \overset{(175)}{\geqslant} \frac{\exp\{2N(\mathrm{RS}(\alpha; U) - o_t(1))\}/4}{\mathbb{E}(\bar{\boldsymbol{Z}}^2 \,|\, \mathscr{F}(t))}$$
$$\overset{(18)}{\geqslant} \frac{1/4}{\exp(2No_t(1))}\,. \tag{176}$$

Next let $\mathbb{P}^j$ denote probability conditional on the first $j$ rows of $\boldsymbol{G}$, and let $\mathbb{E}^j$ denote expectation with respect to $\mathbb{P}^j$. Then, as in the proof of (Talagrand, 2011b, Propn. 9.2.6), we take the martingale decomposition

$$\frac{1}{N}\left\{\log \boldsymbol{Z} - \mathbb{E}\log \boldsymbol{Z}\right\} = \sum_{j \leqslant M} \frac{1}{N}\left\{\mathbb{E}^j \log \boldsymbol{Z} - \mathbb{E}^{j-1}\log \boldsymbol{Z}\right\} \equiv \sum_{j \leqslant M} X_j\,.$$

To bound $X_j$, let $\boldsymbol{Z}_j$ denote the normalized partition function without the $j$-th factor,

$$\boldsymbol{Z}_j \equiv \sum_J \prod_{\substack{a \leqslant M,\\ a \neq j}} U\left(\frac{(\mathbf{g}^a, J)}{N^{1/2}}\right). \tag{177}$$

Since $\boldsymbol{Z}_j$ does not depend on the $j$-th row of $\boldsymbol{G}$, we can rewrite

$$NX_j = \mathbb{E}^j \log \frac{\boldsymbol{Z}}{\boldsymbol{Z}_j} - \mathbb{E}^{j-1} \log \frac{\boldsymbol{Z}}{\boldsymbol{Z}_j} \,.$$

By Assumption 1 and the uniform bound on $u \equiv \log U$, we have

$$\frac{1}{\exp(\|u\|_\infty)} \leqslant \frac{\boldsymbol{Z}}{\boldsymbol{Z}_j} \leqslant 1 \,,$$

which implies $|NX_j| \leqslant \|u\|_\infty$ almost surely. It follows from the Azuma–Hoeffding bound that

$$\mathbb{P}\bigg( \Big| \log \boldsymbol{Z} - \mathbb{E} \log \boldsymbol{Z} \Big| \geqslant N\epsilon \bigg) \leqslant 2 \exp \left\{ \frac{-N\epsilon^2}{2\alpha(\|u\|_\infty)^2} \right\} \equiv \frac{2}{\exp(Ns(\epsilon))} \,. \tag{178}$$

On the other hand, if we fix any $\epsilon > 0$, then (176) implies

$$\mathbb{P}\bigg( \frac{1}{N} \log \boldsymbol{Z} \geqslant \mathrm{RS}(\alpha; U) - \epsilon - \frac{\log 2}{N} \bigg) \geqslant o_N(1) + \frac{1/4}{\exp(2No_t(1))} \geqslant \frac{1/4}{\exp(Ns(\epsilon)/2)} \,. \tag{179}$$

Note that (178) and (179) contradict one another unless

$$\frac{1}{N} \mathbb{E} \log \boldsymbol{Z} \geqslant \mathrm{RS}(\alpha; U) - 2\epsilon - \frac{\log 2}{N} \,. \tag{180}$$

It follows using (178) again that, for $N$ large enough,

$$\mathbb{P}\bigg( \frac{1}{N} \log \boldsymbol{Z} \leqslant \mathrm{RS}(\alpha; U) - 4\epsilon \bigg) \overset{(180)}{\leqslant} \mathbb{P}\bigg( \log \boldsymbol{Z} - \mathbb{E} \log \boldsymbol{Z} \leqslant -N\epsilon \bigg) \overset{(178)}{\leqslant} o_N(1) \,.$$

In the above, the left-hand side does not depend on $t$, so it follows that

$$\liminf_{N \to \infty} \frac{1}{N} \log \boldsymbol{Z} \geqslant \mathrm{RS}(\alpha; U)$$

in probability. This gives the lower bound in Theorem 1.1 in the case $\|u\|_\infty < \infty$. ■

## Appendix E. Local central limit theorem

In this section we state and prove Proposition E.13 (used in the proofs of Proposition A.13 and Proposition D.1) and Proposition E.14 (used in the proof of Proposition D.7). Recall the calculation of $\tilde{\boldsymbol{X}}_J$ from Lemma A.20. Given $J \in \{-1, +1\}^N$ and $\tau \in \mathbb{R}^{t-1}$, we define

$$\begin{aligned} \boldsymbol{X} \equiv \boldsymbol{X}_{J,\tau} &= \tilde{\boldsymbol{X}}_J + N^{1/2} c(\pi(J)) \mathbf{c}[t-1]^{\mathrm{t}} \tau \\ &= \frac{\mathbf{h}[t]^{\mathrm{t}} \hat{\pi}}{q^{1/2}} + \frac{(1-q)\mathbf{n}[t-1]^{\mathrm{t}} \acute{\pi}}{q^{1/2}} + N^{1/2} c(\pi(J)) \mathbf{c}[t-1]^{\mathrm{t}} \tau \\ &\overset{(44)}{=} \frac{\mathbf{h}[t]^{\mathrm{t}} \hat{\pi}}{q^{1/2}} + \mathbf{n}[t-1]^{\mathrm{t}} \bigg\{ \frac{(1-q)\acute{\pi}}{q^{1/2}} + \frac{c(\pi(J))}{\psi^{1/2}} ((\mathbf{\Gamma}_N)^{\mathrm{t}})^{-1} \tau \bigg\} \,. \end{aligned} \tag{181}$$

Now let $\boldsymbol{\zeta}_a$ ($a \leqslant M$) be independent scalar random variables, such that $\boldsymbol{\zeta}_a$ has density given by (cf. Definition B.1)

$$\chi_{\boldsymbol{X}_a,c}(z) \equiv \frac{U(\boldsymbol{X}_a + cz)\varphi(z)}{\mathbb{E}_\xi U(\boldsymbol{X}_a + c\xi)}\,, \tag{182}$$

where $\boldsymbol{X} \equiv \boldsymbol{X}_{J,\tau}$ as above, and $c \equiv c(\pi(J)) \equiv (1 - \|\pi(J)\|^2)^{1/2}$. Note that

$$\mathbb{E}\boldsymbol{\zeta}_a = \frac{\mathbb{E}_\xi[\xi U(\boldsymbol{X}_a + c\xi)]}{\mathbb{E}_\xi U(\boldsymbol{X}_a + c\xi)} \overset{(8)}{=} c(\pi(J))F_{\|\pi(J)\|^2}(\boldsymbol{X}_a)\,. \tag{183}$$

Let $\mathbf{n}_a \in \mathbb{R}^{t-1}$ denote the $a$-th column of the matrix $\mathbf{n}[t-1]$, and consider the random variable

$$\boldsymbol{W} \equiv \frac{1}{N^{1/2}} \sum_{a \leqslant M} (\boldsymbol{\zeta}_a - \mathbb{E}\boldsymbol{\zeta}_a)\mathbf{n}_a = \frac{\mathbf{n}[t-1](\boldsymbol{\zeta} - \mathbb{E}\boldsymbol{\zeta})}{N^{1/2}} \in \mathbb{R}^{t-1}\,. \tag{184}$$

Let $P_{J,\tau}$ denote the law of $\boldsymbol{W}$. We will compare $P_{J,\tau}$ with the gaussian distribution on $\mathbb{R}^{t-1}$ that has mean zero and covariance

$$\Sigma \equiv \Sigma_{J,\tau} \equiv \frac{1}{N} \sum_{a \leqslant M} (\mathrm{Var}\,\boldsymbol{\zeta}_a)\mathbf{n}_a(\mathbf{n}_a)^{\mathrm{t}} \in \mathbb{R}^{(t-1)\times(t-1)}\,. \tag{185}$$

(We bound the singular values of $\Sigma_{J,\tau}$ in Lemma E.2 below.) The majority of this section is occupied with proving the following result:

**Proposition E.1 (local central limit theorem)** *Suppose $U$ satisfies Assumptions 1 and 2. Recall that $P_{J,\tau}$ is the law of the random variable $\boldsymbol{W}$ from (184). For any finite constant $\tau_{\max}$, it holds with high probability that for all $J \in \{-1,+1\}^N$ and all $\|\tau\| \leqslant \tau_{\max}$, the measure $P_{J,\tau}$ has a bounded continuous density $p_{J,\tau}$. Moreover, again with high probability,*

$$\sup\left\{\|p_{J,\tau} - g_{J,\tau}\|_\infty : J \in \{-1,+1\}^N, \|\pi(J)\| \leqslant \frac{4}{5}, \|\tau\| \leqslant \tau_{\max}\right\} \leqslant \frac{1}{(2\pi)^{t-1}N^{0.35}} \leqslant \frac{1}{N^{0.3}}\,,$$

*where $g_{J,\tau}$ denotes the density of the centered gaussian distribution on $\mathbb{R}^{t-1}$ with covariance $\Sigma \equiv \Sigma_{J,\tau}$.*

At the end of this section we will show that Proposition E.1 readily implies the required results Propositions E.13 and E.14. Towards the proof of Proposition E.1, we introduce some notation. Write $p_a$ for the density function of the random variable $\boldsymbol{\zeta}_a - \mathbb{E}\boldsymbol{\zeta}_a$, so in the notation of (182) we have

$$p_a(z) = \chi_{\boldsymbol{X}_a,c}(z + \mathbb{E}\boldsymbol{\zeta}_a) = \chi_{\boldsymbol{X}_a,c}\left(z + \frac{\mathbb{E}_\xi[\xi U(\boldsymbol{X}_a + c\xi)]}{\mathbb{E}_\xi U(\boldsymbol{X}_a + c\xi)}\right).$$

The characteristic function of the random variable $\boldsymbol{W}$ from (184) (i.e., the Fourier transform of the measure $P_{J,\tau}$) is given by the function

$$\hat{p}(\mathfrak{s}) \equiv \hat{p}_{J,\tau}(\mathfrak{s}) \equiv \mathbb{E}\exp(\mathfrak{i}(\mathfrak{s},\boldsymbol{W})) = \prod_{a \leqslant M} \mathbb{E}\exp\left\{\frac{\mathfrak{i}(\mathfrak{s},\mathbf{n}_a)(\boldsymbol{\zeta}_a - \mathbb{E}\boldsymbol{\zeta}_a)}{N^{1/2}}\right\} = \prod_{a \leqslant M} \hat{p}_a\left(\frac{(\mathfrak{s},\mathbf{n}_a)}{N^{1/2}}\right), \tag{186}$$

where $\hat{p}_a$ denotes the Fourier transform of $p_a$. The Fourier transform of the gaussian density $g \equiv g_{J,\tau}$ is given by

$$\hat{g}(\mathfrak{s}) \equiv \hat{g}_{J,\tau}(\mathfrak{s}) \equiv \exp\left\{-\frac{(\mathfrak{s}, \Sigma\mathfrak{s})}{2}\right\} = \prod_{a \leqslant M} \exp\left\{-\frac{(\mathfrak{s}, \mathbf{n}_a)^2 \operatorname{Var} \boldsymbol{\zeta}_a}{2N}\right\} \equiv \prod_{a \leqslant M} \hat{g}_a(\mathfrak{s}) \,. \tag{187}$$

With $\hat{p} \equiv \hat{p}_{J,\tau}$ as in (186) and $\hat{g} \equiv \hat{g}_{J,\tau}$ as in (187), we define

$$I_1(J,\tau) \equiv \int \Big|\hat{p}_{J,\tau}(\mathfrak{s}) - \hat{g}_{J,\tau}(\mathfrak{s})\Big| \mathbf{1}\Big\{\|\mathfrak{s}\| \leqslant N^{0.01}\Big\}\, d\mathfrak{s} \,, \tag{188}$$

$$I_2(J,\tau,\epsilon_2) \equiv \int \Big|\hat{p}_{J,\tau}(\mathfrak{s}) - \hat{g}_{J,\tau}(\mathfrak{s})\Big| \mathbf{1}\Big\{N^{0.01} \leqslant \|\mathfrak{s}\| \leqslant \epsilon_2 N^{1/2}\Big\}\, d\mathfrak{s} \,, \tag{189}$$

$$I_3(J,\tau,\epsilon_2) \equiv \int \Big|\hat{p}_{J,\tau}(\mathfrak{s}) - \hat{g}_{J,\tau}(\mathfrak{s})\Big| \mathbf{1}\Big\{\|\mathfrak{s}\| \geqslant \epsilon_2 N^{1/2}\Big\}\, d\mathfrak{s} \,. \tag{190}$$

In the analysis below we show that the integrals $I_j(J,\tau)$ can be bounded uniformly over $J \in \{-1,+1\}^N$ such that $\|\pi(J)\| \leqslant 4/5$, and any bounded range of vectors $\tau$. The remainder of this section is organized as follows:

- In §E.1 we bound the quantities $I_1$ and $I_2$ from (188) and (189).
- In §E.2, in preparation for bounding $I_3$ from (190), we prove rough estimates concerning the nondegeneracy of the vectors arising from the AMP iteration.
- In §E.3 we bound $I_3$ from (190).
- In §E.4 we combine the bounds from the preceding sections to finish the proof of Proposition E.1. We then state and prove Proposition E.13 and E.14.

The analysis of this section is based on standard methods; see e.g. Petrov (1975); Borovkov (2017).

### E.1. Fourier estimates at low and intermediate frequency

In this subsection we prove Lemmas E.4 and E.5, bounding the quantities $I_1$ and $I_2$ from (188) and (189).

**Lemma E.2** *Suppose $U$ satisfies Assumption 1 and 2, and let $\Sigma$ be as in (185). Given any $\tau_{\max} < \infty$, there is a positive constant $\iota_1$, depending on $t$ and on $\tau_{\max}$, such that we have the bounds*

$$\inf\left\{(u, \Sigma_{J,\tau} u) : \|u\| = 1, J \in \{-1,+1\}^2, \|\pi(J)\| \leqslant \frac{4}{5}, \|\tau\| \leqslant \tau_{\max}\right\} \geqslant \iota_1 \,, \tag{191}$$

$$\sup\left\{(u, \Sigma_{J,\tau} u) : \|u\| = 1, J \in \{-1,+1\}^2, \|\pi(J)\| \leqslant \frac{4}{5}, \|\tau\| \leqslant \tau_{\max}\right\} \leqslant \frac{1}{\iota_1} \,, \tag{192}$$

*with probability* $1 - o_N(1)$.

**Proof** Write $v_a \equiv \operatorname{Var} \boldsymbol{\zeta}_a$. Note that Assumption 2 gives, with $c = c(\pi(J)) \equiv (1 - \|\pi(J)\|^2)^2$,

$$v_a = v(\boldsymbol{X}_a, c) \equiv \frac{1}{2} \frac{\mathbb{E}_\xi[(\xi - \xi')^2 U(\boldsymbol{X}_a + c\xi) U(\boldsymbol{X}_a + c\xi')]}{\mathbb{E}_{\xi,\xi'}[U(\boldsymbol{X}_a + c\xi) U(\boldsymbol{X}_a + c\xi')]} \leqslant \frac{K_2(U)}{2} \,. \tag{193}$$

It follows that, for any unit vector $u \in \mathbb{R}^{t-1}$, and with $\varsigma_t$ as defined by Remark A.5, we have

$$\begin{aligned}(u, \Sigma u) &= \frac{1}{N} \sum_{a \leqslant M} v_a(\mathbf{n}_a, u)^2 \leqslant \frac{K_2(U)}{2N} \sum_{a \leqslant M} (\mathbf{n}_a, u)^2 \\ &= \frac{K_2(U)}{2N} \left\| \mathbf{n}[t-1]^{\mathrm{t}} u \right\|^2 \overset{(44)}{=} \frac{K_2(U)\psi}{2} \left\| (\boldsymbol{\Gamma}_N)^{\mathrm{t}} u \right\|^2 \leqslant \frac{K_2(U)\psi\varsigma_t}{2}\,,\end{aligned}$$

which proves (191). Next, for any $L$, let $M(L) \subseteq [M]$ denote the subset of indices $a \leqslant M$ satisfying the condition

$$\mathfrak{m}_a \equiv \max\left\{ |(\mathbf{h}^{(s)})_a|, |(\mathbf{n}^{(\ell)})_a| : s \leqslant t, \ell \leqslant t-1 \right\} \leqslant L\,. \tag{194}$$

It follows from Lemma A.4 that with high probability we can bound

$$\max\left\{ \frac{1}{M} \sum_{a \leqslant M} ((\mathbf{h}^{(s)})_a)^4, \frac{1}{M} \sum_{a \leqslant M} ((\mathbf{n}^{(\ell)})_a)^4 : s \leqslant t, \ell \leqslant t-1 \right\} \leqslant \wp_4$$

for a constant $\wp_4$. As a result, for any finite $L$, we can bound

$$\frac{1}{M} \sum_{a \leqslant M} \mathbf{1}\left\{ |(\mathbf{h}^{(s)})_a| \geqslant L \right\} \leqslant \frac{1}{M} \sum_{a \leqslant M} \frac{((\mathbf{h}^{(s)})_a)^4}{L^4} \leqslant \frac{\wp_4}{L^4}\,,$$

and similarly with $\mathbf{n}^{(\ell)}$ in place of $\mathbf{h}^{(s)}$. It follows using the Cauchy–Schwarz that

$$\begin{aligned}&\frac{1}{M} \sum_{a \leqslant M} (\mathbf{n}_a^{(\ell)})^2 \mathbf{1}\left\{ |(\mathbf{h}^{(s)})_a| \geqslant L \right\} \\ &\qquad \leqslant \left( \frac{1}{M} \sum_{a \leqslant M} (\mathbf{n}_a^{(\ell)})^4 \right)^{1/2} \left( \frac{1}{M} \sum_{a \leqslant M} \mathbf{1}\left\{ |(\mathbf{h}^{(s)})_a| \geqslant L \right\} \right)^{1/2} \leqslant \frac{\wp_4}{L^2}\,, \\ &\frac{1}{M} \sum_{a \leqslant M} (\mathbf{n}_a^{(\ell)})^2 \mathbf{1}\left\{ |(\mathbf{n}^{(j)})_a| \geqslant L \right\} \\ &\qquad \leqslant \left( \frac{1}{M} \sum_{a \leqslant M} (\mathbf{n}_a^{(\ell)})^4 \right)^{1/2} \left( \frac{1}{M} \sum_{a \leqslant M} \mathbf{1}\left\{ |(\mathbf{n}^{(j)})_a| \geqslant L \right\} \right)^{1/2} \leqslant \frac{\wp_4}{L^2}\,,\end{aligned}$$

where the bounds hold for all $s \leqslant t$ and all $j, \ell \leqslant t-1$. Combining these bounds gives, with $\mathfrak{m}_a$ as defined in (194),

$$\frac{1}{M} \sum_{a \notin M(L)} (\mathbf{n}_a^{(\ell)})^2 = \frac{1}{M} \sum_{a \leqslant M} (\mathbf{n}_a^{(\ell)})^2 \mathbf{1}\left\{ |\mathfrak{m}_a| \geqslant L \right\} \leqslant \frac{2t\wp_4}{L^2}\,. \tag{195}$$

Next, it follows from the definition (181) of $\boldsymbol{X} \equiv \boldsymbol{X}_{J,t}$ that for all $a \leqslant M$,

$$\begin{aligned}|\boldsymbol{X}_a| &\leqslant \frac{\|\hat{\pi}\|_\infty}{q^{1/2}} \sum_{s \leqslant t} |(\mathbf{h}^{(s)})_a| + \left( \frac{\|\hat{\pi}\|_\infty}{q^{1/2}} + \frac{\varsigma_t \|\tau\|}{\psi^{1/2}} \right) \sum_{\ell \leqslant t-1} |(\mathbf{n}^{(\ell)})_a| \\ &\leqslant \frac{\varsigma_t(1 + \|\tau\|)}{(q\psi)^{1/2}} \sum_{s \leqslant t} \left( |(\mathbf{h}^{(s)})_a| + |(\mathbf{n}^{(s)})_a| \right).\end{aligned} \tag{196}$$

If $\|\tau\| \leqslant \tau_{\max}$ where (without loss) $\tau_{\max} \geqslant 1$, then we obtain

$$\max\left\{|\boldsymbol{X}_a| : a \in M(L)\right\} \leqslant \frac{4\varsigma_t \tau_{\max} t L}{(q\psi)^{1/2}} \equiv L' . \tag{197}$$

It follows using Assumption 1 that for any finite $L'$ we must have

$$\inf\left\{v(x,c) : \frac{1}{2} \leqslant c \leqslant 1, |x| \leqslant L'\right\} \geqslant \epsilon(L') > 0 .$$

It follows that, for any unit vector $u \in \mathbb{R}^{t-1}$, we have the lower bound

$$\begin{aligned}(u, \Sigma u) &\geqslant \frac{\epsilon(L')}{N} \sum_{a \in M(L)} (\mathbf{n}_a, u)^2 \geqslant \frac{\epsilon(L')}{N}\left\{\left\|\mathbf{n}[t-1]^{\mathrm{t}} u\right\|^2 - \sum_{a \notin M(L)} (\mathbf{n}_a, u)^2\right\} \\ &\overset{(44)}{\geqslant} \epsilon(L')\left\{\psi\left\|(\boldsymbol{\Gamma}_N)^{\mathrm{t}} u\right\|^2 - \frac{1}{N}\sum_{a \notin M(L)} \|\mathbf{n}_a\|^2\right\} \overset{(195)}{\geqslant} \epsilon(L')\left\{\frac{\psi}{\varsigma_t} - \frac{2t^2 \wp_4}{L^2}\right\} \geqslant \frac{\epsilon(L')\psi}{2\varsigma_t} ,\end{aligned}$$

where the last inequality can be arranged by taking $L$ large enough (note that $L$ depends on $t$, and $L'$ depends on $L$). This proves the second assertion (192). ■

**Lemma E.3 (Taylor expansion of characteristic function)** *Suppose $U$ satisfies Assumptions 1 and 2. Let $\hat{p}_a$ be as in (186), and recall that it depends on both $J$ and $\tau$. It holds with high probability that*

$$\max\left\{\left|\hat{p}_a(\mathfrak{s}) - \left(1 - \frac{(\mathfrak{s}, \mathbf{n}_a)^2 \operatorname{Var} \boldsymbol{\zeta}_a}{2N}\right)\right| : J \in \{-1,+1\}^N, \|\pi(J)\| \leqslant \frac{4}{5}, \|\tau\| \leqslant N^{0.01}\right\} \leqslant \frac{\|\mathfrak{s}\|^3}{N^{1.4}}$$

*for all $\mathfrak{s} \in \mathbb{R}^{t-1}$ and all $a \leqslant M$.*

**Proof** It is well-known that for all $x \in \mathbb{R}$ we have

$$\left|e^{ix} - \left(1 + ix - \frac{x^2}{2}\right)\right| \leqslant \frac{|x|^3}{6} .$$

We also note that Lemma B.3 implies the third moment bound

$$\mathbb{E}\left(\left|\boldsymbol{\zeta}_a - \mathbb{E}\boldsymbol{\zeta}_a\right|^3\right) \leqslant 8\mathbb{E}(|\boldsymbol{\zeta}_a|^3) = \frac{8\mathbb{E}_\xi[|\xi|^3 U(\boldsymbol{X}_a + c\xi)]}{\mathbb{E}_\xi U(\boldsymbol{X}_a + c\xi)} \leqslant 8\Big(C_1(U) + (8|\boldsymbol{X}_a|)^3\Big) .$$

As a consequence, for all $\mathfrak{s} \in \mathbb{R}^{t-1}$ we have

$$\begin{aligned}\left|\hat{p}_a(\mathfrak{s}) - \left(1 - \frac{(\mathfrak{s}, \mathbf{n}_a)^2 \operatorname{Var} \boldsymbol{\zeta}_a}{2N}\right)\right| &\leqslant \frac{|(\mathfrak{s}, \mathbf{n}_a)|^3}{6N^{3/2}} \mathbb{E}\left(\left|\boldsymbol{\zeta}_a - \mathbb{E}\boldsymbol{\zeta}_a\right|^3\right) \\ &\leqslant \frac{4|(\mathfrak{s}, \mathbf{n}_a)|^3}{3N^{3/2}}\Big(C_1(U) + (8|\boldsymbol{X}_a|)^3\Big) .\end{aligned} \tag{198}$$

By combining Lemma B.15 with the bound (196) and the restriction $\|\tau\| \leqslant N^{0.01}$, we must have $\|\boldsymbol{X}\|_\infty \leqslant N^{0.021}$ with high probability. Therefore, with high probability,

$$\frac{4|(\mathfrak{s}, \mathbf{n}_a)|^3}{3N^{3/2}}\Big(C_1(U) + (8|\boldsymbol{X}_a|)^3\Big) \leqslant \frac{4\|\mathfrak{s}\|^3 t^{3/2} N^{0.03}}{3N^{3/2}}\Big(C_1(U) + (8|\boldsymbol{X}_a|)^3\Big) \leqslant \frac{\|\mathfrak{s}\|^3}{N^{1.4}} .$$

Combining with (198) concludes the proof. ■

**Lemma E.4 (low-frequency estimate)** *Suppose $U$ satisfies Assumption 1 and 2. In the notation of (188), we have*

$$\max\left\{I_1(J,\tau) : J \in \{-1,+1\}^N, \|\pi(J)\| \leqslant \frac{4}{5}, \|\tau\| \leqslant N^{0.01}\right\} \leqslant \frac{1}{N^{0.38}}$$

*with probability* $1 - o_N(1)$.

