Decoding from Pooled Data: Phase Transitions of Message Passing

Ahmed El Alaoui, Aaditya Ramdas, Florent Krzakala, Lenka Zdeborova, Michael I. Jordan

Decoding from Pooled Data: Phase Transitions of Message Passing

Ahmed El Alaoui* Aaditya Ramdas*† Florent Krzakala‡ Lenka Zdeborová§ Michael I. Jordan*†

Abstract

We consider the problem of decoding a discrete signal of categorical variables from the observation of several histograms of pooled subsets of it. We present an Approximate Message Passing (AMP) algorithm for recovering the signal in the *random dense* setting where each observed histogram involves a random subset of entries of size proportional to n. We characterize the performance of the algorithm in the asymptotic regime where the number of observations m tends to infinity proportionally to n, by deriving the corresponding State Evolution (SE) equations and studying their dynamics. We initiate the analysis of the multi-dimensional SE dynamics by proving their convergence to a fixed point, along with some further properties of the iterates. The analysis reveals sharp phase transition phenomena where the behavior of AMP changes from exact recovery to weak correlation with the signal as m/n crosses a threshold. We derive formulae for the threshold in some special cases and show that they accurately match experimental behavior.

1 Introduction

Consider a discrete high-dimensional signal consisting of categorical variables, for example, nucleotides in a string of DNA or country of origin for a set of people. In many real-world settings, it is infeasible to observe the entire high-dimensional signal, for reasons of cost or privacy. Instead, in a manner akin to compressed sensing, observations can be obtained in the form of "histograms" or "frequency spectra"—pooled measurements counting the occurence of each category or type across subsets of the variables. Concretely, we investigate the so-called *Histogram Query Problem* (HQP): a database consisting of a population of n individuals, where each individual belongs to one category among d, is queried. In each query, a subset of individuals is selected, and the histogram of their types, along with the individuals in that subset are revealed. Such a data acquisition model is common in applications such as the processing of genetic data, where DNA samples from multiple sources are pooled and analyzed together [SBC$^+$02]. This gives rise to the inferential problem of determining the category of every individual in the population. The question of interest in this paper is to determine the minimal number of observations needed for recovery, and to ascertain whether this inferential problem can be solved in an efficient manner.

*Department of Electrical Engineering and Computer Sciences, UC Berkeley, CA.

†Department of Statistics, UC Berkeley, CA.

‡Laboratoire de Physique Statistique, CNRS, PSL Universités & Ecole Normale Supérieure, Sorbonne Universités et Université Pierre & Marie Curie, Paris, France.

§Institut de Physique Théorique, CNRS, CEA, Université Paris-Saclay, Gif-sur-Yvette, France.

1.1 The setting

Let $\tau^* : \{1, \cdots, n\} \mapsto \{1, \cdots, d\}$ be an assignment of n variables to d categories. We denote the queried subpopulations by $S_a \subset \{1, \cdots, n\}$, $1 \le a \le m$. Given m subsets S_a, the histogram of categories of the pooled subpopulation S_a is denoted by $\boldsymbol{h}_a \in \mathbb{Z}_+^d$, i.e., for all $1 \le a \le m$,

$$\boldsymbol{h}_a := \left(\left|\tau^{*-1}(1) \cap S_a\right|, \cdots, \left|\tau^{*-1}(d) \cap S_a\right|\right). \tag{1}$$

We let $\boldsymbol{\pi} = \frac{1}{n}\left(\left|\tau^{*-1}(1)\right|, \cdots, \left|\tau^{*-1}(d)\right|\right)$ denote the vector of proportions of assigned values; i.e., the empirical distribution of categories. We place ourselves in a random dense regime in which the sets $\{S_a\}_{1 \le a \le m}$ are independent draws of a random set S where $\Pr(i \in S) = \alpha$ independently for each $i \in \{1, \ldots, n\}$, for some fixed $\alpha \in (0, 1)$. Meaning, at each query, the size of the pool is proportional to the size of the population: $\mathbb{E}[|S|] = \alpha n$.

Here we adopt a linear-algebraic formulation which will be more convenient for the presentation of the algorithm. We can represent the map τ^*, which we refer to as *the planted solution*, as a set of vectors $\boldsymbol{x}_i^* = \boldsymbol{e}_{\tau^*(i)} \in \mathbb{R}^d$, for $1 \le i \le n$. Let $\boldsymbol{A} \in \mathbb{R}^{m \times n}$ represent the sensing matrix: $A_{ai} = \mathbb{1}\{i \in S_a\}$, for all $1 \le i \le n, 1 \le a \le m$. The histogram equations (1) can be written in the form of a linear system of m equations:

$$\boldsymbol{h}_a = \sum_{i=1}^{n} A_{ai} \boldsymbol{x}_i^*, \qquad a \in \{1, \cdots, m\}. \tag{2}$$

Our goal can thus be rephrased as that of inverting the linear system (2). Note that the problem becomes trivial if $m = n$, since the square random matrix $\boldsymbol{A}$ will be invertible with high probability. However, as we review in the next section, a detailed information-theoretic analysis of the problem shows that the planted solution is uniquely determined by the above linear system for $m = \gamma \frac{n}{\log n}$, $\gamma > 0$. In this paper we study the algorithmic problem in the regime $m = \kappa n$, $\kappa < 1$.