**Proof** Recall from (193) that $\operatorname{Var}\boldsymbol{\zeta}_a \leqslant K_2(U)/2$. Combining with Lemma B.15 gives, with high probability,

$$\frac{(\mathfrak{s},\mathbf{n}_a)^2 \operatorname{Var}\boldsymbol{\zeta}_a}{2N} \leqslant \frac{\|\mathfrak{s}\|^2 t(\|\mathbf{n}_a\|_\infty)^2 K_2(U)}{4N} \leqslant \frac{\|\mathfrak{s}\|^2 t K_2(U)}{4N^{0.98}} \leqslant \frac{\|\mathfrak{s}\|^2}{N^{0.97}},$$

We have $|\log(1-x)+x| \leqslant x^2$ for all $x$ small enough, so if $\|\mathfrak{s}\| \leqslant N^{0.01}$, then combining with Lemma E.3 gives

$$\begin{aligned}\left|\log \hat{p}_a(\mathfrak{s}) + \frac{(\mathfrak{s},\mathbf{n}_a)^2 \operatorname{Var}\boldsymbol{\zeta}_a}{2N}\right| &\leqslant \frac{\|\mathfrak{s}\|^3}{N^{1.4}} + \left(\frac{\|\mathfrak{s}\|^2}{N^{0.97}} + \frac{\|\mathfrak{s}\|^3}{N^{1.4}}\right)^2 \\ &\leqslant \frac{\|\mathfrak{s}\|^3}{N^{1.4}} + \left(\frac{2\|\mathfrak{s}\|^2}{N^{0.97}}\right)^2 \leqslant \frac{2\|\mathfrak{s}\|^3}{N^{1.4}} \leqslant \frac{1}{N^{1.39}}.\end{aligned}$$

Summing the above over $a \leqslant M$ gives that the multiplicative error between $\hat{p}(\mathfrak{s})$ and $\hat{g}(\mathfrak{s})$ is small for all $\|\mathfrak{s}\| \leqslant N^{0.01}$. Therefore, with high probability, we have the bound

$$I_1(J,\tau) \leqslant \int \hat{g}(\mathfrak{s})\left\{\exp\left(\frac{M}{N^{1.39}}\right) - 1\right\} d\mathfrak{s} \leqslant \frac{(2\pi)^{(t-1)/2}}{N^{0.385}(\det\Sigma)^{1/2}} \leqslant \frac{1}{N^{0.38}},$$

uniformly over all $J \in \{-1,+1\}^N$ and all $\|\tau\| \leqslant N^{0.01}$. ■

**Lemma E.5 (moderate-frequency estimate)** *Suppose $U$ satisfies Assumption 1 and 2. With the notation of (189), for any finite constant $\tau_{\max}$, we can choose $\epsilon_2$ depending on $\tau_{\max}$ such that*

$$\sup\left\{I_2(J,\tau,\epsilon_2) : J \in \{-1,+1\}^N, \|\pi(J)\| \leqslant \frac{4}{5}, \|\tau\| \leqslant \tau_{\max}\right\} \leqslant \frac{1}{\exp(N^{0.01})}$$

*with probability* $1 - o_N(1)$.

**Proof** It follows from the bound (198) in the proof of Lemma E.3 that, with high probability, we have

$$|\hat{p}(\mathfrak{s})| \leqslant \hat{g}(\mathfrak{s}) \exp\left\{\frac{4\|\mathfrak{s}\|^3}{3N^{3/2}} \sum_{a \leqslant M} \|\mathbf{n}_a\|^3 \Big(C_1(U) + (8|\boldsymbol{X}_a|)^3\Big)\right\}$$

for all $\mathfrak{s} \in \mathbb{R}^{t-1}$. Recall the bound (196) on $\boldsymbol{X} = \boldsymbol{X}_{J,\tau}$. If we assume without loss of generality that $\tau_{\max} \geqslant 1$, then combining (196) with Lemma A.4 gives, with high probability,

$$\sup\left\{\frac{4}{3N}\sum_{a \leqslant M} \|\mathbf{n}_a\|^3 \Big(C_1(U) + (8|\boldsymbol{X}_a|)^3\Big) : J \in \{-1,+1\}^n, \|\tau\| \leqslant \tau_{\max}\right\} \leqslant (\tau_{\max})^3 \wp_1,$$

where $\wp_1$ is a finite constant. On the other hand, by Lemma E.2, with high probability

$$\hat{g}(\mathfrak{s}) \leqslant \exp\bigg\{ -\frac{\iota_1 \|\mathfrak{s}\|^2}{2} \bigg\}.$$

It follows that, with high probability,

$$|\hat{p}(\mathfrak{s})| \leqslant \exp\bigg\{ -\frac{\iota_1 \|\mathfrak{s}\|^2}{2} + \frac{(\tau_{\max})^3 \wp_1 \|\mathfrak{s}\|^3}{N^{1/2}} \bigg\}.$$

To ensure that the quadratic term dominates the cubic term, we restrict to $\|\mathfrak{s}\| \leqslant \epsilon_2 N^{1/2}$ where

$$\epsilon_2 \equiv \frac{\iota_1}{4(\tau_{\max})^3 \wp_1}.$$

For this choice of $\epsilon_2$ we find that, with high probability, we have the bound

$$I_2(J,\tau,\epsilon) \leqslant \int_{\|\mathfrak{s}\| \geqslant N^{0.01}} \exp\bigg\{ -\frac{\iota_1 \|\mathfrak{s}\|^2}{4} \bigg\}\, d\mathfrak{s} \leqslant \frac{1}{\exp(N^{0.01})}$$

uniformly over all $J \in \{-1,+1\}^N$ and $\|\tau\| \leqslant \tau_{\max}$. ∎

### E.2. Non-degeneracy of TAP iterates

In this subsection we prove some preliminary results which will be used in §E.3 to estimate the quantity $I_3$ from (190).

**Lemma E.6** *If $B$ is any $k \times M$ matrix such that $BB^{\mathsf{t}} = I_k$, then $B$ must have a $k \times k$ submatrix $U$ such that*

$$|\det U| \geqslant \bigg( \frac{k!}{M^k} \bigg)^{1/2}.$$

**Proof** We argue by induction on $k$. If $k = 1$ then $B$ consists of a single row which is a unit vector in $\mathbb{R}^M$, so clearly $B$ must have an entry with absolute value at least $1/M^{1/2}$. Now suppose $k \geqslant 2$ and that the claim has been proved up to $k-1$. Denote the columns of $B$ as $\mathbf{b}_1, \ldots, \mathbf{b}_M$ where each $\mathbf{b}_a \in \mathbb{R}^k$. Since

$$\sum_{a \leqslant M} \|\mathbf{b}_a\|^2 = \operatorname{tr}(BB^{\mathsf{t}}) = k\,,$$

there must exist at least one index $a \leqslant M$ with

$$\|\mathbf{b}_a\|^2 \geqslant \frac{k}{M}.$$

We assume without loss that $a = 1$. Let $O$ be a $k \times k$ orthonormal matrix such that $O\mathbf{b}_1 = \|\mathbf{b}_1\| e_1$, where $e_1$ denotes the first standard basis vector in $\mathbb{R}^k$. Let $\bar{B} \equiv OB$, and note that $\bar{B}\bar{B}^{\mathsf{t}} = OBB^{\mathsf{t}}O^{\mathsf{t}} = I_k$, so $\bar{B}$ also has orthonormal rows. We can further decompose

$$\bar{B} = OB = \begin{pmatrix} \|\mathbf{b}_1\| & * \\ \mathbf{0} & \tilde{B} \end{pmatrix}$$

where $\mathbf{0}$ denotes the zero vector in $\mathbb{R}^{k-1}$, and $\tilde{B}$ is a $(k-1) \times (M-1)$ matrix with orthonormal rows. It follows from the inductive hypothesis that $\tilde{B}$ has a $(k-1) \times (k-1)$ submatrix $\tilde{U}$ with

$$|\det \tilde{U}| \geqslant \left(\frac{(k-1)!}{(M-1)^{k-1}}\right)^{1/2}.$$

As a result, $\bar{B}$ has a $k \times k$ submatrix $\bar{U}$ with

$$|\det \bar{U}| = \left|\det \begin{pmatrix} \|\mathbf{b}_1\| & * \\ \mathbf{0} & \tilde{U} \end{pmatrix}\right| \geqslant \|\mathbf{b}_1\| \cdot |\det \tilde{U}| \geqslant \frac{k^{1/2}}{M^{1/2}}\left(\frac{(k-1)!}{(M-1)^{k-1}}\right)^{1/2} \geqslant \left(\frac{k!}{M^k}\right)^{1/2}.$$

The claim follows by noting that $U = O^{\mathrm{t}}\bar{U}$ is a submatrix of the original matrix $B$. ■

**Corollary E.7** *If $B$ is any $k \times M$ matrix such that $\|BB^{\mathrm{t}} - I_k\|_\infty \leqslant 1/(3k)$, then $B$ has a $k \times k$ submatrix $U$ with*

$$|\det U| \geqslant \frac{1}{3}\left(\frac{k!}{M^k}\right)^{1/2}. \tag{199}$$

*(In the above, as elsewhere, $\|\cdot\|_\infty$ denotes the entrywise maximum absolute value of the matrix.)*

**Proof** Denote the rows of $B$ as $\mathbf{u}^1, \ldots, \mathbf{u}^k$ where each $\mathbf{u}^\ell \in \mathbb{R}^M$. Consider the Gram–Schmidt orthogonalization of these vectors: for each $\ell \leqslant k$, we decompose

$$\mathbf{u}^\ell \equiv \mathbf{u}^{\ell,\|} + \mathbf{u}^{\ell,\perp} \equiv \sum_{j \leqslant \ell-1} c_{\ell,j}\mathbf{u}^j + \mathbf{u}^{\ell,\perp}$$

where $\mathbf{u}^{\ell,\|}$ is the orthogonal projection of $\mathbf{u}^\ell$ onto the span of $\mathbf{u}^1, \ldots, \mathbf{u}^{\ell-1}$. Then for all $j \leqslant \ell - 1$ we must have

$$0 = (\mathbf{u}^{\ell,\perp}, \mathbf{u}^j) = (\mathbf{u}^\ell, \mathbf{u}^j) - \sum_{i \leqslant \ell-1} \mathbf{1}\{i \neq j\} c_{\ell,i}(\mathbf{u}^i, \mathbf{u}^j) - c_{\ell,j}\|\mathbf{u}^j\|^2.$$

Abbreviate $\epsilon \equiv \epsilon(k) \equiv 1/(3k)$, so the assumptions imply that $\|\mathbf{u}^j\|^2 \geqslant 1 - \epsilon$ while $|(\mathbf{u}^i, \mathbf{u}^j)| \leqslant \epsilon$ for all $i \neq j$. Rearranging the above gives an upper bound for $|c_{\ell,j}|$ in terms of the other coefficients $c_{\ell,i}$ $(i \neq j)$. If we further denote $c_{\max} \equiv \max\{|c_{\ell,j}| : \ell \leqslant k, j \leqslant \ell - 1\}$, then we have

$$c_{\max} \leqslant \frac{\epsilon}{1-\epsilon}\left\{1 + (k-2)c_{\max}\right\}.$$

Rearranging the inequality gives the bound

$$c_{\max} \leqslant \frac{\epsilon}{1-\epsilon}\bigg/\left(1 - \frac{\epsilon(k-2)}{1-\epsilon}\right) = \frac{\epsilon}{1-\epsilon(k-1)} \leqslant \frac{3\epsilon}{2}.$$

From this bound we can deduce that for all $\ell \leqslant k$ we have

$$\|\mathbf{u}^{\ell,\|}\|^2 = \left\|\sum_{j \leqslant \ell-1} c_{\ell,j}\mathbf{u}^j\right\|^2 \leqslant \left(\frac{3\epsilon}{2}\right)^2\left\{(\ell-1)(1+\epsilon) + (\ell-1)(\ell-2)\epsilon\right\} \leqslant \left(\frac{3\epsilon}{2}\right)^2\frac{4k}{3} = \epsilon.$$

It follows that $\|\mathbf{u}^{\ell,\perp}\|^2 = \|\mathbf{u}^\ell\|^2 - \|\mathbf{u}^{\ell,\|}\|^2 \geqslant 1-2\epsilon$. (We also have trivially $\|\mathbf{u}^{\ell,\perp}\|^2 \leqslant \|\mathbf{u}^\ell\|^2 \leqslant 1+\epsilon$.) Let $R$ denote the Gram–Schmidt matrix, so $R$ is $k \times k$ lower triangular with entries

$$R_{\ell,j} = \frac{1}{\|\mathbf{u}^{\ell,\perp}\|}\bigg\{\mathbf{1}\{\ell = j\} - \mathbf{1}\{\ell < j\} c_{\ell,j}\bigg\}\,.$$

Since $R$ is lower triangular, its determinant is simply the product of its diagonal entries, so

$$\frac{1}{(1+\epsilon)^k} \leqslant \det R = \prod_{\ell \leqslant k} \frac{1}{\|\mathbf{u}^{\ell,\perp}\|} \leqslant \frac{1}{(1-2\epsilon)^k}\,.$$

By construction, $\acute{B} = RB$ is a $k \times M$ matrix with orthonormal rows, so Lemma E.6 implies that $\acute{B}$ has a $k \times k$ submatrix $\acute{U}$ with

$$|\det \acute{U}| \geqslant \left(\frac{k!}{M^k}\right)^{1/2}.$$

Therefore $U = R^{-1}\acute{U}$ is a $k \times k$ submatrix of the original matrix $B$, with

$$|\det U| = \frac{|\det \acute{U}|}{\det R} \geqslant (1-2\epsilon)^k \left(\frac{k!}{M^k}\right)^{1/2} = \left(1 - \frac{2}{3k}\right)^k \left(\frac{k!}{M^k}\right)^{1/2} \geqslant \frac{1}{3}\left(\frac{k!}{M^k}\right)^{1/2},$$

where the bound holds for all $k \geqslant 1$. ■

**Lemma E.8** *Suppose $U$ satisfies Assumption 1 and 2. Recall from (44) that the matrix $\mathbf{c}[t-1]$ is $(t-1) \times M$ with orthonormal rows. Let $M(L) \subseteq [M]$ be as defined in the proof of Lemma E.2 (see (194)). If $B = B(L)$ is the submatrix of $\mathbf{c}[t-1]$ with column indices in $M(L)$, then with high probability it satisfies*

$$\|B\|_\infty \leqslant \frac{t\varsigma_t L}{(N\psi)^{1/2}}\,.$$

*It is possible to choose $L = L(t)$ large enough such that, with high probability, $\|BB^{\mathrm{t}} - I_{t-1}\|_\infty \leqslant 1/(4t)$.*

**Proof** It follows using (44) that for each $\ell \leqslant t-1$,

$$\Big((\mathbf{c}^{(\ell)})_a\Big)^2 = \bigg(\sum_{j \leqslant t-1} \frac{((\mathbf{\Gamma}_N)^{-1})_{\ell,j}(\mathbf{n}^{(j)})_a}{(N\psi)^{1/2}}\bigg)^2 \leqslant \frac{t(\varsigma_t)^2}{N\psi} \sum_{j \leqslant t-1} \Big((\mathbf{n}^{(j)})_a\Big)^2. \tag{200}$$

Applying (200) for $a \in M(L)$ gives the claimed bound on $\|B(L)\|_\infty$. On the other hand, by applying (200) for $a \notin M(L)$ and combining with the bound (195) from the proof of Lemma E.2, we find, with high probability,

$$\sum_{a \notin M(L)} \Big((\mathbf{c}^{(\ell)})_a\Big)^2 \leqslant \frac{t(\varsigma_t)^2}{N\psi} \sum_{j \leqslant t-1} \sum_{a \notin M(L)} \Big((\mathbf{n}^{(j)})_a\Big)^2 \overset{(195)}{\leqslant} \frac{Mt^2(\varsigma_t)^2}{N\psi} \cdot \frac{2t\wp_4}{L^2}\,,$$

which can be made $\leqslant 1/(4t)$ by choosing $L$ large enough. Then, for any $\ell, j \leqslant t-1$, we have

$$\bigg|\sum_{a \in M(L)} (\mathbf{c}^{(\ell)})_a (\mathbf{c}^{(j)})_a - \mathbf{1}\{\ell = j\}\bigg| = \bigg|\sum_{a \notin M(L)} (\mathbf{c}^{(\ell)})_a (\mathbf{c}^{(j)})_a\bigg| \leqslant \frac{1}{4t}\,,$$

which shows that the matrix $B = B(L)$ satisfies $\|BB^{\mathrm{t}} - I_{t-1}\|_\infty \leqslant 1/(4t)$ as desired. ■

**Corollary E.9** *Let $M(L) \subseteq [M]$ be as in Lemma E.8, where $L = L(t)$. With high probability, the matrix $\mathbf{n}[t-1]$ has disjoint $(t-1) \times (t-1)$ submatrices $A_1, \ldots, A_{\lfloor N^{0.9} \rfloor}$, all involving only columns indexed by $M(L)$, such that each $A_i$ has minimal singular value lower bounded by a positive constant $\iota_2$ (depending on $t$).*

**Proof** Let $B = B(L)$ be the submatrix of $\mathbf{c}[t-1]$ guaranteed by Lemma E.8, so

$$\|B\|_\infty \leqslant \frac{t\varsigma_t L}{(N\psi)^{1/2}}, \quad \|BB^{\mathrm{t}} - I\| \leqslant \frac{1}{4t}.$$

Then $B$ satisfies the conditions of Corollary E.7, so it has a $(t-1) \times (t-1)$ submatrix $U_1$ satisfying the determinant lower bound (199). Let $B_1$ be the matrix obtained by deleting $U_1$ from $B$. Then for all $N$ large enough we have

$$\left\|(B_1)(B_1)^{\mathrm{t}} - I_{t-1}\right\|_\infty \leqslant \frac{1}{4t} + t\left(\frac{t\varsigma_t L}{(N\psi)^{1/2}}\right)^2 \leqslant \frac{1}{3t}.$$

Thus $B_1$ also satisfies the conditions of Corollary E.7, so it has a $(t-1) \times (t-1)$ submatrix $U_2$ which also satisfies the determinant lower bound (199). Repeating the same argument, we see that with high probability the original matrix $B$ has disjoint $(t-1) \times (t-1)$ submatrices $U_1, \ldots, U_{\lfloor N^{0.9} \rfloor}$, all satisfying (199). Recalling (44), the corresponding submatrices of $\mathbf{n}[t-1]$ are given by $A_i \equiv (N\psi)^{1/2}\mathbf{\Gamma}_N U_i$, and

$$|\det A_i| \geqslant \frac{(N\psi)^{(t-1)/2}|\det U_i|}{\varsigma_t} \geqslant \left(\frac{N\psi}{M}\right)^{(t-1)/2} \frac{((t-1)!)^{1/2}}{3\varsigma_t} \equiv \hat{\iota}_2 .$$

Take any $A = A_i$, and denote its singular values $\sigma_1 \geqslant \ldots \geqslant \sigma_{t-1} \geqslant 0$. Note that $\sigma_1 \leqslant t\|A\|_\infty \leqslant tL$, where the last bound holds since $A$ only involves columns of $\mathbf{n}[t-1]$ indexed by $a \in M(L)$ (as in Lemma E.8). Then

$$\sigma_{t-1} \geqslant \frac{|\det A|}{(\sigma_1)^{t-2}} \geqslant \frac{\hat{\iota}_2}{(tL)^{t-2}} \equiv \iota_2 .$$

This concludes the proof. ■

## E.3. Fourier estimates at high frequency

The main result of this subsection is the following lemma:

**Lemma E.10 (high-frequency estimate)** *Suppose $U$ satisfies Assumption 1 and 2. With the notation of (190), it holds for any $\tau_{\max} < \infty$ and any $\epsilon_2 > 0$ that*

$$\max\left\{I_3(J, \tau, \epsilon_2) : J \in \{-1, +1\}^N, \|\pi(J)\| \leqslant \frac{4}{5}, \|\tau\| \leqslant \tau_{\max}\right\} \leqslant \frac{1}{\exp(N^{0.8})}$$

*with probability* $1 - o_N(1)$.

Towards the proof of Lemma E.10, recall that the random variable $\boldsymbol{\zeta}_a$ has density given by (182). Thus

$$\hat{p}_a(s) = \mathbb{E}\exp\Big\{\mathrm{i}s\Big(\boldsymbol{\zeta}_a - \mathbb{E}\boldsymbol{\zeta}_a\Big)\Big\} = \frac{\hat{\chi}\boldsymbol{x}_{a,c}(s)}{\exp(\mathrm{i}s\mathbb{E}\boldsymbol{\zeta}_a)}\,. \tag{201}$$

We also denote $q_{x,c}(z) \equiv U(x+cz)\varphi(z)$, and note that

$$\hat{\chi}_{x,c}(s) = \frac{\hat{q}_{x,c}(s)}{\mathbb{E}_\xi U(x+c\xi)} = \frac{\hat{q}_{x,c}(s)}{\hat{q}_{x,c}(0)}\,. \tag{202}$$

Note that Jensen's inequality implies

$$\begin{aligned}\Big|\hat{q}_{x,c}(s) - \hat{q}_{x',c'}(s)\Big| &= \bigg|\int e^{isz}\Big(U(x+cz) - U(x'+c'z)\Big)\varphi(z)\,dz\bigg| \\ &\leqslant \int \Big|U(x+cz) - U(x'+c'z)\Big|\varphi(z)\,dz\,, \end{aligned} \tag{203}$$

and the last expression is bounded by Lemma B.2.

**Corollary E.11** *Suppose $U$ satisfies Assumption 1. Given any $\epsilon > 0$ and any $L < \infty$, it is possible to choose $K$ large enough (depending on $\epsilon$ and $L$) such that*

$$\sup\bigg\{|\hat{\chi}_{x,c}(s)| : \frac{1}{2} \leqslant c \leqslant 2, |x| \leqslant L, |s| \geqslant K\bigg\} \leqslant \epsilon\,,$$

*where $\chi_{x,c}$ is as defined by* (182).

**Proof** Recall from (202) the relation

$$\hat{\chi}_{x,c}(s) = \frac{\hat{q}_{x,c}(s)}{\mathbb{E}_\xi U(x+c\xi)} = \frac{\hat{q}_{x,c}(s)}{\hat{q}_{x,c}(0)}\,.$$

By Assumption 1, the denominator $\hat{q}_{x,c}(0) = \mathbb{E}_\xi U(x+c\xi)$ is strictly positive for any given $x \in \mathbb{R}$, $c > 0$. On the other hand, it follows from Lemma B.2 and (203) that $\hat{q}_{x,c}(0)$ is continuous in $(x,c)$. It follows that

$$\inf\bigg\{\mathbb{E}_\xi U(x+c\xi) : \frac{1}{2} \leqslant c \leqslant 2, |x| \leqslant L\bigg\} < \infty$$

for any finite $L$. Therefore it suffices to show the claim with $q_{x,c}$ in place of $\chi_{x,c}$. By Lemma B.2 again, given any $\epsilon > 0$, we can choose $\eta'$ small enough such that

$$\Big\|\hat{q}_{x,c} - \hat{q}_{x',c'}\Big\|_\infty \leqslant \int \Big|U(x+cz) - U(x'+c'z)\Big|\varphi(z)\,dz \leqslant \frac{\epsilon}{2}$$

as long as $c, c' \in [1/2, 2]$, $x, x' \in [-L, L]$, and $\max\{|x-x'|, |c-c'|\} \leqslant \eta'$. Let $\{x_i\}$ be a finite $\eta'$-net of $[-L, L]$, and let $\{c_j\}$ be a finite $\eta'$-net of $[1/2, 2]$. It follows by the Riemann–Lebesgue lemma that there exists $K$ finite such that

$$\sup\bigg\{\max_{i,j}|\hat{q}_{x_i,c_j}(s)| : |s| \geqslant K\bigg\} \leqslant \frac{\epsilon}{2}\,.$$

For any $|x| \leqslant L$ and $1/2 \leqslant c \leqslant 2$, we can find $x_i, c_j$ with $\max\{|x - x_i|, |c - c_j|\} \leqslant \eta'$, so

$$\sup\left\{\hat{q}_{x,c}(s) : |s| \geqslant K\right\} \leqslant \epsilon$$

by combining the previous bounds. This concludes the proof. ■

**Corollary E.12** *Suppose $U$ satisfies Assumption 1. Let $\chi_{x,c}$ be as defined by (182). Then*

$$\sup\left\{|\hat{\chi}_{x,c}(s)| : \frac{1}{2} \leqslant c \leqslant 2, |x| \leqslant L, |s| \geqslant \epsilon\right\} \leqslant 1 - \epsilon' < 1$$

*for any finite $L$ and any $\epsilon > 0$, where $\epsilon'$ is a small positive constant depending on $U$, $L$, and $\epsilon$.*

**Proof** By Lemma E.11, we can choose $K$ large enough such that

$$\sup\left\{|\hat{\chi}_{x,c}(s)| : \frac{1}{2} \leqslant c \leqslant 2, |x| \leqslant L, |s| \geqslant K\right\} \leqslant \frac{1}{2}\,.$$

For any given $x, c$, let $\boldsymbol{\zeta}$ be a random variable with density $\chi_{x,c}$. For any $s \neq 0$,

$$|\hat{\chi}_{x,c}(s)| = \left\{\Big(\mathbb{E}\cos(s\boldsymbol{\zeta})\Big)^2 + \Big(\mathbb{E}\sin(s\boldsymbol{\zeta})\Big)^2\right\}^{1/2} < 1$$

by Jensen's inequality. It follows from Lemma B.2 and (203) that $\hat{\chi}_{x,c}(s)$ is continuous in $(x, c, s)$, so

$$\sup\left\{|\hat{\chi}_{x,c}(s)| : \frac{1}{2} \leqslant c \leqslant 2, |x| \leqslant L, \epsilon \leqslant |s| \leqslant K\right\} < 1$$

by compactness considerations. The claim follows. ■

**Proof** [Proof of Lemma E.10] For any subset of indices $T = \{i(1), \ldots, i(t-1)\} \subseteq [M]$ denote

$$\phi_T(\mathfrak{s}) \equiv \prod_{\ell \leqslant t-1} \hat{p}_{i(\ell)}(\mathfrak{s}_\ell)$$

for $\mathfrak{s} \in \mathbb{R}^{t-1}$. It follows from (201) and Plancherel's identity that the $L^2$ norm of the function $\hat{p}_a(s)$ is the same as the $L^2$ norm of the function $\chi_{\boldsymbol{X}_a,c}(s)$ defined by (182). We also note that Assumption 1 implies

$$\|\chi_{x,c}\|^2 = \int \frac{U(x+cz)^2\varphi(z)^2}{(\mathbb{E}_\xi U(x+c\xi))^2}\,dz \leqslant \frac{1}{(1\pi)^{1/2}} \int \frac{U(x+cz)\varphi(z)}{(\mathbb{E}_\xi U(x+c\xi))^2}\,dz = \frac{1}{\mathbb{E}_\xi U(x+c\xi)}\,.$$

By compactness considerations (similarly as for (90)), we must have

$$\inf\left\{\mathbb{E}_\xi U(x+c\xi) : \frac{1}{2} \leqslant c \leqslant 2, |x| \leqslant L'\right\} \geqslant \bar{c}_1(U, L')\,.$$

If $T \subseteq M(L)$ (as defined by Lemma E.8), then it follows by combining the above with (197) that

$$\|\phi_T\|_2 = \prod_{\ell \leqslant t-1} \|p_{i(\ell)}\|_2 \leqslant \left(\sup\left\{\|\chi_{x,c}\|_2 : \frac{1}{2} \leqslant c \leqslant 2, |x| \leqslant L\right\}\right)^{t-1} \leqslant \left(\frac{1}{\bar{c}_1(U, L')}\right)^t \equiv \wp_5\,.$$

Now let $A_1, \ldots, A_{\lfloor N^{0.9} \rfloor}$ be the submatrices of $\mathbf{n}[t-1]$ guaranteed (with high probability) by Corollary E.9. Let $T_i$ denote the subset of column indices involved in $A_i$, and note

$$|\hat{p}(\mathfrak{s})| \leqslant \prod_{i \leqslant \lfloor N^{0.9} \rfloor} \left| \phi_{T_i}\left( \frac{(A_i)^{\mathsf{t}}\mathfrak{s}}{N^{1/2}} \right) \right| .$$

Moreover, each individual factor $\phi_{T_i}$ has modulus at most one. Combining with the preceding $L^2$ bound gives

$$\int \left| \phi_{T_i}\left( \frac{(A_i)^{\mathsf{t}}\mathfrak{s}}{N^{1/2}} \right) \right|^2 d\mathfrak{s} = \frac{N^{(t-1)/2}(\|\phi_{T_i}\|_2)^2}{|\det A_i|} \leqslant \frac{N^{(t-1)/2}(\wp_5)^2}{(\iota_2)^{t-1}} .$$

It follows using the Cauchy–Schwarz inequality that

$$\int \left| \phi_{T_1}\left( \frac{(A_1)^{\mathsf{t}}\mathfrak{s}}{N^{1/2}} \right) \phi_{T_2}\left( \frac{(A_2)^{\mathsf{t}}\mathfrak{s}}{N^{1/2}} \right) \right| d\mathfrak{s} \leqslant \frac{N^{(t-1)/2}(\wp_5)^2}{(\iota_2)^{t-1}} .$$

On the other hand, if $\|\mathfrak{s}\| \geqslant \epsilon_2 N^{1/2}$, then the least singular value bound from Corollary E.9 implies

$$\max \left\{ \frac{|(\mathfrak{s}, \mathbf{n}_a)|}{N^{1/2}} : a \in T_i \right\} = \frac{\|(A_i)^{\mathsf{t}}\mathfrak{s}\|_\infty}{N^{1/2}} \geqslant \frac{\|(A_i)^{\mathsf{t}}\mathfrak{s}\|}{(Nt)^{1/2}} \geqslant \frac{\iota_2 \epsilon_2}{t^{1/2}} .$$

Recall again that for $a \in M(L)$, $|\boldsymbol{X}_a|$ is bounded by (197). Combining with the result of Corollary E.12 gives

$$\left| \phi_{T_i}\left( \frac{(A_i)^{\mathsf{t}}\mathfrak{s}}{N^{1/2}} \right) \right| \leqslant \sup \left\{ |\hat{\chi}_{x,c}(s)| : \frac{1}{2} \leqslant c \leqslant 2, |x| \leqslant L', |s| \geqslant \frac{\iota_2 \epsilon_2}{t^{1/2}} \right\} \leqslant 1 - \epsilon' < 1 .$$

To conclude we note that the quantity $I_3(J, \tau, \epsilon_2)$ from (190) can be bounded by $I_{3,g} + I_{3,p}$ where $I_{3,g}$ is the integral of $\hat{g}_{J,\tau}$, while $I_{3,p}$ is the integral of $\hat{p}_{J,\tau}$. By (187) and Lemma E.2, we have with high probability

$$I_{3,g} \equiv \int \left| \hat{g}_{J,\tau}(\mathfrak{s}) \right| \mathbf{1}\left\{ \|\mathfrak{s}\| \geqslant \epsilon_2 N^{1/2} \right\} d\mathfrak{s} \leqslant \frac{1}{\exp(N^{0.9})} .$$

By the previous calculations, we also have with high probability

$$\begin{aligned} I_{3,p} &\leqslant \left\{ \int \left| \prod_{i=1,2} \phi_{T_i}\left( \frac{(A_i)^{\mathsf{t}}\mathfrak{s}}{N^{1/2}} \right) \right| d\mathfrak{s} \right\} \cdot \sup \left\{ \prod_{i=3}^{N^{0.9}} \left| \phi_{T_i}\left( \frac{(A_i)^{\mathsf{t}}\mathfrak{s}}{N^{1/2}} \right) \right| : |\mathfrak{s}| \geqslant \epsilon_2 N^{1/2} \right\} \\ &\leqslant \frac{N^{(t-1)/2}(\wp_5)^2}{(\iota_2)^{t-1}} (1 - \epsilon')^{N^{0.85}} \leqslant \frac{1}{\exp(N^{0.8})} . \end{aligned}$$

This concludes the proof. ■

### E.4. Conclusion of local CLT

In this concluding subsection we prove the local CLT Proposition E.1, and apply it to deduce Propositions E.13 and E.14.

**Proof** [Proof of Proposition E.1] Recall that $\hat{p}_{J,\tau}$ and $\hat{g}_{J,\tau}$ are defined by (186) and (187). It follows by combining Lemmas E.4, E.5, and E.10 that for any finite constant $\tau_{\max}$, we have

$$\sup\left\{\int\left|\hat{p}_{J,\tau}(\mathfrak{s})-\hat{g}_{J,\tau}(\mathfrak{s})\right|d\mathfrak{s} : J\in\{-1,+1\}^N, \|\pi(J)\|\leqslant\frac{4}{5}, \|\tau\|\leqslant\tau_{\max}\right\}\leqslant\frac{1}{N^{0.35}}$$

with high probability. Inverting the Fourier transform shows that, with high probability, the random variable $\boldsymbol{W}$ from (184) has a bounded continuous density function $p_{J,\tau}$, which satisfies

$$\sup\left\{\|p_{J,\tau}-g_{J,\tau}\|_\infty : J\in\{-1,+1\}^N, \|\pi(J)\|\leqslant\frac{4}{5}, \|\tau\|\leqslant\tau_{\max}\right\}\leqslant\frac{1}{(2\pi)^{t-1}N^{0.35}}\leqslant\frac{1}{N^{0.3}},$$

as claimed. ■

We now define the transformed gaussian density

$$\mathbf{g}_{J,\tau}(z)\equiv\psi^{1/2}|\det\mathbf{\Gamma}_N|g_{J,\tau}\left(\psi^{1/2}\mathbf{\Gamma}_N(z-N^{1/2}\tau)-\frac{\mathbf{n}[t-1]\mathbb{E}\boldsymbol{\zeta}}{N^{1/2}}\right), \tag{204}$$

where $\mathbb{E}\boldsymbol{\zeta}$ is as in (183).

**Proposition E.13 (density bound for first moment)** *Suppose $U$ satisfies Assumptions 1 and 2. Then we have*

$$\sup\left\{\left\|\mathbf{p}_{J,\tau}(\cdot\,|\,\bar{g}_{\mathrm{R}})-\mathbf{g}_{J,\tau}(\cdot)\right\|_\infty : J\in\{-1,+1\}^N, \|\tau\|\leqslant\tau_{\max}\right\}\leqslant\frac{1}{N^{0.25}}$$

*with high probability, where $\mathbf{p}_{J,\tau}(\cdot\,|\,\bar{g}_{\mathrm{R}})$ is as in (72), while $\mathbf{g}_{J,\tau}$ is as in (204).*

**Proof** Recall that Proposition E.1 above estimates the density $p_{J,\tau}$ of the random variable $\boldsymbol{W}$ from (184),

$$\boldsymbol{W}=\frac{\mathbf{n}[t-1](\boldsymbol{\zeta}-\mathbb{E}\boldsymbol{\zeta})}{N^{1/2}}\in\mathbb{R}^{t-1}, \tag{205}$$

where each $\boldsymbol{\zeta}_a$ has density given by (182). On the other hand, let $\boldsymbol{\xi}\in\mathbb{R}^M$ be a random vector with independent coordinates, such that $\boldsymbol{\xi}_a$ has density

$$\tilde{p}_a(z)\cong U\Big((\tilde{\boldsymbol{X}}_J)_a+cz\Big)\exp\left\{N^{1/2}\tau^{\mathrm{t}}\mathbf{c}[t-1]\mathbf{e}_a z\right\}\varphi(z),$$

where $c=c(\pi(J))$, $\tilde{\boldsymbol{X}}_J$ is as in Lemma A.20, and $\cong$ denotes equality up to a normalizing constant. We see from (72) that $\mathbf{p}_{J,\tau}(\cdot\,|\,\bar{g}_{\mathrm{R}})$ is the density of the random variable $\mathbf{c}[t-1]\boldsymbol{\xi}$, for $\boldsymbol{\xi}$ as we have just described. Note that

$$\begin{aligned}\tilde{p}_a\Big(z+N^{1/2}\tau^{\mathrm{t}}\mathbf{c}[t-1]\mathbf{e}_a\Big)&\cong U\Big((\tilde{\boldsymbol{X}}_J)_a+c\Big\{z+N^{1/2}\tau^{\mathrm{t}}\mathbf{c}[t-1]\mathbf{e}_a\Big\}\Big)\varphi(z)\\&\overset{(181)}{=}U\Big((\boldsymbol{X}_{J,\tau})_a+cz\Big)\varphi(z)\overset{(182)}{\cong}\chi_{\boldsymbol{X}_a,c}(z),\end{aligned}$$

so it follows that $\boldsymbol{\xi} - N^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\tau$ is equidistributed as $\boldsymbol{\zeta}$ for $\boldsymbol{\zeta}$ as in (205). Thus $\mathbf{p}_{J,\tau}(\cdot \,|\, \bar{g}_{\mathrm{R}})$ is the same as the density of

$$\mathbf{c}[t-1]\Big(\boldsymbol{\zeta} + N^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\tau\Big) \overset{(44)}{=} \frac{(\boldsymbol{\Gamma}_N)^{-1}\mathbf{n}[t-1]\boldsymbol{\zeta}}{(N\psi)^{1/2}} + N^{1/2}\tau$$
$$\overset{(72)}{=} \frac{(\boldsymbol{\Gamma}_N)^{-1}\boldsymbol{W}}{\psi^{1/2}} + \frac{(\boldsymbol{\Gamma}_N)^{-1}\mathbf{n}[t-1]\mathbb{E}\boldsymbol{\zeta}}{(N\psi)^{1/2}} + N^{1/2}\tau\,.$$

It follows by making a change of variables that

$$\mathbf{p}_{J,\tau}(z \,|\, \bar{g}_{\mathrm{R}}) = \psi^{1/2}|\det \boldsymbol{\Gamma}_N| p_{J,\tau}\bigg(\psi^{1/2}\boldsymbol{\Gamma}_N(z - N^{1/2}\tau) - \frac{\mathbf{n}[t-1]\mathbb{E}\boldsymbol{\zeta}}{N^{1/2}}\bigg)\,.$$

Comparing with (204), we have

$$\Big\|\mathbf{p}_{J,\tau}(\cdot \,|\, \bar{g}_{\mathrm{R}}) - \mathbf{g}_{J,\tau}(\cdot)\Big\|_\infty = \psi^{1/2}|\det \boldsymbol{\Gamma}_N| \Big\| p_{J,\tau} - g_{J,\tau}\Big\|_\infty\,,$$

so the result follows from Proposition E.1. ■

**Proposition E.14 (density bound for second moment)** *Suppose $U$ satisfies Assumptions 1 and 2. Then the bound (164) holds with high probability, where $\mathbf{p}_{K|J,\tau}(\cdot \,|\, \bar{g}_{\mathrm{R}}, \boldsymbol{\zeta})$ is as in (162).*

**Proof** Through we abbreviate $c = c(\pi(K))$. First we slightly modify the definition from (182): let $\boldsymbol{\sigma} \in \mathbb{R}^M$ be a random vector with independent coordinates, such that each $\boldsymbol{\sigma}_a$ has density given by $\chi_{\boldsymbol{X}_a, e(\lambda)}$ for

$$\boldsymbol{X} = \boldsymbol{X}_{K|J,\tau}(\boldsymbol{\zeta}) \equiv \tilde{\boldsymbol{X}}_K + c \cdot \bigg(\lambda\boldsymbol{\zeta} + (1-\lambda^2)^{1/2}N^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\tau\bigg)$$

and $e(\lambda) = c \cdot (1-\lambda^2)^{1/2}$. In this definition, $\tilde{\boldsymbol{X}}_K$ is as in Lemma D.8, and $\lambda = \lambda(J, K)$. We define also (cf. (184))

$$\boldsymbol{W}' \equiv \frac{\mathbf{n}[t-1](\boldsymbol{\sigma} - \mathbb{E}\boldsymbol{\sigma})}{N^{1/2}} \in \mathbb{R}^{t-1}\,. \tag{206}$$

On the other hand, let $\boldsymbol{\xi} \in \mathbb{R}^M$ be a random vector with independent coordinates, such that $\xi_a$ has density

$$\tilde{p}_a(z) \cong U\bigg((\tilde{\boldsymbol{X}}_K)_a + c\Big(\lambda\boldsymbol{\zeta}_a + (1-\lambda^2)^{1/2}z\Big)\bigg) \exp\Big\{N^{1/2}\tau^{\mathrm{t}}\mathbf{c}[t-1]\mathbf{e}_a z\Big\}\varphi(z)\,.$$

We see from (162) that $\mathbf{p}_{K|J,\tau}(\cdot \,|\, \bar{g}_{\mathrm{R}}, \boldsymbol{\zeta})$ is the density of the random variable $\mathbf{c}[t-1]\boldsymbol{\xi}$. Note that

$$\tilde{p}_a\bigg(z + N^{1/2}\tau^{\mathrm{t}}\mathbf{c}[t-1]\mathbf{e}_a\bigg) \cong U\bigg(\boldsymbol{X}_{K|J,\tau}(\boldsymbol{\zeta}) + c \cdot (1-\lambda^2)^{1/2}z\bigg)\varphi(z) \cong \chi_{\boldsymbol{X}_a, e(\lambda)}\,,$$

which implies that $\boldsymbol{\xi} - N^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\tau$ is equidistributed as $\boldsymbol{\sigma}$. Thus $\mathbf{p}_{K|J,\tau}(\cdot \,|\, \bar{g}_{\mathrm{R}}, \boldsymbol{\zeta})$ is the same as the density of

$$\mathbf{c}[t-1]\Big(\boldsymbol{\sigma} + N^{1/2}\mathbf{c}[t-1]^{\mathrm{t}}\tau\Big) = \frac{(\boldsymbol{\Gamma}_N)^{-1}\boldsymbol{W}'}{\psi^{1/2}} + \frac{(\boldsymbol{\Gamma}_N)^{-1}\mathbf{n}[t-1]\mathbb{E}\boldsymbol{\sigma}}{(N\psi)^{1/2}} + N^{1/2}\tau$$

for $\boldsymbol{\sigma}$ and $\boldsymbol{W}'$ as defined above. It follows by a minor modification of Proposition E.1 (replacing $\boldsymbol{W}$ from (184) with $\boldsymbol{W}'$ from (206)) that $\mathbf{p}_{K|J,\tau}(\cdot \,|\, \bar{g}_{\mathrm{R}}, \boldsymbol{\zeta})$ can be uniformly approximated by a gaussian density. The claim follows. ■

## Appendix F. Concentration of partition function

In this section we prove Propositions 1.6, 1.7, and 1.9; and use these to conclude the proof of Theorem 1.1. The section is organized as follows:

- As commented earlier, both Propositions 1.6 and 1.7 rely on a bound for near-isotropic gaussian processes, Proposition F.1, which is proved in §F.1. See Remark F.2 for further discussion of this result.
- In §F.2 we give the proof of Proposition 1.6.
- In §F.3 we give the proof of Proposition 1.9, and use this to deduce that the free energy of the smoothed model (22) is given by the replica symmetric formula (Corollary F.10).
- In §F.4 we give the proof of Proposition 1.7, and conclude the proof of Theorem 1.1.

Recall from §1.4 that Assumption 1 implies (20), where we can assume without loss that $E(U) \subseteq [-E_{\max}(U), E_{\max}(U)]$ for some finite $E_{\max}(U)$.

### F.1. Bounds for near-isotropic gaussian processes

The following is a variant of (Talagrand, 2011b, Cor. 8.2.5):

**Proposition F.1** *Let $c \in (0, 1/12]$. Let $\mathbf{v}^1, \ldots, \mathbf{v}^n$ be unit vectors in $\mathbb{R}^n$ such that $(\mathbf{v}^i, \mathbf{v}^j) \leqslant c$ for all $i \neq j$. Then*

$$\mathbb{P}\bigg(\frac{1}{n}\Big|\Big\{i \leqslant n : (\mathbf{g}, \mathbf{v}^i) \in E(U)\Big\}\Big| \leqslant \gamma\bigg) \leqslant \gamma^{1/(25c)}$$

*for all $\log(5/c)/(\log n) \leqslant \gamma \leqslant \gamma_0 = \gamma_0(|E(U)|, E_{\max}(U))$ and $n$ large enough.*

**Remark F.2** *We point out that there are two main differences between Proposition F.1 and (Talagrand, 2011b, Cor. 8.2.5). First, (Talagrand, 2011b, Cor. 8.2.5) considers the event $\{(\mathbf{g}, \mathbf{v}^i) \geqslant a\}$, and the proof relies crucially on Gordon's inequality. By contrast, Proposition F.1 considers the event $\{(\mathbf{g}, \mathbf{v}^i) \in E(U)\}$, where it does not seem possible to apply standard gaussian comparison inequalities. As a result we rely on more ad hoc arguments which yield a weaker bound, in the sense that (Talagrand, 2011b, Cor. 8.2.5) holds for $\gamma$ polynomially small in $n$ while Proposition F.1 holds only for $\gamma$ decaying logarithmically in $n$.*

The proof of Proposition F.1 is given at the end of this subsection. We begin with some preparatory lemmas:

**Lemma F.3 (used in proof of Lemma F.4)** *Let $c \in (0, 1)$ and denote $\eta'(c) = 1/\log(4/c)$. For any $K \in \mathbb{N}$ there exists $n_0(c, K) < \infty$ such that the following holds for all $n \geqslant n_0(c, K)$: if $\mathbf{v}^1, \ldots, \mathbf{v}^n$ are unit vectors in $\mathbb{R}^n$ and $m \leqslant \eta'(c) \log n$, then there must exist $K$ distinct indices $m < i_1 < \ldots < i_K \leqslant n$ such that*

$$\max\bigg\{\Big\|P_m\Big(\mathbf{v}^{i_a} - \mathbf{v}^{i_b}\Big)\Big\| : a, b \leqslant K\bigg\} \leqslant c\,,$$

*where $P_m$ denotes the orthogonal projection onto the span of $\{\mathbf{v}^1, \ldots, \mathbf{v}^m\}$.*

**Proof** Suppose for contradiction that for all $m < i_1 < \ldots < i_K \leqslant n$ we have

$$\max\left\{\left\|P_m\left(\mathbf{v}^{i_a} - \mathbf{v}^{i_b}\right)\right\| : a, b \leqslant K\right\} > c\,. \tag{207}$$

Let $U$ denote the *disjoint* union of $U_{m+1}, \ldots, U_n$, where $U_i$ is a *copy* of

$$B_m\left(P_m\mathbf{v}^i, \frac{c}{2}\right) \equiv \left(\operatorname{span}\left\{\mathbf{v}^1, \ldots, \mathbf{v}^m\right\}\right) \cap B\left(P_m\mathbf{v}^i, \frac{c}{2}\right).$$

Note that if $x \in B(P_m\mathbf{v}^i, c/2)$ then $\|x\| \leqslant \|P_m\mathbf{v}^i\| + c/2 \leqslant 3/2$, so we have a natural mapping $i : U \to B_m(\mathbf{0}, 3/2)$. By the assumption (207), each point in $B_m(\mathbf{0}, 3/2)$ has at most $K-1$ distinct preimages under the mapping $i$, so

$$(n-m)\operatorname{vol} B\left(P_m\mathbf{v}^i, \frac{c}{2}\right) = \operatorname{vol} U \leqslant (K-1)\operatorname{vol} B_m\left(\mathbf{0}, \frac{3}{2}\right).$$

If $m' = \dim\operatorname{span}\{\mathbf{v}^1, \ldots, \mathbf{v}^m\} \leqslant m$, then it follows that

$$n - m \leqslant (K-1)\left(\frac{3/2}{c/2}\right)^{m'} \leqslant K\left(\frac{3}{c}\right)^{\eta'(c)\log n} = K\exp\left\{\frac{\log(3/c)}{\log(4/c)}\log n\right\},$$

which yields a contradiction for $n$ large enough (depending on $c$ and $K$). ■

**Lemma F.4** *Let $c \in (0,1)$ and denote $\eta'(c) = 1/\log(4/c)$. There exists $n_0(c) < \infty$ such that the following holds for all $n \geqslant n_0(c)$: if $\mathbf{v}^1, \ldots, \mathbf{v}^n$ are unit vectors in $\mathbb{R}^n$ with $(\mathbf{v}^i, \mathbf{v}^j) \leqslant c$ for all $i \neq j$, then the vectors can be re-indexed in such a way that*

$$\max\left\{\left\|P_m\mathbf{v}^{m+1}\right\| : 1 \leqslant m \leqslant \eta'(c)\log n\right\} \leqslant (3c)^{1/2},$$

*where $P_m$ denotes the orthogonal projection onto the span of $\{\mathbf{v}^1, \ldots, \mathbf{v}^m\}$. (The claim is non-trivial only if $c < 1/3$.)*

**Proof** We shall assume the vectors are indexed such that for all $1 \leqslant \ell \leqslant n$ we have

$$\left\|P_{\ell-1}\mathbf{v}^\ell\right\| = \min\left\{\left\|P_{\ell-1}\mathbf{v}^k\right\| : \ell \leqslant k \leqslant n\right\}. \tag{208}$$

Now suppose for the sake of contradiction that for some $m \leqslant \eta'(c)\log n$ we have

$$\left\|P_m\mathbf{v}^{m+1}\right\| \overset{(208)}{=} \min\left\{\left\|P_m\mathbf{v}^k\right\| : m+1 \leqslant k \leqslant n\right\} > (3c)^{1/2}. \tag{209}$$