1.2 Prior work

The HQP has recently been considered in [WHLC16, ERK$^+$16]. Its study was initiated in [WHLC16] in the two settings where the sets $\{S_a\}$ are deterministic and random. We review the information-theoretic and algorithmic results known so far.

Information-theoretic aspect Under the condition that $\boldsymbol{\pi}$ is the uniform distribution, Wang *et al.* [WHLC16] showed a lower bound on the minimum number of queries m for the problem to be well-posed, namely, if $m < \frac{\log d}{d-1} \frac{n}{\log n}$ then the set of collected histograms does not uniquely determine the planted solution τ^*. Further, under the condition that $\alpha = \frac{1}{2}$, they showed that $m > c_0 \frac{n}{\log n}$ with c_0 a constant independent of d, suffices to uniquely determine τ^*. These results were later generalized and sharpened in [ERK$^+$16], where it was shown that for arbitrary $\boldsymbol{\pi}$ and α, $m \in (\gamma_{\text{low}} \frac{n}{\log n}, \gamma_{\text{up}} \frac{n}{\log n})$ measurements are necessary and sufficient for τ^* to be unique, where $\gamma_{\text{low}} = \frac{H(\boldsymbol{\pi})}{d-1}$, and γ_{up} is "essentially" $2\gamma_{\text{low}}$ (see [ERK$^+$16] for the precise formula), H being the Shannon entropy function.

Algorithmic aspect In the deterministic setting, where one is allowed to design the sensing matrix $\boldsymbol{A}$, i.e. choose the pools S_a at each query, Wang *et al.* [WHLC16] provided a querying strategy that recovers τ^* provided that $m > c_1 \frac{n}{\log n}$, where c_1 is an absolute constant. Ignoring

the dependence on d, this almost matches the information-theoretic limit. The random setting has not been treated so far, and is the subject of the present paper.

1.3 Contributions

We present an Approximate Message Passing (AMP) algorithm for the *random dense* setting, where each query involves a random subset of individuals of size proportional to n. We characterize the exact asymptotic behavior of the algorithm in the limit of large number of individuals n and a proportionally large number of queries m, i.e. $m/n \to \kappa$. This is done by heuristically deriving the corresponding State Evolution (SE) equations corresponding to the AMP algorithm. Then, a rigorous analysis of the SE dynamics reveals a rich and interesting behavior; namely the existence of phase transition phenomena in the parameters $\kappa, d, \boldsymbol{\pi}$ of the problem, due to which the behavior of AMP changes radically, from exact recovery to very weak correlation with the planted solution. We exactly locate these phase transitions in simple situations, such as the binary case $d = 2$, the symmetric case $\boldsymbol{\pi} = (\frac{1}{d}, \cdots, \frac{1}{d})$, and the general case under the condition that the SE iteration is initialized from a special point. The latter exhibits an intriguing phenomenon: the existence of not one, but an entire sequence of thresholds in the parameter κ that rules the behavior of the SE dynamics. These thresholds correspond to sharp changes in the structure of the covariance matrix of the estimates output by AMP. We expect this phenomenon to be generic beyond the special initialization case studied here. Beyond the precise characterization of the phase transition thresholds in these special cases, we initiate the study of State Evolution in a multivariate setting by proving the convergence of the full-dimensional SE iteration, when initialized from a "far enough" point, to a fixed point, and show further properties of the iterate sequence. This paper is intended to be a sequel to the information-theoretic study conducted in [ERK+16].

2 Approximate Message Passing and State Evolution

In this section we present the Approximate Message Passing (AMP) algorithm and the corresponding State Evolution (SE) equations.