Take $K = 2 + \lceil 1/c\rceil$. By Lemma F.3, for all $n$ large enough we can find indices $m < i_1 < \ldots < i_K \leqslant n$ such that

$$\max\left\{\left\|P_m\left(\mathbf{v}^{i_a} - \mathbf{v}^{i_b}\right)\right\| : a, b \leqslant K\right\} \leqslant c\,. \tag{210}$$

As a consequence, for any $a \neq b$ where $a, b \leqslant K$, we have

$$\begin{aligned}\Big((I-P_m)\mathbf{v}^{i_a},(I-P_m)\mathbf{v}^{i_b}\Big) &= (\mathbf{v}^{i_a},\mathbf{v}^{i_b}) - (P_m\mathbf{v}^{i_a},P_m\mathbf{v}^{i_b}) \\ &= -\|P_m\mathbf{v}^{i_a}\|^2 + \Big\{(\mathbf{v}^{i_a},\mathbf{v}^{i_b}) - \Big(P_m\mathbf{v}^{i_a},P_m(\mathbf{v}^{i_b}-\mathbf{v}^{i_a})\Big)\Big\} \leqslant -c\,,\end{aligned}$$

where the last bound uses (209), (210), and the assumption that $(\mathbf{v}^i,\mathbf{v}^j) \leqslant c$ for all $i \neq j$. If we let

$$\mathbf{x}^a \equiv \frac{(I-P_m)\mathbf{v}^{i_a}}{\|(I-P_m)\mathbf{v}^{i_a}\|}\,,$$

then the above implies that $(\mathbf{x}^a,\mathbf{x}^b) \leqslant -c$ for all $a \neq b$. It follows that

$$0 \leqslant \Big\|\sum_{a\leqslant K}\mathbf{x}^a\Big\|^2 = \sum_{a,b\leqslant K}(\mathbf{x}^a,\mathbf{x}^b) \leqslant K\Big(1-c(K-1)\Big)\,,$$

which gives a contradiction since we chose $K \geqslant 2+1/c$. ■

**Lemma F.5** *Let $\mathbf{v}^1,\ldots,\mathbf{v}^m$ be unit vectors in $\mathbb{R}^n$ (for any $m,n$) such that*

$$\max\Big\{\Big\|P_{\ell-1}\mathbf{v}^\ell\Big\| : 1 \leqslant \ell \leqslant m\Big\} \leqslant c' \leqslant \frac{1}{2}\,,$$

*where $P_{\ell-1}$ denotes the orthogonal projection onto the span of $\{\mathbf{v}^1,\ldots,\mathbf{v}^{\ell-1}\}$. Let $\mathbf{g}$ be a standard gaussian random vector in $\mathbb{R}^n$. There exists $\gamma_0 = \gamma_0(|E(U)|, E_{\max}(U)) > 0$ such that*

$$\mathbb{P}\bigg(\frac{1}{m}\Big|\Big\{i \leqslant m : (\mathbf{g},\mathbf{v}^i) \in E(U)\Big\}\Big| \leqslant \gamma\bigg) \leqslant \gamma^{1/(8(c')^2)}$$

*for all $1/m \leqslant \gamma \leqslant \gamma_0$.*

**Proof** We shall assume without loss that $m\gamma$ is integer-valued. Let $u_i \equiv (\mathbf{g},\mathbf{v}^i)$, so that $(u_i)$ defines a (centered) gaussian random vector indexed by $i \leqslant n$. For each $i$ we can decompose $u_i \equiv \zeta_i + \xi_i$ where $\zeta_i \equiv (\mathbf{g}, P_{i-1}\mathbf{v}^i)$; at the first step $\zeta_1 = 0$. Define a parameter

$$s \equiv s(U) \leqslant \max\bigg\{10, E_{\max}(U), \Big(\Big|\log|E(U)|\Big|\Big)^{1/2}\bigg\}\,, \tag{211}$$

and define the random subset of indices

$$B \equiv \Big\{i \leqslant m : |\zeta_i| \leqslant s\Big\}\,.$$

Let $\Omega_\gamma$ denote the event of interest,

$$\Omega_\gamma \equiv \bigg\{\frac{1}{m}\Big|\Big\{i \leqslant m : u_i \in E(U)\Big\}\Big| \leqslant \gamma\bigg\}\,.$$

On the event $\Omega_\gamma$ there must be a subset $A \subseteq [m]$ of size $m\gamma$ such that $u_i \notin E(U)$ for all $i \notin A$. Therefore

$$\mathbb{P}(\Omega_\gamma) \leqslant \mathbb{P}\bigg(|B| \leqslant \frac{m}{2}\bigg) + \sum_{|A|=m\gamma} \mathbb{P}\bigg(u_i \notin E(U)\ \forall i \notin A; |B| > \frac{m}{2}\bigg)\,. \tag{212}$$

To bound the above we will consider a fixed subset $A$, without loss $A = \{m - m\gamma + 1, \ldots, m\}$. Define

$$\mathscr{G}_\ell \equiv \sigma\bigg((\zeta_i, \xi_i) : 1 \leqslant i \leqslant \ell\bigg)\,.$$

Let $\tau_0 \equiv 0$ and define the increasing sequence

$$\tau_\ell \equiv \inf\bigg\{i > \tau_{\ell-1} : i \leqslant m, |\zeta_i| \leqslant s\bigg\}\,.$$

Note that since $\zeta_\ell \in \mathscr{G}_{\ell-1}$, the $\tau_\ell$ are stopping times with respect to the filtration $\mathscr{G}_\ell$. We take the usual convention that $\inf \varnothing \equiv \infty$, so the set of finite stopping times corresponds exactly to the set $B$. Let $f(i) \equiv \mathbf{1}\{u_i \notin E(U)\}$. It follows from the assumption that $\xi_i$ has the law of a gaussian random variable which is independent of $\mathscr{G}_i$, and has variance between $1 - (c')^2 \geqslant 3/4$ and 1. Therefore we have

$$\begin{aligned} p_\ell \equiv \mathbb{E}\bigg(\mathbf{1}\{\tau_\ell < \infty\} f(\tau_\ell) \,\bigg|\, \mathscr{G}_{\tau_\ell - 1}\bigg) &= \mathbf{1}\{\tau_\ell < \infty\}\mathbb{P}\bigg(u_{\tau_\ell} = \zeta_{\tau_\ell} + \xi_{\tau_\ell} \notin E(U) \,\bigg|\, \mathscr{G}_{\tau_\ell - 1}\bigg) \\ &\leqslant \max\bigg\{\mathbb{P}\bigg(Z \notin \frac{E(U) - x}{\lambda}\bigg) : \bigg(\frac{3}{4}\bigg)^{1/2} \leqslant \lambda \leqslant 1, |x| \leqslant s\bigg\}\,. \end{aligned}$$

To bound the above, note that the set $\lambda^{-1}(E(U) - x)$ has Lebesgue measure at least $|E(U)|$ (since $\lambda \leqslant 1$), and is contained in the interval $[-5s/2, 5s/2]$ (by the assumption $s \geqslant E_{\max}(U)$ from (211), together with the restriction $\lambda \geqslant (3/4)^{1/2}$). It follows that

$$p_\ell \leqslant 1 - |E(U)|\varphi\bigg(\frac{5s}{2}\bigg) \leqslant 1 - \frac{1}{(2\pi)^{1/2}} \exp\bigg\{-\frac{7s^2}{2}\bigg\}\,,$$

where the last bound uses the assumption $s^2 \geqslant |\log|E(U)||$ from (211). It then follows by iterated expectations that

$$\begin{aligned} \mathbb{P}\bigg(u_i \notin E(U)\ \forall i \notin A; |B| > \frac{m}{2}\bigg) &\leqslant \mathbb{E}\bigg[\prod_{j \leqslant m/2} \mathbf{1}\{\tau_j < \infty\} f(\tau_j)\bigg] \\ &\leqslant \mathbb{E}\bigg[\bigg(\prod_{j \leqslant m/2 - 1} \mathbf{1}\{\tau_j < \infty\} f(\tau_j)\bigg)\mathbb{E}\bigg(\mathbf{1}\{\tau_{\lceil m/2\rceil} < \infty\} f(\tau_{\lceil m/2\rceil}) \,\bigg|\, \mathscr{G}_{\tau_{\lceil m/2\rceil} - 1}\bigg)\bigg] \\ &\leqslant \bigg(1 - \frac{1}{(2\pi)^{1/2}} \exp\bigg\{-\frac{7s^2}{2}\bigg\}\bigg)^{m/2} \leqslant \exp\bigg\{-\frac{m\exp(-7s^2/2)}{2(2\pi)^{1/2}}\bigg\}\,. \end{aligned}$$

Substituting this bound into (212) and accounting for the number of choices of $A$ gives

$$\mathbb{P}(\Omega_\gamma) \leqslant \mathbb{P}\bigg(|B| \leqslant \frac{m}{2}\bigg) + \exp\bigg\{m\bigg[\mathcal{H}(\gamma) - \frac{\exp(-7s^2/2)}{2(2\pi)^{1/2}}\bigg]\bigg\}\,,$$

where $\mathcal{H}$ denotes the binary entropy function, and satisfies $\mathcal{H}(\gamma) \leqslant \gamma \log(e/\gamma)$. If we take $\gamma = \exp(-4s^2)$, then

$$\mathcal{H}(\gamma) - \frac{\exp(-7s^2/2)}{2(2\pi)^{1/2}} \leqslant \frac{1}{\exp(7s^2/2)}\left(\frac{1+4s^2}{\exp(s^2/2)} - \frac{1}{2(2\pi)^{1/2}}\right) \leqslant \frac{-1}{6\exp(7s^2/2)}\,,$$

where the last bound uses the assumption $s \geqslant 10$ from (211). It follows that

$$\mathbb{P}(\Omega_\gamma) \leqslant \mathbb{P}\bigg(|B| \leqslant \frac{m}{2}\bigg) + \exp\bigg\{-\frac{m}{6\exp(7s^2/2)}\bigg\}\,, \tag{213}$$

and it remains to bound the probability that $|B| \leqslant m/2$. To this end, note each $\zeta_i$ is a gaussian random variable with variance at most $(c')^2$, so

$$\mathbb{P}(|\zeta_i| \geqslant s) \leqslant \mathbb{P}(c'|Z| \geqslant s) \leqslant \frac{c'}{s}\exp\bigg\{-\frac{s^2}{2(c')^2}\bigg\}\,.$$

It follows by Markov's inequality and the preceding bound that

$$\begin{aligned}\mathbb{P}\bigg(|B| \leqslant \frac{m}{2}\bigg) &= \mathbb{P}\bigg(|B^c| \geqslant \frac{m}{2}\bigg) \leqslant 2\max\Big\{\mathbb{P}(|\zeta_i| \geqslant s) : i \leqslant m\Big\} \\ &\leqslant \frac{2c'}{s}\exp\bigg\{-\frac{s^2}{2(c')^2}\bigg\} \leqslant \frac{1}{2}\exp\bigg\{-\frac{s^2}{2(c')^2}\bigg\}\,,\end{aligned}$$

where the last bound follows trivially from the bounds $c' \leqslant 1$ and $s \geqslant 10$ (from (211)). If $m \geqslant 1/\gamma$, then

$$\frac{s^2}{2}\cdot 6\exp(7s^2/2) = \frac{3s^2}{\exp(s^2/2)}\cdot\frac{1}{\gamma} \leqslant \frac{1}{\gamma} \leqslant m\,,$$

so that (213) is dominated by the first term. It follows that

$$\mathbb{P}(\Omega_\gamma) \leqslant \exp\bigg\{-\frac{s^2}{2(c')^2}\bigg\} = \gamma^{1/(8(c')^2)}\,,$$

provided $\gamma = \exp(-4s^2)$ for $s$ satisfying (211), and $m \geqslant 1/\gamma$. This concludes the proof. ∎

**Proof** [Proof of Proposition F.1] As in Lemma F.4, let $\eta'(c) = 1/\log(4/c)$. Let

$$m = \bigg\lfloor \frac{1}{2}\eta'(c)\log n \bigg\rfloor\,, \qquad L = \bigg\lfloor \frac{n - n^{1/2}}{m} \bigg\rfloor\,.$$

By repeatedly applying Lemma F.4, we see that there exists a re-indexing of $\mathbf{v}^1, \ldots, \mathbf{v}^n$ such that

$$\max\bigg\{\Big\|P_{\ell m, i-1}\mathbf{v}_{\ell m+i}\Big\|^2 : 0 \leqslant \ell \leqslant L-1, 1 \leqslant i \leqslant m\bigg\} \leqslant (3c)^{1/2} \equiv c' \leqslant \frac{1}{2}\,,$$

where $P_{\ell m,i-1}$ denotes the orthogonal projection onto the span of $\{\mathbf{v}^{\ell m+1}, \ldots, \mathbf{v}^{\ell m+i-1}\}$. Let

$$N_\ell \equiv \bigg|\Big\{1 \leqslant i \leqslant m : (\mathbf{g}, \mathbf{v}^{\ell m+i}) \in E(U)\Big\}\bigg|\,.$$

Note that if $N_\ell \geqslant 2m\gamma$ for at least $n/(2m)$ indices $0 \leqslant \ell \leqslant L-1$, then we will have $(\mathbf{g}, \mathbf{v}^i) \in E(U)$ for at least $n\gamma$ indices $1 \leqslant i \leqslant n$. It follows by combining with Markov's inequality that

$$\mathbb{P}\bigg(\frac{1}{n}\Big|\Big\{i \leqslant n : (\mathbf{g}, \mathbf{v}^i) \in E(U)\Big\}\Big| \leqslant \gamma\bigg) \leqslant \mathbb{P}\bigg(\sum_{\ell \leqslant L} \mathbf{1}\{N_\ell \leqslant 2m\gamma\} \geqslant \frac{n}{3m}\bigg)$$
$$\leqslant \frac{3m}{n} \sum_{0 \leqslant \ell \leqslant L-1} \mathbb{P}(N_\ell \leqslant 2m\gamma)\,.$$

Applying Lemma F.5 gives, for $1/m \leqslant 2\gamma \leqslant \gamma_0 = \gamma_0(|E(U)|, E_{\max}(U))$,

$$\mathbb{P}\bigg(\frac{1}{n}\Big|\Big\{i \leqslant n : (\mathbf{g}, \mathbf{v}^i) \in E(U)\Big\}\Big| \leqslant \gamma\bigg) \leqslant 4(2\gamma)^{1/(24c)}\,.$$

The claim follows. ■

## F.2. Polynomial concentration of free energy

In this subsection we give the proof of Proposition 1.6. Towards this end, we first state and prove Lemma F.6 below. This is an adaptation of (Talagrand, 2011b, Propn. 8.2.6) (see also (Talagrand, 2011b, Lem. 9.2.2)), using Proposition F.1 in place of (Talagrand, 2011b, Cor. 8.2.5).

**Lemma F.6** *Let $\mu$ be any probability measure on $\{-1, +1\}^N$ with weights proportional to $w(J)$ such that $0 \leqslant w(J) \leqslant 1/2^N$ for all $J \in \{-1, +1\}^N$, and*

$$W = \sum_J w(J) \geqslant e^{-N\tau}$$

*for $\tau = \exp(-12)$. If $\mathbb{P}$ denotes the law of a standard gaussian vector $\mathbf{g}$ in $\mathbb{R}^N$, then*

$$\mathbb{P}\bigg(\mu\bigg(\bigg\{J \in \{-1, +1\}^N : \frac{(\mathbf{g}, J)}{N^{1/2}} \in E(U)\bigg\}\bigg) \leqslant \frac{\gamma}{4}\bigg) \overset{(217)}{\leqslant} \gamma^{11/2}\,,$$

*for $\exp(14)/N \leqslant \gamma \leqslant \gamma_0 = \gamma_0(|E(U)|, E_{\max}(U))$ and $N$ large enough.*

**Proof** First, it follows by a direct application of (Talagrand, 2011b, Lem. 9.2.1) that since $W \geqslant \exp(-N\tau)$, we have

$$\mu^{\otimes 2}\bigg(\bigg\{(J^1, J^2) \in \{-1, +1\}^{2N} : \frac{(J^1, J^2)}{N} \geqslant (8\tau)^{1/2}\bigg\}\bigg) \leqslant \frac{1}{\exp(2N\tau)}\,. \tag{214}$$

We then proceed to adapt the proof of (Talagrand, 2011b, Propn. 8.2.6). Let

$$Q_n \equiv \bigg\{J^{1:n} \equiv (J^1, \ldots, J^n) \in \{-1, +1\}^{nN} : \frac{(J^k, J^\ell)}{N} \leqslant (8\tau)^{1/2}\ \forall 1 \leqslant k < \ell \leqslant n\bigg\}\,.$$

It follows from (214) (and taking a union bound over all $1 \leqslant k < \ell \leqslant n$) that

$$\mu^{\otimes n}(Q_n) \overset{(214)}{\geqslant} 1 - \frac{n^2}{2\exp(2N\tau)} \geqslant \frac{1}{2}\,, \tag{215}$$

where the last inequality holds provided $n \leqslant \exp(N\tau)$. Next define

$$\Omega_\gamma(J^{1:n}) \equiv \left\{ \mathbf{g} : \frac{1}{n} \left| \left\{ \ell \leqslant n : \frac{(\mathbf{g}, J^\ell)}{N^{1/2}} \in E(U) \right\} \right| \leqslant \gamma \right\}.$$

If we take $c = (8\tau)^{1/2}$, then $c \leqslant 1/12$ by the assumption $\tau = \exp(-12)$, and so Proposition F.1 implies that for every $J^{1:n} \in Q_n$ we have the bound

$$\mathbb{P}\Big(\Omega_\gamma(J^{1:n})\Big) \leqslant \gamma^{1/(25c)}, \tag{216}$$

for $\log(5/c)/(\log n) \leqslant \gamma \leqslant \gamma_0$ and $n$ large enough. Define the random variable

$$\Upsilon_\gamma \equiv \sum_{J^{1:n} \in Q_n} \mu^{\otimes n}(J^{1:n}) \mathbf{1}\Big\{ \mathbf{g} \in \Omega_\gamma(J^{1:n}) \Big\},$$

and note that Markov's inequality combined with (216) gives

$$\mathbb{P}\left(\Upsilon_\gamma \geqslant \frac{1}{4}\right) \leqslant \frac{\mathbb{E}\Upsilon_\gamma}{1/4} = 4 \sum_{J^{1:n} \in Q_n} \mu^{\otimes n}(J^{1:n}) \mathbb{P}\Big(\Omega_\gamma(J^{1:n})\Big) \overset{(216)}{\leqslant} 4\gamma^{1/(25c)}. \tag{217}$$

On the other hand, we can lower bound

$$\begin{aligned} \Gamma \equiv \mu\left( \left\{ J \in \{-1,+1\}^N : \frac{(\mathbf{g}, J)}{N^{1/2}} \in E(U) \right\} \right) &= \sum_{J^{1:n}} \mu^{\otimes n}(J^{1:n}) \frac{1}{n} \left| \left\{ \ell \leqslant n : \frac{(\mathbf{g}, J^\ell)}{N^{1/2}} \in E(U) \right\} \right| \\ \geqslant \gamma \sum_{J^{1:n} \in Q_n} \mu^{\otimes n}(J^{1:n}) \mathbf{1}\Big\{ \mathbf{g} \notin \Omega_\gamma(J^{1:n}) \Big\} &= \gamma\Big( \mu^{\otimes n}(Q_n) - \Upsilon_\gamma \Big) \overset{(215)}{\geqslant} \gamma\left( \frac{1}{2} - \Upsilon_\gamma \right). \end{aligned}$$

As a consequence, if $\Gamma \leqslant \gamma/4$, we must have $\Upsilon_\gamma \geqslant 1/4$. It follows that

$$\mathbb{P}\left( \Gamma \leqslant \frac{\gamma}{4} \right) \leqslant \mathbb{P}\left( \Upsilon_\gamma \geqslant \frac{1}{4} \right) \overset{(217)}{\leqslant} 4\gamma^{1/(25c)},$$

again for $\log(5/c)/(\log n) \leqslant \gamma \leqslant \gamma_0$ and $n$ large enough. Recall moreover that for (215) to hold we must have $n \leqslant \exp(N\tau)$, so we must ultimately require

$$\gamma_0 \geqslant \gamma \geqslant \frac{\log(5/c)}{N\tau} = \frac{\log(5/(8\tau)^{1/2})}{N\tau}.$$

The claim follows by recalling $\tau = \exp(-12)$ and $c = (8\tau)^{1/2}$. ■

We now proceed to prove Proposition 1.6. This is an adaptation of the proof of (Talagrand, 2011b, Propn. 9.2.6), using the above result Lemma F.6 in place of (Talagrand, 2011b, Propn. 8.2.6).
**Proof** [Proof of Proposition 1.6] As in the proof of Theorem 1.1 in the bounded case, let $\mathbb{P}^j$ denote probability conditional on the first $j$ rows of $\boldsymbol{G}$, and let $\mathbb{E}^j$ denote expectation with respect to $\mathbb{P}^j$. Then, as in the proof of (Talagrand, 2011b, Propn. 9.2.6), we let $\boldsymbol{W} \equiv \boldsymbol{Z}/2^N$ and decompose

$$\frac{1}{N}\Big\{ \log_{N\tau} \boldsymbol{W} - \mathbb{E} \log_{N\tau} \boldsymbol{W} \Big\} = \sum_{j \leqslant M} \frac{1}{N} \Big\{ \mathbb{E}^j \log_{N\tau} \boldsymbol{W} - \mathbb{E}^{j-1} \log_{N\tau} \boldsymbol{W} \Big\} \equiv \sum_{j \leqslant M} X_j.$$

To bound $X_j$, recall (177) and denote

$$\boldsymbol{W}_j \equiv \frac{\boldsymbol{Z}_j}{2^N} \equiv \sum_J w_j(J) \equiv \sum_J \frac{1}{2^N} \prod_{\substack{a \leqslant M, \\ a \neq j}} U\bigg(\frac{(\mathbf{g}^a, J)}{N^{1/2}}\bigg).$$

Note that $0 \leqslant \boldsymbol{W} \leqslant \boldsymbol{W}_j \leqslant 1$. Since $\boldsymbol{W}_j$ does not depend on the $j$-th row of $\boldsymbol{G}$, we can rewrite

$$NX_j = \mathbb{E}^j\Big(\log_{N\tau} \boldsymbol{W} - \log_{N\tau} \boldsymbol{W}_j\Big) - \mathbb{E}^{j-1}\Big(\log_{N\tau} \boldsymbol{W} - \log_{N\tau} \boldsymbol{W}_j\Big).$$

Recall that $0 \leqslant \boldsymbol{W} \leqslant \boldsymbol{W}_j$, so if $\boldsymbol{W}_j \leqslant e^{-N\tau}$ then $\log_{N\tau} \boldsymbol{W}_j = -N\tau = \log_{N\tau} \boldsymbol{W}$. It follows that

$$L_j \equiv \log_{N\tau} \boldsymbol{W}_j - \log_{N\tau} \boldsymbol{W} = \mathbf{1}\Big\{\boldsymbol{W}_j \geqslant e^{-N\tau}\Big\}\Big(\log_{N\tau} \boldsymbol{W}_j - \log_{N\tau} \boldsymbol{W}\Big) \in [0, N\tau].$$

Recall that $\mathbb{P}_j$ denotes probability conditional on all rows of $\boldsymbol{G}$ except the $j$-th one, and note $\mathbb{E}^{j-1} = \mathbb{E}_j\mathbb{E}^j$ where $\mathbb{E}_j$ is expectation with respect to $\mathbb{P}_j$. We can rewrite $X_j = -\dot{x}_j + \ddot{x}_j$ where

$$\begin{aligned} N\dot{x}_j &\equiv \mathbb{E}^j\bigg[\Big(\log_{N\tau} \boldsymbol{W}_j - \log_{N\tau} \boldsymbol{W}\Big); \boldsymbol{W}_j \geqslant e^{-N\tau}\bigg] = \mathbb{E}^j L_j \in [0, N\tau], \\ N\ddot{x}_j &\equiv \mathbb{E}^{j-1}\bigg[\Big(\log_{N\tau} \boldsymbol{W}_j - \log_{N\tau} \boldsymbol{W}\Big); \boldsymbol{W}_j \geqslant e^{-N\tau}\bigg] = \mathbb{E}^{j-1} L_j = \mathbb{E}_j(N\dot{x}_j). \end{aligned} \tag{218}$$

For comparison let $\bar{X}_j = -\dot{z}_j + \ddot{z}_j$ where $\dot{z}_j \equiv \dot{x}_j - \dot{e}_j$ and $\ddot{z}_j \equiv \ddot{x}_j - \ddot{e}_j$, for

$$\begin{aligned} N\dot{e}_j &\equiv \mathbb{E}^j\bigg[L_j; \frac{\boldsymbol{W}}{\boldsymbol{W}_j} < \frac{\delta' e^{14}}{4N}\bigg] = \mathbb{E}^j\bigg[L_j; \frac{\boldsymbol{W}}{\boldsymbol{W}_j} < \frac{\delta' e^{14}}{4N}\bigg] \in [0, N\tau], \\ N\ddot{e}_j &\equiv \mathbb{E}^{j-1}\bigg[L_j; \frac{\boldsymbol{W}}{\boldsymbol{W}_j} < \frac{\delta' e^{14}}{4N}\bigg] = \mathbb{E}^{j-1}\bigg[L_j; \frac{\boldsymbol{W}}{\boldsymbol{W}_j} < \frac{\delta' e^{14}}{4N}\bigg] = \mathbb{E}_j(N\dot{e}_j). \end{aligned}$$

Similarly to Lemma F.6, let $\mu_j$ be the probability measure on $\{-1, +1\}^N$ with weights proportional to $w_j(J)$. Then note the assumption $U(x) \geqslant \delta' \mathbf{1}\{x \in E(U)\}$ implies

$$\frac{\boldsymbol{W}}{\boldsymbol{W}_j} \geqslant \delta' \mu_j\bigg(\bigg\{J \in \{-1, +1\}^N : \frac{(\mathbf{g}^j, J)}{N^{1/2}} \in E(U)\bigg\}\bigg) \equiv \delta' \Gamma_j.$$

Since $0 \leqslant L_j \leqslant N\tau$, we can use Markov's inequality to bound

$$0 \leqslant \mathbb{E}_j(N\dot{e}_j) = N\ddot{e}_j \leqslant N\tau\, \mathbb{E}^{j-1}\bigg[\mathbf{1}\Big\{\boldsymbol{W}_j \geqslant e^{-N\tau}\Big\}\mathbb{P}_j\bigg(\frac{\boldsymbol{W}}{\boldsymbol{W}_j} < \frac{\delta' e^{14}}{4N}\bigg)\bigg] \leqslant N\tau\bigg(\frac{\delta' e^{14}}{N}\bigg)^{11/2} \tag{219}$$

where the last inequality is by Lemma F.6. It follows using Markov's inequality again that

$$\mathbb{P}\bigg(\sum_{j \leqslant M} \Big|X_j - \bar{X}_j\Big| \geqslant \frac{1}{2N^2}\bigg) \leqslant 2N^2 \sum_{j \leqslant M} \mathbb{E}\Big(\dot{e}_j + \ddot{e}_j\Big) \overset{(219)}{\leqslant} N^3\bigg(\frac{\delta' e^{14}}{N}\bigg)^{11/2}. \tag{220}$$

It remains to bound the random variables $\bar{X}_j = -\dot{z}_j + \ddot{z}_j$. Using Jensen's inequality,

$$\exp(N\ddot{z}_j) \leqslant \mathbb{E}^{j-1}\exp(N\dot{z}_j) \leqslant 1 + \mathbb{E}^{j-1}\bigg[\frac{\boldsymbol{W}_j}{\boldsymbol{W}}; \boldsymbol{W}_j \geqslant e^{-N\tau}, \frac{\boldsymbol{W}_j}{\boldsymbol{W}} \leqslant \frac{4N}{\delta' e^{14}}\bigg].$$

It then follows by using Lemma F.6 again that the above can be bounded by

$$1 + \mathbb{E}^{j-1}\bigg[\frac{\boldsymbol{W}_j}{\boldsymbol{W}}; \boldsymbol{W}_j \geqslant e^{-N\tau}, \frac{\boldsymbol{W}_j}{\boldsymbol{W}} \leqslant \frac{4N}{\delta' e^{14}}\bigg] \leqslant 1 + \int_0^{4N/(\delta' e^{14})} \mathbb{P}^{j-1}\bigg(\boldsymbol{W}_j \geqslant e^{-N\tau}; \frac{\boldsymbol{W}_j}{\boldsymbol{W}} \geqslant u\bigg)\, du$$

$$\leqslant 1 + \frac{4}{\delta'\gamma_0} + \int_{4/(\delta'\gamma_0)}^{\infty} \bigg(\frac{4}{\delta' u}\bigg)^{11/2} du \leqslant C_0 \equiv C_0(|E(U)|, E_{\max}(U), \delta')\,. \tag{221}$$

It follows that we can choose $\lambda_0$ small enough (depending on $C_0$) such that for all $0 \leqslant \lambda \leqslant \lambda_0$,

$$\mathbb{E}^{j-1}\Big[\exp(N\lambda|\bar{X}_j|)\Big] \leqslant \exp(N\lambda\ddot{z}_j)\cdot\mathbb{E}^{j-1}\Big[\exp(N\lambda\dot{z}_j)\Big]$$
$$\leqslant \exp(N\lambda\ddot{z}_j)\cdot\Big(\mathbb{E}^{j-1}\exp(N\dot{z}_j)\Big)^{\lambda} \leqslant (C_0)^{2\lambda} \leqslant 2\,.$$

It follows by the martingale Bernstein's inequality (see e.g. (Talagrand, 2011b, eq. (A.41))) that

$$\mathbb{P}\bigg(\Big|\sum_{j\leqslant M}\bar{X}_j\Big| \geqslant t\bigg) \leqslant 2\exp\bigg(-\frac{Nt\lambda}{2}\min\Big\{1, \frac{t\lambda}{2}\Big\}\bigg)$$

for all $t \geqslant 0$. In particular, taking $t = (\log N)/N^{1/2}$ gives

$$\mathbb{P}\bigg(\Big|\sum_{j\leqslant M}\bar{X}_j\Big| \geqslant \frac{\log N}{N^{1/2}}\bigg) \leqslant \exp\bigg(-\frac{\lambda^2(\log N)^2}{2}\bigg)\,. \tag{222}$$

The claimed bound follows by combining (220) with (222). ■

### F.3. Exponential concentration for smoothed model

In this subsection we give the proof of Proposition 1.9, showing concentration for the log-partition function of the smoothed model (22).

**Theorem F.7 ((Pisier, 1986))** *If $f : \mathbb{R}^n \to \mathbb{R}$ is $C^1$, and $X$ and $Y$ are independent standard gaussian random variables in $\mathbb{R}^n$, then for any convex function $g : \mathbb{R} \to \mathbb{R}$ it holds that*

$$\mathbb{E}g\Big(f(X) - f(Y)\Big) \leqslant \mathbb{E}g\bigg(\frac{\pi}{2}(\nabla f(X), Y)\bigg)\,.$$

*In particular, taking $g(x) = \exp(sx)$ for any real number $s$ gives*

$$\mathbb{E}\exp\Big\{s\Big(f(X) - f(Y)\Big)\Big\} \leqslant \mathbb{E}\exp\Big\{\frac{s^2\pi^2}{8}\|\nabla f(X)\|^2\Big\}\,.$$

*In the case that $\nabla f$ is bounded, this recovers the standard theorem of Tsirelson et al. (1976) (see also Borell, 1975) on concentration of Lipschitz functionals of gaussian random variables.*

We also recall that if $\boldsymbol{G}$ is an $M \times N$ matrix with i.i.d. standard gaussian entries and $M \leqslant N$, then the maximum singular value $s_{\max}(\boldsymbol{G})$ satisfies the tail bound

$$\mathbb{P}\bigg(s_{\max}(\boldsymbol{G}) \geqslant (C_2 N)^{1/2} + t\bigg) \leqslant \frac{2}{\exp(c_2 t^2)} \tag{223}$$

for all $t \geqslant 0$, where $c_2$ and $C_2$ are absolute constants. See for instance (Rudelson and Vershynin, 2010, Propn. 2.4) where the result is in fact stated more generally for matrices with independent subgaussian entries (with mean zero and unit variance). From this bound it is straightforward to deduce the following:

**Lemma F.8** *If $\boldsymbol{G}$ is an $M \times N$ matrix with i.i.d. standard gaussian entries and $M \leqslant N$, then we can take $c_2 = 1/C_2 \leqslant 1$ in the bound (223). With this choice of constants, we have*

$$\mathbb{E} \exp\Big(\vartheta s_{\max}(\boldsymbol{G})^2\Big) \leqslant 16N \exp(2\vartheta C_2 N)$$

*for all $0 \leqslant \vartheta \leqslant c_2/2 = 1/(2C_2)$.*

**Proof** It follows by a change of variables that

$$\begin{aligned} E(\vartheta) \equiv \mathbb{E} \exp\Big(\vartheta s_{\max}(\boldsymbol{G})^2\Big) &= \int_0^\infty \mathbb{P}\bigg(\exp(\vartheta s_{\max}(\boldsymbol{G})^2) \geqslant x\bigg)\, dx \\ &= 2\vartheta \int_0^\infty u \exp(\vartheta u^2) \cdot \mathbb{P}\bigg(s_{\max}(\boldsymbol{G}) \geqslant u\bigg)\, du \leqslant \text{(I)} + \text{(II)}\,, \end{aligned}$$

where (I) is the contribution to the integral from $u \leqslant (C_2 N)^{1/2}$, while (II) is the contribution from $u \geqslant (C_2 N)^{1/2}$. We then have the trivial bound

$$\begin{aligned} \text{(I)} &\leqslant 2\vartheta \int_0^{(C_2N)^{1/2}} u \exp(\vartheta u^2)\, du \leqslant 2\vartheta \exp(\vartheta C_2 N) \int_0^{(C_2N)^{1/2}} u\, du \\ &= \vartheta C_2 N \exp(\vartheta C_2 N) \leqslant \frac{N}{2} \exp(\vartheta C_2 N)\,, \end{aligned}$$

where the last inequality uses the assumption $\vartheta \leqslant c_2/2 = 1/(2C_2)$. For the other term, it follows from the singular value tail bound (223) (and again using $\vartheta \leqslant c_2/2 = 1/(2C_2)$) that

$$\begin{aligned} \text{(II)} &\leqslant 4\vartheta \int_0^\infty \Big((C_2N)^{1/2} + u\Big) \exp\bigg\{\vartheta\Big((C_2N)^{1/2} + u\Big)^2 - c_2 u^2\bigg\}\, du \\ &\leqslant 4\vartheta \exp(\vartheta C_2 N) \int_0^\infty \Big((C_2N)^{1/2} + u\Big) \exp\bigg\{2\vartheta (C_2N)^{1/2} u - \frac{c_2 u^2}{2}\bigg\}\, du\,. \end{aligned}$$

Completing the square and making another change of variables gives

$$\begin{aligned} \text{(II)} &\leqslant 4\vartheta \exp\bigg\{\Big(1 + \frac{2\vartheta}{c_2}\Big)\vartheta C_2 N\bigg\} \int_{-\infty}^\infty \bigg| u + \Big(1 + \frac{2\vartheta}{c_2}\Big)(C_2N)^{1/2}\bigg| \exp\bigg\{-\frac{c_2 u^2}{2}\bigg\}\, du \\ &\leqslant \frac{4\vartheta}{(c_2)^{1/2}} \exp(2\vartheta C_2 N) \int_{-\infty}^\infty \bigg|\frac{u}{(c_2)^{1/2}} + 2(C_2N)^{1/2}\bigg| \exp\bigg\{-\frac{u^2}{2}\bigg\}\, du \\ &\leqslant \exp(2\vartheta C_2 N) \frac{4\vartheta (2\pi)^{1/2}}{c_2} \Big(1 + 2N^{1/2}\Big) \leqslant 6(2\pi)^{1/2} \cdot N \exp(2\vartheta C_2 N)\,. \end{aligned}$$

Combining the bounds for (I) and (II) gives the claimed bound. ■

**Lemma F.9** *Suppose $U$ satisfies Assumption 1, and let $\boldsymbol{Z}(\eta)$ be as defined by (22). If $f = \log \boldsymbol{Z}(\eta)$ viewed as a function of the gaussian disorder $\boldsymbol{G}$, then there exists a finite constant $C_1(U;\eta)$ such that*

$$\mathbb{E}\exp\left(s^2\|\nabla f(\boldsymbol{G})\|^2\right) \leqslant 16N \cdot \exp\left\{N \cdot 6C_2C_1(U;\eta)^2s^2\right\}$$

*for all $|s| \leqslant (c_2)^{1/2}/(2C_1(U;\eta))$, where $C_2$ and $c_2$ are the constants from Lemma F.8.*

**Proof** Recall that $U_\eta \equiv U * \varphi_\eta$, and denote $u_\eta \equiv \log U_\eta$. Denote the probability meausure

$$\mu_\eta(J) \equiv \frac{w_\eta(J)}{\boldsymbol{Z}(\eta)} = \frac{1}{\boldsymbol{Z}(\eta)}\prod_{a\leqslant M} U_\eta\left(\frac{(\mathbf{g}^a, J)}{N^{1/2}}\right) = \frac{1}{\boldsymbol{Z}(\eta)}\prod_{a\leqslant M} U_\eta(\Delta_a)\,,$$

where we abbreviate $\Delta_a = (\mathbf{g}^a, J)/N^{1/2}$. Then

$$\left|\frac{df}{dg_{a,i}}\right| = \left|\sum_J \mu_\eta(J)(u_\eta)'(\Delta_a)\frac{J_i}{N^{1/2}}\right| \leqslant \frac{1}{N^{1/2}}\sum_J w(J)|(u_\eta)'(\Delta_a)|\,.$$

Note that if $(u_\eta)'$ were uniformly bounded, then $f$ would be $A$-Lipschitz with $A = \|(u_\eta)'\|_\infty/N^{1/2}$, and the desired exponential concentration for $\log \boldsymbol{Z}(\eta)$ would follow from standard concentration theorems for Lipschitz functionals of gaussians. Since $(u_\eta)'$ may be unbounded, we cannot conclude that $f$ is Lipschitz. However, we note that

$$(u_\eta)'(x) = \frac{\mathbb{E}_\xi[\xi U(x+\eta\xi)]}{\eta\mathbb{E}_\xi U(x+\eta\xi)} \leqslant C_1(U;\eta)\Big(1+|x|\Big)\,,$$

where the last bound holds by an obvious extension of Lemma B.3 (using Assumption 1). Therefore

$$\left|\frac{df}{dg_{a,i}}\right| \leqslant \frac{C_1(U;\eta)}{N^{1/2}}\left(1+\sum_J \mu_\eta(J)|\Delta_a|\right) = \frac{C_1(U;\eta)}{N^{1/2}}\Big(1+\langle|\Delta_a|\rangle_\eta\Big)\,,$$

where $\langle\cdot\rangle_\eta$ denotes expectation over $\mu_\eta$. It follows that

$$\begin{aligned}\|\nabla f\|^2 &\leqslant C_1(U;\eta)^2\sum_{a\leqslant M}\Big(1+\langle|\Delta_a|\rangle_\eta\Big)^2 \leqslant 2C_1(U;\eta)^2\sum_{a\leqslant M}\Big(1+(\langle|\Delta_a|\rangle_\eta)^2\Big)\\ &\leqslant 2C_1(U;\eta)^2\sum_{a\leqslant M}\Big(1+\langle(\Delta_a)^2\rangle_\eta\Big) = 2C_1(U;\eta)^2\left\{M+\frac{\|\boldsymbol{G}J\|^2}{N}\right\}\\ &\leqslant 2C_1(U;\eta)^2\Big\{M+s_{\max}(\boldsymbol{G})^2\Big\}\,,\end{aligned}$$

where $s_{\max}(\boldsymbol{G})$ denotes the maximum singular value of $\boldsymbol{G}$, as above. Taking the expectation over $\boldsymbol{G}$ and applying Lemma F.8 gives

$$\mathbb{E}\exp\left(s^2\|\nabla f(\boldsymbol{G})\|^2\right) \leqslant 16N\cdot\exp\left\{2\Big(M+2C_2N\Big)C_1(U;\eta)^2s^2\right\}\,,$$

where the bound holds provided $|s| \leqslant (c_2)^{1/2}/(2C_1(U;\eta))$. The result follows by recalling that we assumed $M \leqslant N$ and $C_2 \geqslant 1$. ■

**Proof** [Proof of Proposition 1.9] Let $\boldsymbol{G}'$ be an independent copy of $\boldsymbol{G}$. It follows by Theorem F.7 and Lemma F.9 that

$$\begin{aligned}\mathbb{E}\exp\left\{s\Big(f(\boldsymbol{G})-\mathbb{E}f(\boldsymbol{G})\Big)\right\} &\leqslant \mathbb{E}\exp\left\{s\Big(f(\boldsymbol{G})-f(\boldsymbol{G}')\Big)\right\} \\ &\leqslant \mathbb{E}\exp\left\{\frac{s^2\pi^2}{8}\|\nabla f(\boldsymbol{G})\|^2\right\} \leqslant 16N\cdot\exp\left\{N\cdot 8C_2C_1(U;\eta)^2s^2\right\},\end{aligned}$$

for all $|s|\leqslant (c_2)^{1/2}/(3C_1(U;\eta))$. Thus, for $x\geqslant 0$, it holds for $0\leqslant s\leqslant (c_2)^{1/2}/(3C_1(U;\eta))$ that

$$\begin{aligned}\mathbb{P}\Big(f(\boldsymbol{G})-\mathbb{E}f(\boldsymbol{G})\geqslant Nx\Big) &\leqslant \mathbb{E}\exp\left\{s\Big(f(\boldsymbol{G})-\mathbb{E}f(\boldsymbol{G})\Big)-Nsx\right\} \\ &\leqslant 16N\cdot\exp\left\{N\Big(8C_2C_1(U;\eta)^2s^2-sx\Big)\right\}.\end{aligned}$$

A similar bound holds for $x\leqslant 0$. In any case it is clear that we can take $s$ small enough to obtain exponential decay. In particular, for $x\geqslant 0$ small enough we can let

$$s=\frac{x}{16C_2\cdot C_1(U;\eta)^2}\leqslant\frac{(c_2)^{1/2}}{3C_1(U;\eta)},$$

where the last bound holds for $x\leqslant 5(C_2)^{1/2}C_1(U;\eta)$. This results in the bound

$$\mathbb{P}\left(\Big|f(\boldsymbol{G})-\mathbb{E}f(\boldsymbol{G})\Big|\geqslant Nx\right)\leqslant 32N\cdot\exp\left\{-\frac{Nx^2}{32C_2C_1(U;\eta)^2}\right\},$$

which concludes the proof. ■

**Corollary F.10** *Suppose $U$ satisfies Assumptions 1 and 2, and let $\boldsymbol{Z}(\eta)$ be as in (22). Then*

$$\lim_{N\to\infty}\frac{1}{N}\log\boldsymbol{Z}(\eta)=\mathrm{RS}(\alpha;U_\eta)$$

*for all $0<\alpha\leqslant\alpha_\wr(U)$.*

**Proof** Recall from (102) that if $0<\alpha\leqslant\alpha_\wr(U)$, then we will also have $\alpha\leqslant\alpha(U_\eta)$ for $\eta$ small enough. The upper bound on $\boldsymbol{Z}(\eta)$ follows from the upper bound in Theorem 1.1, which was already proved at the end of Section C. For the lower bound on $\boldsymbol{Z}(\eta)$, we argue similarly as in the proof of the Theorem 1.1 lower bound for the case $\|u\|_\infty<\infty$, but using the concentration result from Proposition 1.9 in place of the Azuma–Hoeffding bound. To this end, let $\bar{\boldsymbol{Z}}(\eta)$ be defined as $\bar{\boldsymbol{Z}}$ from (144), but with $U_\eta$ in place of $U$. It follows from Theorem 1.5 (by the same calculation leading to (176)) that, with high probability,

$$\mathbb{P}\left(\frac{1}{N}\log\bar{\boldsymbol{Z}}(\eta)\geqslant\mathrm{RS}(\alpha;U_\eta)-o_t(1)\,\middle|\,\mathscr{F}(t)\right)\geqslant\frac{1}{\exp(No_t(1))}.$$

On the other hand, it follows from Proposition 1.9 that, again with high probability,

$$\mathbb{P}\left(\frac{1}{N}\log\boldsymbol{Z}\geqslant\frac{1}{N}\mathbb{E}\log\boldsymbol{Z}(\eta)+x\,\middle|\,\mathscr{F}(t)\right)\leqslant 35N\cdot\exp\left\{-\frac{Nx^2}{35C_2C_1(U;\eta)^2}\right\}$$

for sufficiently small $x > 0$. The above two bounds are in contradiction with one another unless

$$\frac{1}{N}\mathbb{E}\log \boldsymbol{Z}(\eta) \geqslant \mathrm{RS}(\alpha; U_\eta) - o_N(1)\,.$$

It then follows by another application of Proposition 1.9 that

$$\begin{aligned}\mathbb{P}\bigg(\frac{1}{N}\log \boldsymbol{Z}(\eta) \leqslant \mathrm{RS}(\alpha; U_\eta) - o_N(1) - x\bigg) &\leqslant \mathbb{P}\bigg(\frac{1}{N}\log \boldsymbol{Z}(\eta) \leqslant \frac{1}{N}\mathbb{E}\log \boldsymbol{Z}(\eta) - x\bigg)\\ &\leqslant 35N\cdot\exp\bigg\{-\frac{Nx^2}{35C_2C_1(U;\eta)^2}\bigg\}\end{aligned}$$

for sufficiently small $x > 0$. This yields the lower bound for $\boldsymbol{Z}(\eta)$ and concludes the proof. ■

### F.4. Comparison with smoothed model and conclusion

In this subsection we prove Proposition 1.7 which gives the comparison between the quantities $\boldsymbol{Z}$ and $\boldsymbol{Z}(\eta)$ from (1) and (22). We then conclude the proof of the main theorem.

**Proof** [Proof of Proposition 1.7] Some of the steps below are similar to the steps in the proof of Proposition 1.6. Let

$$\boldsymbol{V}_k \equiv \frac{1}{2^N}\sum_J\bigg\{\prod_{a\leqslant k} U_\eta\bigg(\frac{(\mathbf{g}^a, J)}{N^{1/2}}\bigg)\bigg\}\bigg\{\prod_{k<a\leqslant M} U\bigg(\frac{(\mathbf{g}^a, J)}{N^{1/2}}\bigg)\bigg\}\,.$$

Recall $\boldsymbol{W} \equiv \boldsymbol{Z}/2^N$, and write $\tilde{\boldsymbol{W}} \equiv \boldsymbol{Z}(\eta)/2^N$. Note $\boldsymbol{V}_0 = \boldsymbol{W}$, and $\boldsymbol{V}_M = \tilde{\boldsymbol{W}}$. Let us also define

$$\boldsymbol{V}_{k,\circ} \equiv \frac{1}{2^N}\sum_J\bigg\{\prod_{a<k} U_\eta\bigg(\frac{(\mathbf{g}^a, J)}{N^{1/2}}\bigg)\bigg\}\bigg\{\prod_{k<a\leqslant M} U\bigg(\frac{(\mathbf{g}^a, J)}{N^{1/2}}\bigg)\bigg\} \equiv \sum_J w_{k,\circ}(J)\,. \tag{224}$$

Note that $\boldsymbol{V}_{k,\circ} \geqslant \max\{\boldsymbol{V}_{k-1}, \boldsymbol{V}_k\}$. We can then decompose

$$\frac{1}{N}\mathbb{E}\Big(\log_{N\tau}\tilde{\boldsymbol{W}} - \log_{N\tau}\boldsymbol{W}\Big) = \frac{1}{N}\sum_{k\leqslant M}\mathbb{E}\Big(\log_{N\tau}\boldsymbol{V}_k - \log_{N\tau}\boldsymbol{V}_{k-1}\Big) = \sum_{k\leqslant M} y_k$$

(compare with (218)). Let $G_{k,\circ}$ be the probability measure on $\{-1,+1\}^N$ with weights proportional to $w_{k,\circ}(J)$ as defined by (224). Write $\langle\cdot\rangle_{k,\circ}$ for expectation with respect to $G_{k,\circ}$. Abbreviate

$$U_k \equiv U\bigg(\frac{(\mathbf{g}^k, J)}{N^{1/2}}\bigg)\,,\quad \tilde{U}_k \equiv U_\eta\bigg(\frac{(\mathbf{g}^k, J)}{N^{1/2}}\bigg)\,.$$

Recalling that $U(x) > \delta'\mathbf{1}\{x \in E(U)\}$ (from (20)), we have

$$\frac{\boldsymbol{V}_k}{\boldsymbol{V}_{k,\circ}} = \langle U_k\rangle_{k,\circ} \geqslant \delta' G_{k,\circ}\bigg(\bigg\{J\in\{-1,+1\}^N : \frac{(\mathbf{g}^k, J)}{N^{1/2}} \in E(U)\bigg\}\bigg) \equiv \delta'\Gamma_{k,\circ}\,.$$

For $\eta$ small enough we will also have $U_\eta(x) > \delta'\mathbf{1}\{x \in E(U)\}$, so we can also bound

$$\frac{\boldsymbol{V}_{k-1}}{\boldsymbol{V}_{k,\circ}} = \langle \tilde{U}_k\rangle_{k,\circ} \geqslant \delta' G_{k,\circ}\bigg(\bigg\{J\in\{-1,+1\}^N : \frac{(\mathbf{g}^k, J)}{N^{1/2}} \in E(U)\bigg\}\bigg) = \delta'\Gamma_{k,\circ}\,.$$

We also have from (Talagrand, 2011b, Lem. 8.3.10) that if $x, y, z \leqslant 1$, then

$$\Big|\log_A(xz) - \log_A(yz)\Big| \leqslant \Big|\log_A x - \log_A y\Big| \cdot \mathbf{1}\Big\{z \geqslant e^{-A}\Big\}.$$

Combining the above bounds gives

$$\begin{aligned} |Ny_k| &\leqslant \mathbb{E}\Big|\log_{N\tau}\Big(\boldsymbol{V}_{k,\circ}\langle U_k\rangle_{k,\circ}\Big) - \log_{N\tau}\Big(\boldsymbol{V}_{k,\circ}\langle \tilde{U}_k\rangle_{k,\circ}\Big)\Big| \\ &\leqslant \mathbb{E}\bigg[\Big|\log_{N\tau}\langle U_k\rangle_{k,\circ} - \log_{N\tau}\langle \tilde{U}_k\rangle_{k,\circ}\Big|; \boldsymbol{V}_{k,\circ} \geqslant e^{-N\tau}\bigg] \leqslant \text{(I)} + \text{(II)}\,, \end{aligned}$$

for (I) and (II) defined by

$$\begin{aligned} \text{(I)} &\equiv N\tau\mathbb{P}\bigg(\boldsymbol{V}_{k,\circ} \geqslant e^{-N\tau}, \delta'\Gamma_{k,\circ} < \frac{e^{14}}{4N}\bigg)\,, \\ \text{(II)} &\equiv \mathbb{E}\bigg[\log\bigg\{1 + \bigg|\frac{\langle \tilde{U}_k\rangle_{k,\circ} - \langle U_k\rangle_{k,\circ}}{\delta'\Gamma_{k,\circ}}\bigg|\bigg\}; \boldsymbol{V}_{k,\circ} \geqslant e^{-N\tau}, \Gamma_{k,\circ} \geqslant \frac{e^{14}}{4N}\bigg]\,. \end{aligned}$$

Combining with Lemma F.6 gives (similarly to (219))

$$\text{(I)} \leqslant N\tau\bigg(\frac{e^{14}}{N}\bigg)^{11/2}\,.$$

Meanwhile, using the bound $\log(1+x) \leqslant x$ together with the Cauchy–Schwarz inequality gives

$$\begin{aligned} \text{(II)} &\leqslant \mathbb{E}\bigg[\bigg|\frac{\langle \tilde{U}_k\rangle_{k,\circ} - \langle U_k\rangle_{k,\circ}}{\delta'\Gamma_{k,\circ}}\bigg|; \boldsymbol{V}_{k,\circ} \geqslant e^{-N\tau}, \Gamma_{k,\circ} \geqslant \frac{e^{14}}{4N}\bigg] \\ &\leqslant \frac{1}{\delta'}\bigg\{\mathbb{E}\bigg[\Big(\langle \tilde{U}_k - U_k\rangle_{k,\circ}\Big)^2\bigg] \cdot \mathbb{E}\bigg[\frac{1}{(\Gamma_{k,\circ})^2}; \boldsymbol{V}_{k,\circ} \geqslant e^{-N\tau}, \Gamma_{k,\circ} \geqslant \frac{e^{14}}{4N}\bigg]\bigg\}^{1/2}\,. \end{aligned}$$

For the first factor we note that

$$\mathbb{E}\bigg[\Big(\langle \tilde{U}_k - U_k\rangle_{k,\circ}\Big)^2\bigg] \leqslant \bigg\langle \mathbb{E}\Big[(\tilde{U}_k - U_k)^2\Big]\bigg\rangle_{k,\circ} = \mathbb{E}\bigg[\Big(U_\eta(\xi) - U(\xi)\Big)^2\bigg] \leqslant o_\eta(1)\,.$$

For the second factor, applying Lemma F.6 again gives (similarly to (221))

$$\begin{aligned} \mathbb{E}\bigg[\frac{1}{(\Gamma_{k,\circ})^2}; \boldsymbol{V}_{k,\circ} \geqslant e^{-N\tau}, \Gamma_{k,\circ} \geqslant \frac{e^{14}}{4N}\bigg] &\leqslant \int_0^{(4N/e^{14})^2} \mathbb{P}\bigg(\frac{e^{14}}{4N} \leqslant \Gamma_{k,\circ} \leqslant \frac{1}{y^{1/2}}\bigg)\,dy \\ &\leqslant \bigg(\frac{\gamma_0}{4}\bigg)^2 + \int_{(\gamma_0/4)^2}^{(4N/e^{14})^2} \bigg(\frac{4}{y^{1/2}}\bigg)^{11/2} dy \leqslant \frac{e^{12}}{(\gamma_0)^{7/2}}\,, \end{aligned}$$

where $\gamma_0 = \gamma_0(|E(U)|, E_{\max}(U))$ is as in Proposition F.1. Altogether it follows that

$$|Ny_k| \leqslant N\tau\bigg(\frac{e^{14}}{N}\bigg)^{11/2} + \frac{o_\eta(1)e^6}{\delta'(\gamma_0)^{7/4}}\,,$$

and the claim follows by summing over $k \leqslant M = N\alpha$. ■

We now finally finish the proof of the main theorem:

**Proof** [Proof of Theorem 1.1 (conclusion)] The proof of the upper bound was given at the end of Section C, after the proof of Theorem 1.4. The proof of the lower bound in the case $\|u\|_\infty < \infty$ was given at the end of Section D, after the proof of Theorem 1.5. It remains to prove the lower bound in the case $\|u\|_\infty = \infty$. We follow the proof sketch given at the end of Section 1. It follows from Propositions 1.6 and 1.7 that

$$\mathbb{P}\left( \left| \frac{1}{N} \log_{N\tau}\left( \frac{\boldsymbol{Z}}{2^N} \right) - \frac{1}{N} \mathbb{E} \log_{N\tau}\left( \frac{\boldsymbol{Z}(\eta)}{2^N} \right) \right| \geqslant \frac{(\log N)^2}{N^{1/2}} + o_\eta(1) \right) \leqslant o_N(1)\,. \tag{225}$$

Given $\epsilon > 0$, we can choose $\eta$ small enough such that the $o_\eta(1)$ error above is at most $\epsilon$ in absolute value. By Proposition 1.8 together with Corollary F.10, for $0 < \alpha \leqslant \alpha_\wr(U)$ and $\eta$ small enough we have

$$\mathbb{P}\left( \frac{1}{N} \log \boldsymbol{Z}(\eta) \leqslant \mathrm{RS}(\alpha; U) - 2\epsilon \right) \leqslant \mathbb{P}\left( \frac{1}{N} \log \boldsymbol{Z}(\eta) \leqslant \mathrm{RS}(\alpha; U_\eta) - \epsilon \right) \leqslant o_N(1)\,. \tag{226}$$

It follows from Corollary B.8 that $\mathrm{RS}(\alpha; U) \geqslant \log 2 - \tau/4$ for $0 < \alpha \leqslant \alpha(U)$, so taking $\epsilon \leqslant \tau/8$ in the above gives

$$0 \leqslant \frac{1}{N} \left\{ \mathbb{E} \log_{N\tau}\left( \frac{\boldsymbol{Z}(\eta)}{2^N} \right) - \mathbb{E} \log\left( \frac{\boldsymbol{Z}(\eta)}{2^N} \right) \right\} \leqslant \tau \mathbb{P}\left( \frac{1}{N} \log \frac{\boldsymbol{Z}(\eta)}{2^N} \leqslant -\frac{\tau}{2} \right) \overset{(226)}{\leqslant} o_N(1)\,.$$

It follows by combining with (225) and (226) that

$$\mathbb{P}\left( \frac{1}{N} \log_{N\tau}\left( \frac{\boldsymbol{Z}}{2^N} \right) \leqslant \mathrm{RS}(\alpha; U) - \log 2 - 4\epsilon \right) \leqslant o_N(1)\,.$$

Since $\mathrm{RS}(\alpha; U) - \log 2 - 4\epsilon \geqslant -\tau/4 - 4\epsilon \geqslant -\tau$, it follows that in fact

$$\mathbb{P}\left( \frac{1}{N} \log \boldsymbol{Z} \leqslant \mathrm{RS}(\alpha; U) - 4\epsilon \right) \leqslant o_N(1)\,,$$

as claimed. ■

## Appendix G. Review of AMP for perceptron

In §G.1 and G.2 we prove Lemma A.16. In the rest of the section, we give a heuristic derivation of the state evolution recursions introduced in Definition A.2. We emphasize that §G.1 and G.2 are rigorous, while §G.3–G.4 are not (and are intended only to provide intuition). For rigorous derivations of the asymptotics described in §G.3–G.4, we again refer the reader to Bayati and Montanari (2011); Bolthausen (2014).

### G.1. Gaussian conditioning results

Suppose for simplicity that $t, F : \mathbb{R} \to \mathbb{R}$ are two smooth functions. Let $Z$ denote a standard gaussian random variable. Suppose we have $(q, \psi)$ such that (cf. (9))

$$\begin{pmatrix} q \\ \psi \end{pmatrix} = \begin{pmatrix} \mathbb{E}[t(\psi^{1/2}Z)^2] \\ \alpha\mathbb{E}[F(q^{1/2}Z)^2] \end{pmatrix} . \tag{227}$$

Let $\mathbf{m}^{(0)} = \mathbf{0} \in \mathbb{R}^N$, $\mathbf{n}^{(0)} = \mathbf{0} \in \mathbb{R}^M$, $\mathbf{m}^{(1)} = q^{1/2}\mathbf{1} \in \mathbb{R}^N$, $\mathbf{n}^{(1)} = (\psi/\alpha)^{1/2}\mathbf{1} \in \mathbb{R}^M$. The AMP iteration in this setting is given by (cf. (14) and (15))

$$\mathbf{m}^{(t+1)} = t\left(\frac{\boldsymbol{G}^{\mathrm{t}}\mathbf{n}^{(t)}}{N^{1/2}} - \beta\mathbf{m}^{(t-1)}\right) \in \mathbb{R}^N , \tag{228}$$

$$\mathbf{n}^{(t+1)} = F\left(\frac{\boldsymbol{G}\mathbf{m}^{(t)}}{N^{1/2}} - \beta'\mathbf{n}^{(t-1)}\right) \in \mathbb{R}^M , \tag{229}$$

where the Onsager coefficients are defined as (cf. (30))

$$\begin{pmatrix} \beta \\ \beta' \end{pmatrix} = \begin{pmatrix} \alpha\mathbb{E}F'(q^{1/2}Z) \\ \mathbb{E}t'(\psi^{1/2}Z) \end{pmatrix} .$$

A preliminary observation is the following:

**Lemma G.1** *Let $G$ be any $M \times N$ matrix with real entries. Suppose $\mathbf{r}$ is a unit vector in $\mathbb{R}^N$, while $\mathbf{c}$ is a unit vector in $\mathbb{R}^M$. Denote $\boldsymbol{R}_a \equiv \mathbf{e}_a\mathbf{r}^{\mathrm{t}}$ for $a \leqslant M$, and denote $\boldsymbol{C}_i \equiv \mathbf{c}(\mathbf{e}_i)^{\mathrm{t}}$ for $i \leqslant N$. Let $V_{\mathrm{R}}$ be the span of all the $\boldsymbol{R}_a$; let $V_{\mathrm{C}}$ be the span of all the $\boldsymbol{C}_i$; and let $V \equiv V_{\mathrm{RC}} \equiv V_{\mathrm{R}} + V_{\mathrm{C}}$. Then*

$$\mathrm{proj}_V(G) = (G\mathbf{r})\mathbf{r}^{\mathrm{t}} + \mathbf{c}(G^{\mathrm{t}}\mathbf{c})^{\mathrm{t}} - (\mathbf{c}^{\mathrm{t}}G\mathbf{r})\mathbf{c}\mathbf{r}^{\mathrm{t}} \equiv \boldsymbol{\Gamma}\Big(\mathbf{r}, \mathbf{c}, G\mathbf{r}, G^{\mathrm{t}}\mathbf{c}\Big)$$

*where $\mathrm{proj}_V$ denotes orthogonal projection onto $V$.*

**Proof** Write $(\cdot, \cdot)$ for the Frobenius inner product. The $\boldsymbol{R}_a$ form an orthonormal basis for $V_{\mathrm{R}}$, so

$$\mathrm{proj}_{V_{\mathrm{R}}}(G) = \sum_{a \leqslant M} (G, \boldsymbol{R}_a)\boldsymbol{R}_a = \sum_{a \leqslant M} (G\mathbf{r})_a\mathbf{e}_a\mathbf{r}^{\mathrm{t}} = G\mathbf{r}\mathbf{r}^{\mathrm{t}} .$$

Similarly, the $\boldsymbol{C}_i$ form an orthonormal basis for $V_{\mathrm{C}}$, so

$$\mathrm{proj}_{V_{\mathrm{C}}}(G) = \sum_{i \leqslant N} (G, \boldsymbol{C}_i)\boldsymbol{C}_i = \sum_{i \leqslant N} (G^{\mathrm{t}}\mathbf{c})_i\mathbf{c}(\mathbf{e}_i)^{\mathrm{t}} = \mathbf{c}\mathbf{c}^{\mathrm{t}}G .$$

The lemma follows by noting that the matrix $\Gamma = \boldsymbol{\Gamma}(\mathbf{r}, \mathbf{c}, G\mathbf{r}, G^{\mathrm{t}}\mathbf{c})$ lies in $V$, and satisfies the conditions $(G - \Gamma, \boldsymbol{R}_a) = 0$ for all $a \leqslant M$, as well as $(G - \Gamma, \boldsymbol{C}_i) = 0$ for all $i \leqslant N$. ■

**Corollary G.2** *Let $\boldsymbol{G}$ be an $M \times N$ random matrix with jointly gaussian entries. Suppose $\mathbf{r}$ is a unit vector in $\mathbb{R}^N$, while $\mathbf{c}$ is a unit vector in $\mathbb{R}^M$, and let $V \equiv V_{\mathrm{RC}}$ as in Lemma G.1. Then*

$$\mathbb{E}\Big(\boldsymbol{G}\,\Big|\,\boldsymbol{G}\mathbf{r}, \boldsymbol{G}^{\mathrm{t}}\mathbf{c}\Big) = \boldsymbol{\Gamma}\Big(\mathbf{r}, \mathbf{c}, \boldsymbol{G}\mathbf{r}, \boldsymbol{G}^{\mathrm{t}}\mathbf{c}\Big) \equiv \boldsymbol{\Gamma} \tag{230}$$

*as long as $\mathrm{proj}_V(\boldsymbol{G})$ is independent of $\boldsymbol{G} - \mathrm{proj}_V(\boldsymbol{G})$.*

**Proof** Conditioning on $\boldsymbol{G}\mathbf{r}$ amounts to conditioning on the Frobenius inner products $(\boldsymbol{G}, \boldsymbol{R}_a)$ for all $a \leqslant M$. Similarly, conditioning on $\boldsymbol{G}^{\mathsf{t}}\mathbf{c}$ amounts to conditioning on the inner products $(\boldsymbol{G}, \boldsymbol{C}_i)$ for all $i \leqslant N$. By Lemma G.1, $\operatorname{proj}_V(\boldsymbol{G})$ equals $\boldsymbol{\Gamma}$, which is a measurable function of $(\boldsymbol{G}\mathbf{r}, \boldsymbol{G}^{\mathsf{t}}\mathbf{c})$. If $\boldsymbol{G} - \boldsymbol{\Gamma}$ is independent of $\boldsymbol{\Gamma}$, then it follows that $\boldsymbol{\Gamma}$ equals the conditional expectation of $\boldsymbol{G}$ given $(\boldsymbol{G}\mathbf{r}, \boldsymbol{G}^{\mathsf{t}}\mathbf{c})$. ■

Let $\mathbf{r}^{(1)}, \ldots, \mathbf{r}^{(t)}$ be the Gram–Schmidt orthogonalization of the vectors $\mathbf{m}^{(1)}, \ldots, \mathbf{m}^{(t)}$. Likewise let $\mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(t)}$ be the Gram–Schmidt orthogonalization of the vectors $\mathbf{n}^{(1)}, \ldots, \mathbf{n}^{(t)}$. Let $\boldsymbol{G}^{(1)} \equiv \boldsymbol{G}$, and suppose recursively that $\boldsymbol{G}^{(s)}$ has been defined. Let $\boldsymbol{G}^{(s)}\mathbf{r}^{(s)} = \bar{\mathbf{x}}^{(s)}$, $(\boldsymbol{G}^{(s)})^{\mathsf{t}}\mathbf{c}^{(s)} = \bar{\mathbf{y}}^{(s)}$, and define (cf. (230))

$$\boldsymbol{G}^{(s+1)} \equiv \boldsymbol{G}^{(s)} - \boldsymbol{\Gamma}\bigg(\mathbf{r}^{(s)}, \mathbf{c}^{(s)}, \bar{\mathbf{x}}^{(s)}, \bar{\mathbf{y}}^{(s)}\bigg) \equiv \boldsymbol{G}^{(s)} - \boldsymbol{\Gamma}^{(s)} . \tag{231}$$

We also define a corresponding $\sigma$-field

$$\mathscr{F}_\star(t) \equiv \sigma\bigg((\bar{\mathbf{x}}^{(s)} : s \leqslant t), (\bar{\mathbf{y}}^{(s)} : s \leqslant t)\bigg) . \tag{232}$$

The next lemma records some basic facts about $\mathscr{F}_\star(t)$.

**Lemma G.3** *For the AMP iteration described above, the random variables*

$$\bigg(\Big(\mathbf{m}^{(s)}, \mathbf{n}^{(s)}, \mathbf{r}^{(s)}, \mathbf{c}^{(s)} : s \leqslant t+1\Big), \Big(\boldsymbol{G}\mathbf{m}^{(\ell)}, \boldsymbol{G}^{\mathsf{t}}\mathbf{n}^{(\ell)}, \boldsymbol{G}\mathbf{r}^{(\ell)}, \boldsymbol{G}^{\mathsf{t}}\mathbf{c}^{(\ell)}, \boldsymbol{\Gamma}^{(\ell)} : \ell \leqslant t\Big)\bigg)$$

*are all measurable with respect to $\mathscr{F}_\star(t)$.*

**Proof** Recall that the initial vectors $\mathbf{m}^{(0)}$, $\mathbf{n}^{(0)}$, $\mathbf{m}^{(1)}$, $\mathbf{n}^{(1)}$ are fixed and deterministic, so they are measurable with respect to the trivial $\sigma$-field $\mathscr{F}_\star(0)$. From these we can also obtain the deterministic vectors $\mathbf{r}^{(1)}$ and $\mathbf{c}^{(1)}$. Next we consider the $\sigma$-field $\mathscr{F}_\star(1)$: it is clear that $\boldsymbol{\Gamma}^{(1)}$ is $\mathscr{F}_\star(1)$-measurable. Next note that

$$\bar{\mathbf{x}}^{(1)} = \boldsymbol{G}\mathbf{r}^{(1)} = \frac{\boldsymbol{G}\mathbf{m}^{(1)}}{\|\mathbf{m}^{(1)}\|} , \quad \bar{\mathbf{y}}^{(1)} = \boldsymbol{G}^{\mathsf{t}}\mathbf{c}^{(1)} = \frac{\boldsymbol{G}^{\mathsf{t}}\mathbf{n}^{(1)}}{\|\mathbf{n}^{(1)}\|} ,$$

so we see that $\boldsymbol{G}\mathbf{m}^{(1)}$ and $\boldsymbol{G}^{\mathsf{t}}\mathbf{n}^{(1)}$ are measurable with respect to $\mathscr{F}_\star(1)$. We can then apply the AMP iteration (228) and (229) to obtain $\mathbf{m}^{(2)}$ and $\mathbf{n}^{(2)}$, so these are also measurable with respect to $\mathscr{F}_\star(1)$. It follows by Gram–Schmidt orthogonalization that $\mathbf{r}^{(2)}$ and $\mathbf{c}^{(1)}$ are also $\mathscr{F}_\star(1)$-measurable.

Now suppose inductively that the claim holds up to $\mathscr{F}_\star(t-1)$, and consider the $\sigma$-field $\mathscr{F}_\star(t)$. Then the matrix $\boldsymbol{\Gamma}^{(t)}$ is clearly $\mathscr{F}_\star(t)$-measurable. Next note that (231) implies

$$\boldsymbol{G} = \boldsymbol{G}^{(1)} = \boldsymbol{\Gamma}^{(1)} + \boldsymbol{G}^{(2)} = \ldots = \sum_{s=1}^{t-1} \boldsymbol{\Gamma}^{(s)} + \boldsymbol{G}^{(t)} ,$$

where the $\boldsymbol{\Gamma}^{(s)}$, $s \leqslant t-1$, are all measurable with respect to $\mathscr{F}_\star(t-1) \subseteq \mathscr{F}_\star(t)$. Therefore

$$\boldsymbol{G}\mathbf{r}^{(t)} = \sum_{s=1}^{t-1} \boldsymbol{\Gamma}^{(s)}\mathbf{r}^{(t)} + \bar{\mathbf{x}}^{(t)}$$

is $\mathscr{F}_\star(t)$-measurable, as is $\boldsymbol{G}^{\mathrm{t}}\mathbf{c}^{(t)}$. Recall from the Gram–Schmidt orthogonalization that

$$\mathbf{r}^{(t)} = \frac{\mathbf{m}^{(t)} - \sum_{s\leqslant t-1}(\mathbf{m}^{(t)}, \mathbf{r}^{(s)})\mathbf{r}^{(s)}}{\|\mathbf{m}^{(t)} - \sum_{s\leqslant t-1}(\mathbf{m}^{(t)}, \mathbf{r}^{(s)})\mathbf{r}^{(s)}\|},$$

which we can rearrange to obtain an expression for $\mathbf{m}^{(t)}$. It follows from this that $\boldsymbol{G}\mathbf{m}^{(t)}$ is $\mathscr{F}_\star(t)$-measurable, as is $\boldsymbol{G}^{\mathrm{t}}\mathbf{n}^{(t)}$. We can then apply the AMP iteration (228) and (229) to obtain $\mathbf{m}^{(t+1)}$ and $\mathbf{n}^{(t+1)}$, so these are also measurable with respect to $\mathscr{F}_\star(t)$. Finally, it follows by Gram–Schmidt orthogonalization that $\mathbf{r}^{(t+1)}$ and $\mathbf{c}^{(t+1)}$ are also $\mathscr{F}_\star(t)$-measurable. This verifies the inductive hypothesis and proves the claim. ■

## G.2. Projection and resampling

In this subsection we give the proof of Lemma A.16. For notational convenience, the roles of $\boldsymbol{G}$ and $\boldsymbol{G}'$ through this section are switched from the main body of the paper.

**Definition G.4 (similar to Definition A.14)** *Given $\mathscr{F}_\star(t-1)$ as in (232), consider the linear subspaces*

$$V_{\mathrm{R}}(t) \equiv \operatorname{span}\left\{\mathbf{e}_a(\mathbf{m}^{(s)})^{\mathrm{t}} : 1 \leqslant a \leqslant M, 1 \leqslant s \leqslant t\right\},$$
$$V_{\mathrm{C}}(t) \equiv \operatorname{span}\left\{\mathbf{n}^{(\ell)}(\mathbf{e}_i)^{\mathrm{t}} : 1 \leqslant i \leqslant N, 1 \leqslant \ell \leqslant t\right\}.$$

*It follows from Lemma G.3 that these (random) subspaces are measurable with respect to $\mathscr{F}_\star(t-1)$. Let $V_\star(t) = V_{\mathrm{R}}(t) + V_{\mathrm{C}}(t)$, and let $\operatorname{proj}_t$ denote orthogonal projection onto $V_\star(t)$.*

We remark that $V_\star(t)$ is very similar to the (random) subspace $V_{\mathrm{RC}} = V_{\mathrm{R}}(t) + V_{\mathrm{C}}(t-1)$ which appears in the proof of Lemma A.16. We will address the discrepancy between $V_\star(t)$ and $V_{\mathrm{RC}}$ in the proof of Lemma A.16, below. The following is a straightforward consequence of the preceding lemmas and the definition:

**Corollary G.5** *Let $\boldsymbol{G}$ be an $M \times N$ matrix with i.i.d. standard gaussian entries. With $\mathscr{F}_\star(t)$ as in (232),*

$$\mathbb{E}\Big(\boldsymbol{G}\,\Big|\,\mathscr{F}_\star(t)\Big) = \sum_{s\leqslant t}\boldsymbol{\Gamma}^{(s)} = \boldsymbol{G} - \boldsymbol{G}^{(t+1)} = \operatorname{proj}_t(\boldsymbol{G}),$$

*where $\operatorname{proj}_t$ is the orthogonal projection onto the (random) subspace $V_\star(t)$ from Definition G.4. Moreover, conditional on $\mathscr{F}_\star(t-1)$, $\boldsymbol{G}^{(t+1)}$ is distributed as a standard gaussian element of the ($\mathscr{F}_\star(t-1)$-measurable) subspace $V_\star(t)^\perp$, and is independent of $\mathscr{F}_\star(t)$.*

**Proof** Note that the recursive definition (231) implies

$$\boldsymbol{G}^{(t)} = \boldsymbol{G}^{(t-1)} - \boldsymbol{\Gamma}^{(t-1)} = \ldots = \boldsymbol{G} - \sum_{s=1}^{t-1}\boldsymbol{\Gamma}^{(s)}. \tag{233}$$

By induction, conditional on $\mathscr{F}_\star(t-2)$, the random matrix $\boldsymbol{G}^{(t)}$ is distributed as a standard gaussian element of the ($\mathscr{F}_\star(t-2)$-measurable) subspace $V_\star(t-1)^\perp$, and is independent of $\mathscr{F}_\star(t-1)$.

It follows that $\boldsymbol{G}^{(t)}$ has jointly gaussian entries conditional on $\mathscr{F}_\star(t-1)$. We also have from Lemma G.3 that the vectors $\mathbf{r}^{(t)}$ and $\mathbf{c}^{(t)}$ are measurable with respect to $\mathscr{F}_\star(t-1)$. Note that

$$\boldsymbol{G}^{(s+1)}\mathbf{r}^{(s)} = (\boldsymbol{G}^{(s)} - \boldsymbol{\Gamma}^{(s)})\mathbf{r}^{(s)} = \mathbf{0} \in \mathbb{R}^M$$

by the construction of $\boldsymbol{\Gamma}^{(s)}$, and likewise $(\boldsymbol{G}^{(s+1)})^{\mathrm{t}}\mathbf{c}^{(s)} = 0$. As a result

$$\boldsymbol{\Gamma}^{(s+1)}\mathbf{r}^{(s)} = \Big(\boldsymbol{G}\mathbf{r}\mathbf{r}^{\mathrm{t}} + \mathbf{c}\mathbf{c}^{\mathrm{t}}\boldsymbol{G} - (\mathbf{c}^{\mathrm{t}}\boldsymbol{G}\mathbf{r})\mathbf{c}\mathbf{r}^{\mathrm{t}}\Big)^{(s+1)}\mathbf{r}^{(s)} = \mathbf{0} \in \mathbb{R}^M\,,$$

and similarly $(\boldsymbol{\Gamma}^{(s+1)})^{\mathrm{t}}\mathbf{c}^{(s)} = \mathbf{0} \in \mathbb{R}^N$. One can then show by induction that for all $s < t$ we have $\boldsymbol{G}^{(t)}\mathbf{r}^{(s)} = \mathbf{0} \in \mathbb{R}^M$, and likewise $(\boldsymbol{G}^{(t)})^{\mathrm{t}}\mathbf{c}^{(s)} = \mathbf{0} \in \mathbb{R}^N$. It follows that

$$\Big(\boldsymbol{G}^{(t)} - \boldsymbol{\Gamma}^{(t)}, \mathbf{e}_a(\mathbf{r}^{(s)})^{\mathrm{t}}\Big) = 0 = \Big(\boldsymbol{G}^{(t)} - \boldsymbol{\Gamma}^{(t)}, \mathbf{c}^{(s)}(\mathbf{e}_i)^{\mathrm{t}}\Big)$$

for all $s \leqslant t$. This shows that $\boldsymbol{\Gamma}^{(t)}$ is the orthogonal projection of $\boldsymbol{G}^{(t)}$ onto $V_\star(t)$. We further have, for all $\ell \leqslant t$,

$$\Big(\boldsymbol{G} - \sum_{s\leqslant t}\boldsymbol{\Gamma}^{(s)}\Big)\mathbf{r}^{(\ell)} \overset{(233)}{=} \boldsymbol{G}^{(t+1)}\mathbf{r}^{(\ell)} = \mathbf{0} \in \mathbb{R}^M\,,$$
$$\Big(\boldsymbol{G} - \sum_{s\leqslant t}\boldsymbol{\Gamma}^{(s)}\Big)^{\mathrm{t}}\mathbf{c}^{(\ell)} \overset{(233)}{=} (\boldsymbol{G}^{(t+1)})^{\mathrm{t}}\mathbf{c}^{(\ell)} = \mathbf{0} \in \mathbb{R}^N\,.$$

This shows that $\boldsymbol{\Gamma}^{(1)} + \ldots + \boldsymbol{\Gamma}^{(t)}$ is the orthogonal projection of $\boldsymbol{G}$ onto $V_\star(t)$. It follows that $\boldsymbol{G}^{(t+1)}$ is the orthogonal projection of $\boldsymbol{G}$ onto $V_\star(t)^\perp$. On the other hand, the $\sigma$-field $\mathscr{F}_\star(t)$ is generated by $\mathscr{F}_\star(t-1)$ and the orthogonal projection of $\boldsymbol{G}^{(t)}$ onto $V_\star(t)$. Since $\boldsymbol{G}^{(t)}$ is standard gaussian given $\mathscr{F}_\star(t-1)$, it follows that $\boldsymbol{G}^{(t+1)}$ and $\mathscr{F}_\star(t)$ are independent given $\mathscr{F}_\star(t-1)$. We can therefore apply Corollary G.2 (conditional on $\mathscr{F}_\star(t-1)$) to conclude that

$$\mathbb{E}\Big(\boldsymbol{G}^{(t)}\,\Big|\,\mathscr{F}_\star(t)\Big) = \boldsymbol{\Gamma}\Big(\mathbf{r}^{(t)}, \mathbf{c}^{(t)}, \bar{\mathbf{x}}^{(t)}, \bar{\mathbf{y}}^{(t)}\Big) = \boldsymbol{\Gamma}^{(t)}\,. \tag{234}$$

It follows that

$$\mathbb{E}\Big(\boldsymbol{G}\,\Big|\,\mathscr{F}_\star(t)\Big) \overset{(231)}{=} \mathbb{E}\Big(\sum_{s\leqslant t-1}\boldsymbol{\Gamma}^{(s)} + \boldsymbol{G}^{(t)}\,\Big|\,\mathscr{F}_\star(t)\Big) = \sum_{s\leqslant t-1}\boldsymbol{\Gamma}^{(s)} + \mathbb{E}\Big(\boldsymbol{G}^{(t)}\,\Big|\,\mathscr{F}_\star(t)\Big)$$
$$\overset{(234)}{=} \sum_{s\leqslant t}\boldsymbol{\Gamma}^{(s)} \overset{(233)}{=} \boldsymbol{G} - \boldsymbol{G}^{(t+1)}\,,$$

which concludes the proof. ■

The next result is similar to Lemma A.16:

**Lemma G.6** *Let $\boldsymbol{G}$ be an $M \times N$ matrix with i.i.d. gaussian entries, and use it to define $\mathscr{F}_\star(t)$ as in (232). As in Definition G.4, let* $\mathrm{proj}_t$ *denote the orthogonal projection onto the $\mathscr{F}_\star(t-1)$-measurable subspace $V_\star(t)$. Then, for any bounded measurable function $f : \mathbb{R}^{M\times N} \to \mathbb{R}$, we* *have*

$$\mathbb{E}\left( f(\boldsymbol{G}^{(t+1)}) \,\middle|\, \mathscr{F}_\star(t) \right) = \mathbb{E}\left( f(\boldsymbol{G}^{(t+1)}) \,\middle|\, \mathscr{F}_\star(t-1) \right) \tag{235}$$

$$= \mathbb{E}\left( f\Big(\boldsymbol{G}' - \mathrm{proj}_t(\boldsymbol{G}')\Big) \,\middle|\, \mathscr{F}_\star(t-1) \right) \tag{236}$$

*where $\boldsymbol{G}'$ is an independent copy of $\boldsymbol{G}$.*

**Proof** We saw in Corollary G.5 that $\boldsymbol{G}^{(t+1)}$ and $\mathscr{F}_\star(t)$ are independent conditional on $\mathscr{F}_\star(t-1)$, so the first claim (235) follows. Since $\boldsymbol{G}$ and $\boldsymbol{G}'$ are independent, if we condition on $\mathscr{F}_\star(t-1)$ then the random matrix $\boldsymbol{G}' - \mathrm{proj}_t(\boldsymbol{G}')$ is also distributed as a standard gaussian element of $V_\star(t)^\perp$. This implies (236). ■

**Remark G.7** *We can also give a more explicit description of the projection of $\boldsymbol{G}'$ onto $V_\star(t)$, although it is not needed in the above proof of Lemma G.6. Define $\boldsymbol{G}^{\bullet(1)} \equiv \boldsymbol{G}'$, and recursively*

$$\boldsymbol{G}^{\bullet(t+1)} \equiv \boldsymbol{G}^{\bullet(t)} - \boldsymbol{\Gamma}^{\bullet(t)} \equiv \boldsymbol{G}^{\bullet(t)} - \boldsymbol{\Gamma}\left( \mathbf{r}^{(t)}, \mathbf{c}^{(t)}, \boldsymbol{G}^{\bullet(t)}\mathbf{r}^{(t)}, (\boldsymbol{G}^{\bullet(t)})^{\mathrm{t}}\mathbf{r}^{(t)} \right). \tag{237}$$

*Note that $\boldsymbol{\Gamma}^{\bullet(t)}$ is defined using the vectors $\mathbf{r}^{(t)}$ and $\mathbf{c}^{(t)}$ that came from $\boldsymbol{G}$, not $\boldsymbol{G}'$. As in Definition G.4, we let $\mathrm{proj}_t$ denote the orthogonal projection onto the $\mathscr{F}_\star(t-1)$-measurable subspace $V_\star(t)$. We then claim that*

$$\mathrm{proj}_t(\boldsymbol{G}') = \boldsymbol{G}' - \boldsymbol{G}^{\bullet(t+1)} \overset{(237)}{=} \sum_{s\leqslant t} \boldsymbol{\Gamma}^{\bullet(t)}. \tag{238}$$

*This is very similar to the proof of Corollary G.5, but in fact simpler because $\boldsymbol{G}$ and $\boldsymbol{G}'$ are independent, which implies that $\boldsymbol{G}'$ is independent of the random subspace $V_\star(t)$. Arguing as before, we have by construction $\boldsymbol{G}^{\bullet(s+1)}\mathbf{r}^{(s)} = \mathbf{0}$ and $(\boldsymbol{G}^{\bullet(s+1)})^{\mathrm{t}}\mathbf{c}^{(s)} = \mathbf{0}$. One can then show by induction that for all $s < t$ we have $\boldsymbol{G}^{\bullet(t)}\mathbf{r}^{(s)} = \mathbf{0}$ and $(\boldsymbol{G}^{\bullet(t)})^{\mathrm{t}}\mathbf{c}^{(s)} = \mathbf{0}$. This implies, for all $\ell \leqslant t$,*

$$\Big(\boldsymbol{G}' - \sum_{s\leqslant t}\boldsymbol{\Gamma}^{\bullet(s)}\Big)\mathbf{r}^{(\ell)} \overset{(237)}{=} \boldsymbol{G}^{\bullet(t+1)}\mathbf{r}^{(\ell)} = \mathbf{0} \in \mathbb{R}^M,$$

$$\Big(\boldsymbol{G}' - \sum_{s\leqslant t}\boldsymbol{\Gamma}^{\bullet(s)}\Big)^{\mathrm{t}}\mathbf{c}^{(\ell)} \overset{(237)}{=} (\boldsymbol{G}^{\bullet(t+1)})^{\mathrm{t}}\mathbf{c}^{(\ell)} = \mathbf{0} \in \mathbb{R}^N.$$

*It follows from this that $\boldsymbol{G}^{\bullet(t+1)}$ is orthogonal to $V_\star(t)$. This verifies (238), since we see that the right-hand side of (238) lies in $V_\star(t)$.*

**Proof** [Proof of Lemma A.16] Recall that, for notational convenience, the roles of $\boldsymbol{G}$ and $\boldsymbol{G}'$ in this section are switched from the statement of Lemma A.16. Thus, for the purposes of the proof, we use $\boldsymbol{G}$ for the AMP iteration (228) and (229), and this defines $\mathscr{F}_\star(t)$ as in (232). We also let R and C be as in Definition A.15, but with $\boldsymbol{G}$ and $\boldsymbol{G}'$ switched. The $\sigma$-field $\mathscr{F}(t)$ from (16) is very closely related to $\mathscr{F}_\star(t-1)$, but is not exactly the same: indeed, we can see from the proof of Lemma G.3 that

$$\mathscr{F}(t) = \sigma\Big(\mathscr{F}_\star(t-1), \bar{\mathbf{x}}^{(t)}\Big) = \sigma\Big(\mathscr{F}_\star(t-1), \boldsymbol{G}\mathbf{m}^{(t)}, \mathbf{n}^{(t+1)}\Big).$$

By a similar (but simpler) argument as in Corollary G.5, we see that

$$\mathbb{E}\Big(\boldsymbol{G}\,\Big|\,\mathscr{F}(t)\Big) = \sum_{s\leqslant t-1}\boldsymbol{\Gamma}^{(s)} + \mathbf{r}^{(t)}\bar{\mathbf{x}}^{(t)}(\bar{\mathbf{x}}^{(t)})^{\mathrm{t}} = \mathrm{proj}_{\mathrm{RC}}(\boldsymbol{G}) = \boldsymbol{G}_{\mathrm{RC}}\,,$$

where $\mathrm{proj}_{\mathrm{RC}}$ denotes orthogonal projection onto $V_{\mathrm{RC}}$ as in Definition A.14, except that $V_{\mathrm{RC}}$ here is defined for $\boldsymbol{G}$ rather than $\boldsymbol{G}'$. Conditional on $\mathscr{F}(t-1)$, the random matrix $\boldsymbol{G} - \mathrm{proj}_{\mathrm{RC}}(\boldsymbol{G})$ is distributed as a standard gaussian element of the $\mathscr{F}(t-1)$-measurable vector space $(V_{\mathrm{RC}})^{\perp}$, and is conditionally independent of $\mathscr{F}(t)$. Therefore

$$\mathbb{E}\Big(f(\boldsymbol{G})\,\Big|\,\mathscr{F}(t)\Big) = \mathbb{E}\Big[f\Big(\boldsymbol{G}_{\mathrm{RC}} + \Big(\boldsymbol{G}' - \mathrm{proj}_{\mathrm{RC}}(\boldsymbol{G}')\Big)\Big)\,\Big|\,\mathscr{F}(t)\Big] = \mathbb{E}\Big(f(\boldsymbol{G}')\,\Big|\,\mathrm{R},\mathrm{C},\boldsymbol{G}_{\mathrm{RC}}\Big)\,.$$

This concludes the proof. ■

### G.3. AMP iterates at $t = 2$ and $t = 3$

Returning to the AMP iteration (228) and (229) we have (cf. (38) and (39))

$$\begin{aligned}\mathbf{m}^{(2)} &\equiv t(\mathbf{H}^{(2)}) = t\bigg(\frac{\boldsymbol{G}^{\mathrm{t}}\mathbf{n}^{(1)}}{N^{1/2}}\bigg) = t\bigg(\psi^{1/2}\boldsymbol{G}^{\mathrm{t}}\frac{\mathbf{n}^{(1)}}{(N\psi)^{1/2}}\bigg) = t(\psi^{1/2}\boldsymbol{G}^{\mathrm{t}}\mathbf{c}^{(1)}) = t(\psi^{1/2}\bar{\mathbf{y}}^{(1)})\,,\\ \mathbf{n}^{(2)} &\equiv F(\mathbf{h}^{(2)}) = F\bigg(\frac{\boldsymbol{G}\mathbf{m}^{(1)}}{N^{1/2}}\bigg) = F\bigg(q^{1/2}\boldsymbol{G}\frac{\mathbf{m}^{(1)}}{(Nq)^{1/2}}\bigg) = F(q^{1/2}\boldsymbol{G}\mathbf{r}^{(1)}) = F(q^{1/2}\bar{\mathbf{x}}^{(1)})\,.\end{aligned}\tag{239}$$

It follows using (227) that $\|\mathbf{m}^{(2)}\|^2 \simeq Nq$, $\|\mathbf{n}^{(2)}\|^2 \simeq N\psi$, and moreover (cf. (32))

$$\begin{aligned}\frac{(\mathbf{m}^{(2)},\mathbf{m}^{(1)})}{Nq} &\simeq \Big(\frac{1}{q}\Big)^{1/2}\mathbb{E}t(\psi^{1/2}Z) \equiv \lambda_1 \equiv \rho_1\,,\\ \frac{(\mathbf{n}^{(2)},\mathbf{n}^{(1)})}{N\psi} &\simeq \Big(\frac{\alpha}{\psi}\Big)^{1/2}\mathbb{E}F(q^{1/2}Z) \equiv \gamma_1 \equiv \mu_1\,.\end{aligned}\tag{240}$$

Therefore in the Gram–Schmidt orthogonalization we have

$$\begin{aligned}\mathbf{r}^{(2)} &= \frac{(\mathbf{m}^{(2)})^{\perp}}{\|(\mathbf{m}^{(2)})^{\perp}\|} \simeq \frac{\mathbf{m}^{(2)} - \lambda_1\mathbf{m}^{(1)}}{[Nq(1-(\lambda_1)^2)]^{1/2}}\,,\\ \mathbf{c}^{(2)} &= \frac{(\mathbf{n}^{(2)})^{\perp}}{\|(\mathbf{n}^{(2)})^{\perp}\|} \simeq \frac{\mathbf{n}^{(2)} - \gamma_1\mathbf{n}^{(1)}}{[N\psi(1-(\gamma_1)^2)]^{1/2}}\,.\end{aligned}\tag{241}$$

We can express the $\mathbf{m}$, $\mathbf{n}$ vectors in terms of the $\mathbf{r}$, $\mathbf{c}$ vectors as

$$\begin{aligned}\frac{\mathbf{m}^{(2)}}{(Nq)^{1/2}} &\simeq \lambda_1\mathbf{r}^{(1)} + \Big(1-(\lambda_1)^2\Big)^{1/2}\mathbf{r}^{(2)}\,,\\ \frac{\mathbf{n}^{(2)}}{(N\psi)^{1/2}} &\simeq \gamma_1\mathbf{c}^{(1)} + \Big(1-(\gamma_1)^2\Big)^{1/2}\mathbf{c}^{(2)}\,.\end{aligned}\tag{242}$$

At the next step of the AMP iteration we have (cf. (239))

$$\begin{aligned}
\mathbf{m}^{(3)} &\equiv t(\mathbf{H}^{(3)}) = t\left(\frac{\boldsymbol{G}^{\mathrm{t}}\mathbf{n}^{(2)}}{N^{1/2}} - \beta\mathbf{m}^{(1)}\right) = t\left(\frac{(\boldsymbol{G}^{(2)})^{\mathrm{t}}(\mathbf{n}^{(2)})^{\perp}}{N^{1/2}} + \frac{(\boldsymbol{\Gamma}^{(1)})^{\mathrm{t}}\mathbf{n}^{(2)}}{N^{1/2}} - \beta\mathbf{m}^{(1)}\right),\\
\mathbf{n}^{(3)} &\equiv t(\mathbf{h}^{(3)}) = F\left(\frac{\boldsymbol{G}\mathbf{m}^{(2)}}{N^{1/2}} - \beta'\mathbf{n}^{(1)}\right) = F\left(\frac{\boldsymbol{G}^{(2)}(\mathbf{m}^{(2)})^{\perp}}{N^{1/2}} + \frac{\boldsymbol{\Gamma}^{(1)}\mathbf{m}^{(2)}}{N^{1/2}} - \beta'\mathbf{n}^{(1)}\right). \qquad (243)
\end{aligned}$$

In order to evaluate $(\boldsymbol{\Gamma}^{(1)})^{\mathrm{t}}\mathbf{n}^{(2)}/N^{1/2}$, we calculate

$$\begin{aligned}
\left\{\frac{\mathbf{r}\mathbf{r}^{\mathrm{t}}\boldsymbol{G}^{\mathrm{t}}}{N^{1/2}}\right\}^{(1)}\mathbf{n}^{(2)} &= \frac{\mathbf{m}^{(1)}}{Nq^{1/2}}(\bar{\mathbf{x}}^{(1)},\mathbf{n}^{(2)}) = \frac{\mathbf{m}^{(1)}}{Nq^{1/2}}(\bar{\mathbf{x}}^{(1)},F(q^{1/2}\bar{\mathbf{x}}^{(1)})) \simeq \beta\mathbf{m}^{(1)},\\
\left\{\frac{\boldsymbol{G}^{\mathrm{t}}\mathbf{c}\mathbf{c}^{\mathrm{t}}}{N^{1/2}}\right\}^{(1)}\mathbf{n}^{(2)} &= \frac{\bar{\mathbf{y}}^{(1)}}{N^{1/2}}\frac{(\mathbf{n}^{(1)},\mathbf{n}^{(2)})}{(N\psi)^{1/2}} \simeq \psi^{1/2}\gamma_1\bar{\mathbf{y}}^{(1)},\\
\left\{\frac{(\mathbf{c}^{\mathrm{t}}\boldsymbol{G}\mathbf{r})\mathbf{r}\mathbf{c}^{\mathrm{t}}}{N^{1/2}}\right\}^{(1)}\mathbf{n}^{(2)} &= \frac{1}{N^{1/2}}\frac{\mathbf{1}^{\mathrm{t}}\boldsymbol{G}\mathbf{1}}{N\alpha^{1/2}}\frac{(\mathbf{n}^{(1)},\mathbf{n}^{(2)})}{N(q\psi)^{1/2}}\mathbf{m}^{(1)} = O\left(\frac{1}{N^{1/2}}\right)\mathbf{m}^{(1)}.
\end{aligned}$$

In order to evaluate $\boldsymbol{\Gamma}^{(1)}\mathbf{m}^{(2)}/N^{1/2}$, we calculate

$$\begin{aligned}
\left\{\frac{\boldsymbol{G}\mathbf{r}\mathbf{r}^{\mathrm{t}}}{N^{1/2}}\right\}^{(1)}\mathbf{m}^{(2)} &= \frac{\bar{\mathbf{x}}^{(1)}}{N^{1/2}}\frac{(\mathbf{m}^{(1)},\mathbf{m}^{(2)})}{(Nq)^{1/2}} \simeq q^{1/2}\lambda_1\bar{\mathbf{x}}^{(1)},\\
\left\{\frac{\mathbf{c}\mathbf{c}^{\mathrm{t}}\boldsymbol{G}}{N^{1/2}}\right\}^{(1)}\mathbf{m}^{(2)} &= \frac{\mathbf{n}^{(1)}}{N\psi^{1/2}}(\bar{\mathbf{y}}^{(1)},\mathbf{m}^{(2)}) = \frac{\mathbf{n}^{(1)}}{N\psi^{1/2}}(\bar{\mathbf{y}}^{(1)},t(\psi^{1/2}\bar{\mathbf{y}}^{(1)})) \simeq \beta'\mathbf{n}^{(1)},\\
\left\{\frac{(\mathbf{c}^{\mathrm{t}}\boldsymbol{G}\mathbf{r})\mathbf{c}\mathbf{r}^{\mathrm{t}}}{N^{1/2}}\right\}^{(1)}\mathbf{m}^{(2)} &= \frac{1}{N^{1/2}}\frac{\mathbf{1}^{\mathrm{t}}\boldsymbol{G}\mathbf{1}}{N\alpha^{1/2}}\frac{(\mathbf{m}^{(1)},\mathbf{m}^{(2)})}{N(q\psi)^{1/2}}\mathbf{n}^{(1)} = O\left(\frac{1}{N^{1/2}}\right)\mathbf{n}^{(1)}.
\end{aligned}$$

Substituting this back into (243) gives the decomposition (cf. (38), (39), and (239))

$$\begin{aligned}
\mathbf{m}^{(3)} &\equiv t(\mathbf{H}^{(3)}) \simeq t\left(\psi^{1/2}\left\{\gamma_1\bar{\mathbf{y}}^{(1)} + \left(1-(\gamma_1)^2\right)^{1/2}\bar{\mathbf{y}}^{(2)}\right\}\right),\\
\mathbf{n}^{(3)} &\equiv F(\mathbf{h}^{(3)}) \simeq F\left(q^{1/2}\left\{\lambda_1\bar{\mathbf{x}}^{(1)} + \left(1-(\lambda_1)^2\right)^{1/2}\bar{\mathbf{x}}^{(2)}\right\}\right). \qquad (244)
\end{aligned}$$

It follows that (240) continues to hold (approximately) with $\mathbf{m}^{(3)}$, $\mathbf{n}^{(3)}$ in place of $\mathbf{m}^{(2)}$, $\mathbf{n}^{(2)}$. We also see by combining (239) with (244) that

$$\begin{aligned}
\frac{(\mathbf{H}^{(2)},\mathbf{H}^{(3)})}{N\psi} &\simeq \frac{1}{N}\left(\bar{\mathbf{y}}^{(1)},\gamma_1\bar{\mathbf{y}}^{(1)} + \left(1-(\gamma_1)^2\right)\bar{\mathbf{y}}^{(2)}\right) \simeq \gamma_1 \equiv \mu_1,\\
\frac{(\mathbf{h}^{(2)},\mathbf{h}^{(3)})}{Mq} &\simeq \frac{1}{M}\left(\bar{\mathbf{x}}^{(1)},\lambda_1\bar{\mathbf{x}}^{(1)} + \left(1-(\lambda_1)^2\right)\bar{\mathbf{x}}^{(2)}\right) \simeq \lambda_1 \equiv \rho_1, \qquad (245)
\end{aligned}$$

from which we obtain (cf. (33))

$$\begin{aligned}
\frac{(\mathbf{m}^{(2)},\mathbf{m}^{(3)})}{Nq} &\simeq \frac{1}{q}\mathbb{E}\left[t\left(\psi^{1/2}\left\{\gamma_1 Z + \left(1-(\gamma_1)^2\right)^{1/2}\xi\right\}\right)t(\psi^{1/2}Z)\right] \equiv \rho(\gamma_1) = \rho(\mu_1) \equiv \rho_2,\\
\frac{(\mathbf{n}^{(2)},\mathbf{n}^{(3)})}{N\psi} &\simeq \frac{\alpha}{\psi}\mathbb{E}\left[F\left(q^{1/2}\left\{\lambda_1 Z + \left(1-(\lambda_1)^2\right)^{1/2}\xi\right\}\right)F(q^{1/2}Z)\right] \equiv \mu(\lambda_1) = \mu(\rho_1) \equiv \mu_2.
\end{aligned}$$

(246)

It follows that (cf. (34))

$$\begin{aligned}\left(\frac{\mathbf{m}^{(3)}}{(Nq)^{1/2}},\mathbf{r}^{(2)}\right) &\simeq \left(\frac{\mathbf{m}^{(3)}}{(Nq)^{1/2}},\frac{\mathbf{m}^{(2)}-\lambda_1\mathbf{m}^{(1)}}{[Nq(1-(\lambda_1)^2)]^{1/2}}\right)\simeq\frac{\rho_2-(\lambda_1)^2}{[1-(\lambda_1)^2]^{1/2}}\equiv\lambda_2\,,\\ \left(\frac{\mathbf{n}^{(3)}}{(N\psi)^{1/2}},\mathbf{c}^{(2)}\right) &\simeq \left(\frac{\mathbf{n}^{(3)}}{(N\psi)^{1/2}},\frac{\mathbf{n}^{(2)}-\gamma_1\mathbf{n}^{(1)}}{[N\psi(1-(\gamma_1)^2)]^{1/2}}\right)\simeq\frac{\mu_2-(\gamma_1)^2}{[1-(\gamma_1)^2]^{1/2}}\equiv\gamma_2\,.\end{aligned}\tag{247}$$

Then in the Gram–Schmidt orthogonalization we have (cf. (241))

$$\begin{aligned}\mathbf{r}^{(3)} &\simeq \frac{\mathbf{m}^{(3)}-(Nq)^{1/2}(\lambda_1\mathbf{r}^{(1)}+\lambda_2\mathbf{r}^{(2)})}{[Nq(1-(\lambda_1)^2-(\lambda_2)^2)]^{1/2}}\,,\\ \mathbf{c}^{(3)} &\simeq \frac{\mathbf{n}^{(3)}-(N\psi)^{1/2}(\gamma_1\mathbf{c}^{(1)}+\gamma_2\mathbf{c}^{(2)})}{[N\psi((1-(\gamma_1)^2-(\gamma_2)^2)]^{1/2}}\,.\end{aligned}$$

We can express the $\mathbf{m}$, $\mathbf{n}$ vectors in terms of the $\mathbf{r}$, $\mathbf{c}$ vectors as (cf. (43), (44), and (242))

$$\begin{aligned}\frac{\mathbf{m}^{(3)}}{(Nq)^{1/2}} &\simeq \lambda_1\mathbf{r}^{(1)}+\lambda_2\mathbf{r}^{(2)}+\Big(1-(\lambda_1)^2-(\lambda_2)^2\Big)^{1/2}\mathbf{r}^{(3)}\,,\\ \frac{\mathbf{n}^{(3)}}{(N\psi)^{1/2}} &\simeq \gamma_1\mathbf{c}^{(1)}+\gamma_2\mathbf{c}^{(2)}+\Big(1-(\gamma_1)^2-(\gamma_2)^2\Big)^{1/2}\mathbf{c}^{(3)}\,.\end{aligned}\tag{248}$$

### G.4. AMP iterates at $t=4$

At the next step of the AMP iteration we have (cf. (243))

$$\begin{aligned}\mathbf{m}^{(4)} &\equiv t(\mathbf{H}^{(4)}) = t\bigg(\frac{(\boldsymbol{G}^{(3)})^{\mathsf{t}}(\mathbf{n}^{(3)})^{\perp}}{N^{1/2}}+\frac{(\boldsymbol{\Gamma}^{(2)})^{\mathsf{t}}\mathbf{n}^{(3)}}{N^{1/2}}+\frac{(\boldsymbol{\Gamma}^{(1)})^{\mathsf{t}}\mathbf{n}^{(3)}}{N^{1/2}}-\beta\mathbf{m}^{(2)}\bigg)\,,\\ \mathbf{n}^{(4)} &\equiv F(\mathbf{h}^{(4)}) = F\bigg(\frac{\boldsymbol{G}^{(3)}(\mathbf{m}^{(3)})^{\perp}}{N^{1/2}}+\frac{\boldsymbol{\Gamma}^{(2)}\mathbf{m}^{(3)}}{N^{1/2}}+\frac{\boldsymbol{\Gamma}^{(1)}\mathbf{m}^{(3)}}{N^{1/2}}-\beta'\mathbf{n}^{(2)}\bigg)\,.\end{aligned}\tag{249}$$

For the purposes of evaluating $(\boldsymbol{\Gamma}^{(s)})\mathbf{n}^{(3)}$ for $s=1,2$ we calculate

$$\begin{aligned}\left\{\frac{\mathbf{r}\mathbf{r}^{\mathsf{t}}\boldsymbol{G}}{N^{1/2}}\right\}^{(1)}\mathbf{n}^{(3)} &= \frac{\mathbf{r}^{(1)}}{N^{1/2}}(\bar{\mathbf{x}}^{(1)},\mathbf{n}^{(3)})\\ &\simeq \frac{\mathbf{r}^{(1)}}{N^{1/2}}N\alpha\mathbb{E}\bigg[\Big(\lambda_1 Z+\Big(1-(\lambda_1)^2\Big)^{1/2}\xi\Big)F(q^{1/2}Z)\bigg] = (Nq)^{1/2}\beta\lambda_1\mathbf{r}^{(1)}\,,\\ \left\{\frac{\boldsymbol{G}\mathbf{c}\mathbf{c}^{\mathsf{t}}}{N^{1/2}}\right\}^{(1)}\mathbf{n}^{(3)} &= \frac{\bar{\mathbf{y}}^{(1)}}{N^{1/2}}(\mathbf{c}^{(1)},\mathbf{n}^{(3)}) = \psi^{1/2}\gamma_1\bar{\mathbf{y}}^{(1)}\,.\end{aligned}$$

Substituting back into (249) gives (cf. (38), (39), (239), and (244))

$$\begin{aligned}\mathbf{m}^{(4)} &\equiv t(\mathbf{H}^{(4)}) \simeq t\bigg(\psi^{1/2}\Big\{\gamma_1\bar{\mathbf{y}}^{(1)}+\gamma_2\bar{\mathbf{y}}^{(2)}+\Big(1-(\gamma_1)^2-(\gamma_2)^2\Big)^{1/2}\bar{\mathbf{y}}^{(3)}\Big\}\bigg)\,,\\ \mathbf{n}^{(4)} &\equiv F(\mathbf{h}^{(4)}) \simeq F\bigg(q^{1/2}\Big\{\lambda_1\bar{\mathbf{x}}^{(1)}+\lambda_2\bar{\mathbf{x}}^{(2)}+\Big(1-(\lambda_1)^2-(\lambda_2)^2\Big)^{1/2}\bar{\mathbf{x}}^{(3)}\Big\}\bigg)\,.\end{aligned}\tag{250}$$

It follows that (240) continues to hold (approximately) with $\mathbf{m}^{(4)}$, $\mathbf{n}^{(4)}$ in place of $\mathbf{m}^{(2)}$, $\mathbf{n}^{(2)}$. Likewise, (247) continues to approximately hold with $\mathbf{m}^{(4)}$, $\mathbf{n}^{(4)}$ in place of $\mathbf{m}^{(3)}$, $\mathbf{n}^{(3)}$. We also have (cf. (245))

$$\begin{aligned}\frac{(\mathbf{H}^{(3)},\mathbf{H}^{(4)})}{N\psi} &\simeq (\gamma_1)^2+\gamma_2\Big(1-(\gamma_1)^2\Big)^{1/2} \overset{(247)}{=} \mu_2\,,\\ \frac{(\mathbf{h}^{(3)},\mathbf{h}^{(4)})}{Mq} &\simeq (\lambda_1)^2+\lambda_2\Big(1-(\lambda_1)^2\Big)^{1/2} \overset{(247)}{=} \rho_2\,,\end{aligned}$$

from which we obtain (cf. (33) and (246))

$$\frac{(\mathbf{m}^{(4)},\mathbf{m}^{(3)})}{Nq} \simeq \rho(\mu_2)\equiv\rho_3\,,\quad \frac{(\mathbf{n}^{(4)},\mathbf{n}^{(3)})}{N\psi}\simeq\mu(\rho_2)\equiv\mu_3\,. \tag{251}$$

It then follows that (cf. (34) and (247))

$$\begin{aligned}\left(\frac{\mathbf{m}^{(4)}}{(Nq)^{1/2}},\mathbf{r}^{(3)}\right) &\simeq \left(\frac{\mathbf{m}^{(4)}}{(Nq)^{1/2}},\frac{\mathbf{m}^{(3)}/(Nq)^{1/2}-\lambda_1\mathbf{r}^{(1)}-\lambda_2\mathbf{r}^{(2)}}{[1-(\lambda_1)^2-(\lambda_2)^2]^{1/2}}\right)\\ &\simeq \frac{\rho_3-(\lambda_1)^2-(\lambda_2)^2}{[1-(\lambda_1)^2-(\lambda_2)^2]^{1/2}}\equiv\lambda_3\,,\\ \left(\frac{\mathbf{n}^{(4)}}{(N\psi)^{1/2}},\mathbf{c}^{(3)}\right) &\simeq \left(\frac{\mathbf{n}^{(4)}}{(N\psi)^{1/2}},\frac{\mathbf{n}^{(3)}/(N\psi)^{1/2}-\gamma_1\mathbf{c}^{(1)}-\gamma_2\mathbf{c}^{(2)}}{[1-(\gamma_1)^2-(\gamma_2)^2]^{1/2}}\right)\\ &\simeq \frac{\mu_3-(\gamma_1)^2-(\gamma_2)^2}{[1-(\gamma_1)^2-(\gamma_2)^2]^{1/2}}\equiv\gamma_3\,.\end{aligned} \tag{252}$$

In summary, using the notation (35), we have (cf. (38), (39), (239), (244), and (250))

$$\mathbf{m}^{(t+1)}\equiv t(\mathbf{H}^{(t+1)})\simeq t\bigg(\psi^{1/2}\Big\{\gamma_1\bar{\mathbf{y}}^{(1)}+\ldots+\gamma_{t-1}\bar{\mathbf{y}}^{(t-1)}+(1-\Gamma_{t-1})^{1/2}\bar{\mathbf{y}}^{(t)}\Big\}\bigg)\,, \tag{253}$$

$$\mathbf{n}^{(t+1)}\equiv F(\mathbf{h}^{(t+1)})\simeq F\bigg(q^{1/2}\Big\{\lambda_1\bar{\mathbf{x}}^{(1)}+\ldots+\lambda_{t-1}\bar{\mathbf{x}}^{(t-1)}+(1-\Lambda_{t-1})^{1/2}\bar{\mathbf{x}}^{(t)}\Big\}\bigg)\,, \tag{254}$$

where the coefficients are defined recursively: we start with $\lambda_1\equiv\rho_1$ and $\gamma_1\equiv\mu_1$ as in (240) (cf. (32)). For $s\geqslant 1$ we let $\rho_{s+1}\equiv\rho(\mu_s)$ and $\mu_{s+1}\equiv\mu(\rho_s)$ as in (246) and (251) (cf. (33)). Then, as in (247) and (252) (cf. (34)), we can define recursively the constants

$$\lambda_s=\frac{\rho_s-\Lambda_{s-1}}{(1-\Lambda_{s-1})^{1/2}}\,,\quad \gamma_s=\frac{\mu_s-\Gamma_{s-1}}{(1-\Gamma_{s-1})^{1/2}}\,. \tag{255}$$

We use these to define the matrices $\boldsymbol{\Gamma}$ and $\boldsymbol{\Lambda}$ as in (36) and (37). Then (253) and (254) can be rewritten as (38) and (39). The Gram–Schmidt orthogonalization (242) and (248) then correspond (approximately) to (43) and (44).

### G.5. Idealized moment calculation

In this subsection we present a simplified version of the moment calculations that appear in this paper. For expository purposes, we will make several non-rigorous simplifications in what follows, and will be loose in our handling of error terms. The mathematically rigorous moment calculation appears in the proofs in the main body of this paper. By contrast, the purpose of this subsection is to informally highlight some of the basic techniques underlying the proofs.

As at the start of Section A, we consider the perceptron model (1) with an independent copy $\boldsymbol{G}'$ of the disorder matrix $\boldsymbol{G}$. Then, rather than condition on the AMP filtration (16), we pretend that we have access to an exact TAP solution $(\mathbf{m}, \mathbf{n})$ for $\boldsymbol{G}'$:

$$\mathbf{m} \equiv \operatorname{th}(\mathbf{H}) = \operatorname{th}\left(\frac{(\boldsymbol{G}')^{\mathsf{t}}\mathbf{n}}{N^{1/2}} - \beta\mathbf{m}\right), \quad \beta = \alpha\mathbb{E}(F_q)'(q^{1/2}Z) \tag{256}$$

$$\mathbf{n} \equiv F_q(\mathbf{h}) = F_q\left(\frac{\boldsymbol{G}'\mathbf{m}}{N^{1/2}} - \beta'\mathbf{n}\right), \quad \beta' = 1 - q\,, \tag{257}$$

(i.e., the equations (10) and (11) with $\boldsymbol{G}'$ in place of $\boldsymbol{G}$). We assume that $\mathbf{H}/\psi^{1/2}$ and $\mathbf{h}/q^{1/2}$ behave like standard gaussian vectors, in the sense of Lemma A.4. Let

$$S_* \equiv \left\{ J \in \{-1,+1\}^N : J - \mathbf{m} \perp \operatorname{span}\{\mathbf{m}, \mathbf{H}\} \right\},$$

where $\perp$ indicates approximate orthogonality. This is a simplification of the condition (19), which is formalized by (142). We shall estimate the contribution to (1) only from configurations in $S_*$,

$$\boldsymbol{Z}_* \equiv \sum_{J \in S_*} \prod_{a \leqslant M} U\left(\frac{(\mathbf{e}_a)^{\mathsf{t}}\boldsymbol{G}'J}{N^{1/2}}\right).$$

The quantity $\boldsymbol{Z}_*$ above is an informal version of (143), and is moreover essentially similar to the quantity $\bar{\boldsymbol{Z}}$ appearing in Theorem 1.5 (cf. (144)).

We will assume for simplicity that $U$ is $\{0,1\}$-valued, and let $\mathrm{S}_J$ refer to the event that $J$ gives a positive contribution to the sum $\boldsymbol{Z}_*$ above. Recall that $\boldsymbol{G}$ is an independent copy of $\boldsymbol{G}'$, and define the events (cf. (60) and (61))

$$\mathrm{R} \equiv \left\{ \frac{\boldsymbol{G}\mathbf{m}}{N^{1/2}} = \mathbf{h} + \beta'\mathbf{n} \right\} \tag{258}$$

$$\mathrm{C} \equiv \left\{ \frac{\boldsymbol{G}^{\mathsf{t}}\mathbf{n}}{N^{1/2}} = \mathbf{H} + \beta\mathbf{m} \right\} \tag{259}$$

We next pretend that $\boldsymbol{G}'$ is gaussian given the TAP equations (256) and (257) — that is to say, the probability of $\mathrm{S}_J(\boldsymbol{G}')$ given the TAP solution is the same as $\mathbb{P}(\mathrm{S}_J(\boldsymbol{G}) \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R}, \mathrm{C})$. In the proofs, this heuristic is formalized by Lemma A.16.

We will estimate $\mathbb{P}(\mathrm{S}_J(\boldsymbol{G}) \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R}, \mathrm{C})$ for $J \in S_*$. Note that for such $J$ we can decompose

$$\frac{J}{N^{1/2}} = \frac{\mathbf{m}}{N^{1/2}} + \frac{J - \mathbf{m}}{N^{1/2}} = \frac{\mathbf{m}}{N^{1/2}} + (1-q)^{1/2}\mathbf{v}\,, \tag{260}$$

where $\mathbf{v}$ is a unit vector orthogonal to $\operatorname{span}\{\mathbf{m}, \mathbf{H}\}$. Now note that the event C of (259) implies

$$\mathrm{A} = \left\{ \frac{\mathbf{n}^{\mathsf{t}}\boldsymbol{G}\mathbf{v}}{N} = \frac{(\mathbf{H} + \beta\mathbf{m}, \mathbf{v})}{N^{1/2}} = 0 \right\}, \tag{261}$$

where the middle equality is by (259), and the last equality is by the restriction $J \in S_*$. It follows by orthogonality considerations (formalized by Lemma A.19) and Bayes's rule that

$$\mathbb{P}(\mathrm{S}_J(\boldsymbol{G}) \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R}, \mathrm{C}) = \mathbb{P}(\mathrm{S}_J(\boldsymbol{G}) \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R}, \mathrm{A})\,.$$

Applying Bayes's rule gives

$$\mathbb{P}(\mathrm{S}_J(\boldsymbol{G}) \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R}, \mathrm{A}) = \frac{\tilde{\mathbb{P}}(\mathrm{S}_J(\boldsymbol{G}) \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R})\tilde{\mathbb{P}}(\mathrm{A} \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R}, \mathrm{S}_J(\boldsymbol{G}))}{\tilde{\mathbb{P}}(\mathrm{A} \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R})}\,, \tag{262}$$

where $\tilde{\mathbb{P}}$ denotes the tilted gaussian measure (cf. (69))

$$\frac{d\tilde{\mathbb{P}}}{d\mathbb{P}} = \exp\left\{\tau(\boldsymbol{G}, \mathbf{n}\mathbf{v}^{\mathrm{t}}) - \frac{\tau^2\|\mathbf{n}\|^2}{2}\right\}.$$

The identity (262) holds for any $\tau \in \mathbb{R}$. We next explain how to choose $\tau$ to facilitate the computation of the factors appearing on the right-hand side of (262). Note that we have been informal in conditioning on events of zero probability; in the main text of the paper this is formalized by dealing with densities rather than probabilities.

We first consider the factor $\tilde{\mathbb{P}}(\mathrm{S}_J(\boldsymbol{G}) \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R})$ appearing in the numerator on the right-hand side of (262). On the event R of (258), it follows using the decomposition (260) that

$$\frac{\boldsymbol{G}J}{N^{1/2}} = \frac{\boldsymbol{G}\mathbf{m}}{N^{1/2}} + \frac{\boldsymbol{G}(J - \mathbf{m})}{N^{1/2}} = \mathbf{h} + \beta'\mathbf{n} + (1-q)^{1/2}\boldsymbol{G}\mathbf{v}\,.$$

Under the tilted measure $\tilde{\mathbb{P}}(\cdot \,|\, \mathrm{R})$, the difference $\boldsymbol{G} - \tau\mathbf{n}\mathbf{v}^{\mathrm{t}}$ has the law of an $M \times N$ matrix with i.i.d. standard gaussian entries, so we have

$$\tilde{\mathbb{P}}(\mathrm{S}_J(\boldsymbol{G}) \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R}) = \prod_{a \leqslant M} \mathbb{E}_\xi U\bigg((\mathbf{e}_a)^{\mathrm{t}}\Big(\mathbf{h} + (\beta' + (1-q)^{1/2}\tau)\mathbf{n} + (1-q)^{1/2}\xi\Big)\bigg).$$

To simplify the above, it is natural to choose $\tau = -\beta/(1-q)^{1/2} = -(1-q)^{1/2}$. This results in

$$\tilde{\mathbb{P}}(\mathrm{S}_J(\boldsymbol{G}) \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R}) \doteq \exp\left\{N\alpha\mathbb{E}L_q(q^{1/2}Z)\right\}$$

for $L_q$ as defined by (26), and $Z$ a standard gaussian.

The denominator on the right-hand side of (262) is easy to estimate for any $\tau$: it is the probability that (261) holds, where again we note that $\boldsymbol{G} - \tau\mathbf{n}\mathbf{v}^{\mathrm{t}}$ has the law of an $M \times N$ matrix with i.i.d. standard gaussian entries. It follows that

$$\frac{1}{\tilde{\mathbb{P}}(\mathrm{A} \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R})} \doteq \exp\left\{\frac{\tau^2\|n\|^2}{2}\right\} \doteq \exp\left\{\frac{N\psi(1-q)}{2}\right\},$$

where the last equality is for our particular choice $\tau = -(1-q)^{1/2}$.

It remains to consider the other factor $\tilde{\mathbb{P}}(\mathrm{A} \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R}, \mathrm{S}_J(\boldsymbol{G}))$ in the numerator on the right-hand side of (262), and we claim this is $\doteq 1$: indeed,

$$\begin{aligned}\tilde{\mathbb{E}}\bigg(\frac{\mathbf{n}^{\mathrm{t}}\boldsymbol{G}\mathbf{v}}{N}\,\bigg|\,\mathbf{m}, \mathbf{n}, \mathrm{R}, \mathrm{S}_J\bigg) &= \frac{(\tau\mathbf{n}\mathbf{v}^{\mathrm{t}}, \mathbf{n}\mathbf{v}^{\mathrm{t}})}{N} + \frac{1}{N}\bigg(\mathbf{n}, \frac{\mathbb{E}_\xi[\xi U(\mathbf{h} + (1-q)^{1/2}\xi)]}{\mathbb{E}_\xi U(\mathbf{h} + (1-q)^{1/2}\xi)}\bigg) \\ &= \frac{\tau\|\mathbf{n}\|^2}{N} + \frac{(\mathbf{n}, (1-q)^{1/2}F(\mathbf{h}))}{N} = 0\,,\end{aligned}$$

so $\tilde{\mathbb{P}}(\mathrm{A} \,|\, \mathbf{m}, \mathbf{n}, \mathrm{S}_J(\boldsymbol{G}), \mathrm{R}) \doteq 1$ by (local) central limit theorem considerations. This is formalized by the local CLT estimates of Section E.

Substituting the above calculations into (262) gives, for any $J \in S_*$,

$$\mathbb{P}(\mathrm{S}_J(\boldsymbol{G}) \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R}, \mathrm{A}) \doteq \exp\left\{N\left[\frac{\psi(1-q)}{2} + \alpha\mathbb{E}L_q(q^{1/2}Z)\right]\right\}. \tag{263}$$

It remains to estimate the size of $S_*$. To this end, we can let $\mathbf{P}$ be the uniform measure on $\{-1,+1\}^N$, and consider the change of measure

$$\frac{d\mathbf{Q}}{d\mathbf{P}} = \frac{\exp\{(\mathbf{H}, J)\}}{\exp\{(\log\mathrm{ch}(\mathbf{H}), 1)\}}\,.$$

The mean of the measure $\mathbf{Q}$ is exactly $\mathbf{m}$, so $S_*$ has large probability under $\mathbf{Q}$. It follows that

$$\frac{|S_*|}{2^N} = \mathbf{P}(S_*) = \mathbb{E}_{\mathbf{Q}}\left[\mathbf{1}\{S_*\}\frac{d\mathbf{Q}}{d\mathbf{P}}\right] \doteq \frac{\exp\{(\mathbf{H}, \mathbf{m})\}}{\exp\{(\log\mathrm{ch}(\mathbf{H}), 1)\}}\,.$$

We then apply Stein's identity and the fixed point equation (9) to estimate

$$\frac{(\mathbf{H}, \mathbf{m})}{N} \doteq \mathbb{E}[\psi^{1/2}Z\,\mathrm{th}(\psi^{1/2}Z)] = \psi\mathbb{E}\,\mathrm{th}'(\psi^{1/2}Z) = \psi\mathbb{E}\Big[1 - \mathrm{th}(\psi^{1/2}Z)^2\Big] = \psi(1-q)\,.$$

Rearranging the above calculations leads to

$$|S_*| \doteq \exp\left\{N\left[\mathbb{E}\log\left(2\,\mathrm{ch}(q^{1/2}Z)\right) - \psi(1-q)\right]\right\}. \tag{264}$$

Combining (263) and (264) gives

$$\frac{1}{N}\log\mathbb{E}(\boldsymbol{Z}_*(\boldsymbol{G}) \,|\, \mathbf{m}, \mathbf{n}, \mathrm{R}, \mathrm{C}) \doteq \mathrm{RS}(\alpha; U)$$

for $\mathrm{RS}(\alpha; U)$ as in (29).

The above is a simplified presentation of the first moment calculation appearing in Section C. The two main simplifications were (i) the assumption that the disorder is gaussian conditional on an exact TAP solution satisfying (256) and (256); and (ii) the restriction to configurations $J \in S_*$. The above calculation then shows that the conditional expectation of the partition function restricted to $S_*$ matches the replica symmetric formula. In Section C we remove these simplifications by computing the first moment of the unrestricted partition function (1) conditional on the AMP filtration. We show the main contribution to the conditional first moment comes from configurations $J$ which approximately satisfy (19) (which is similar to the $S_*$ restriction). This already implies that the asymptotic free energy is upper bounded by the replica symmetric value. For the lower bound, we may restrict the partition function in any way that is convenient to the calculation, and in Section D we compute the second moment of the partition function restricted to (19) (and with a further technical restriction; see (144)).