2.1 The AMP algorithm

The AMP algorithm [DMM09], known as the Thouless-Anderson-Palmer equations in the statistical physics literature [TAP77], can be derived from Belief Propagation (BP) on the factor graph modeling the recovery problem. The latter is a bipartite graph of $n+m$ vertices. The variables $\{\boldsymbol{x}_i : 1 \le i \le n\}$ constitute one side of the bipartition, and the observations $\{\boldsymbol{h}_a : 1 \le a \le m\}$ constitute the other side. The adjacency structure is encoded in the sensing matrix $\boldsymbol{A}$. Endowing each edge (i, a) with two messages $\boldsymbol{m}_{i\to a}, \boldsymbol{m}_{a\to i} \in \Delta^{d-1}$, Δ^{d-1} being the probability simplex, one can write the self-consistency equations for the messages at each node by enforcing the histogram constraints at each observation (or check) node while treating the incoming messages as probabilistically independent in the marginalization operation. The iterative version of these self-consistency equations is the BP algorithm. BP is further simplified to AMP by exploiting the fact that the factor graph is random and dense, i.e. one only needs to track the average of the messages incoming to each node. This reduces the number of passed messages from $m \times n$ to $m + n$. For the present d-variate problem, the algorithm we present is a special case of Hybrid-GAMP of [RFGS12]. We let $\bar{\boldsymbol{h}}_a = (\boldsymbol{h}_a - \alpha n \boldsymbol{\pi})/\sqrt{n}$ and $\overline{\boldsymbol{A}} = (\boldsymbol{A} - \alpha \mathbf{1}_m \mathbf{1}_n^\top)/\sqrt{n}$ be the centered and rescaled data, and

assume that the parameters α and $\boldsymbol{\pi}$ are known to the algorithm. The AMP algorithm reads as follows: At iteration $t = 1, 2, \ldots$, we update the check nodes $a = 1, \cdots, m$ as

$$\begin{aligned}\boldsymbol{\omega}_a^t &= \sum_{j \in \partial a} \bar{A}_{aj} \hat{\boldsymbol{x}}_j^t - \boldsymbol{V}_a^t \left(\boldsymbol{V}_a^{t-1}\right)^{-1} (\bar{\boldsymbol{h}}_a - \boldsymbol{\omega}_a^{t-1}),\\ \boldsymbol{V}_a^t &= \sum_{j \in \partial a} \bar{A}_{aj}^2 \boldsymbol{B}_j^t,\end{aligned}$$

and then update the variable nodes $i = 1, \cdots, n$ as

$$\begin{aligned}\boldsymbol{z}_i^t &= \hat{\boldsymbol{x}}_i^t + \boldsymbol{\Sigma}_i^t \cdot \sum_{b \in \partial i} \bar{A}_{bi} \left(\boldsymbol{V}_b^t\right)^{-1} (\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_b^t),\\ \boldsymbol{\Sigma}_i^t &= \left(\sum_{b \in \partial i} \bar{A}_{bi}^2 \left(\boldsymbol{V}_b^t\right)^{-1}\right)^{-1},\\ \hat{\boldsymbol{x}}_i^{t+1} &= \boldsymbol{\eta}(\boldsymbol{z}_i^t, \boldsymbol{\Sigma}_i^t),\\ \boldsymbol{B}_i^{t+1} &= \mathrm{Diag}(\hat{\boldsymbol{x}}_i^{t+1}) - \hat{\boldsymbol{x}}_i^{t+1} \cdot \hat{\boldsymbol{x}}_i^{t+1\top},\end{aligned}$$

with

$$\boldsymbol{\eta}(\boldsymbol{z}, \boldsymbol{\Sigma}) := \sum_{r=1}^{d} \pi_r \boldsymbol{e}_r \frac{e^{-\frac{1}{2}(\boldsymbol{z}-\boldsymbol{e}_r)^\top \boldsymbol{\Sigma}^{-1}(\boldsymbol{z}-\boldsymbol{e}_r)}}{Z(\boldsymbol{z}, \boldsymbol{\Sigma})} \in \mathbb{R}^d, \tag{3}$$

where $Z(\boldsymbol{z}, \boldsymbol{\Sigma}) = \sum_{r=1}^{d} \pi_r e^{-\frac{1}{2}(\boldsymbol{z}-\boldsymbol{e}_r)^\top \boldsymbol{\Sigma}^{-1}(\boldsymbol{z}-\boldsymbol{e}_r)}$ is a normalization factor so that the entries of $\boldsymbol{\eta}$ sum to one. The map $\boldsymbol{\eta}$ plays the role of a "thresholding function" with a matrix parameter $\boldsymbol{\Sigma}$ that is adaptively tuned by the algorithm. One should compare this situation to the case of sparse estimation [DMM09] where the soft thresholding function is used. Here, the form taken by $\boldsymbol{\eta}$ is adapted to the structure of the signal we seek to recover. The variables $\boldsymbol{\omega}_a$ and $\boldsymbol{V}_a$ represent estimates of the histogram $\boldsymbol{h}_a$ and their variances. The variables $\boldsymbol{z}_i$ and $\boldsymbol{\Sigma}_i$ are estimators of the planted solution $\boldsymbol{x}_i^*$ and their variances before thresholding, while $\hat{\boldsymbol{x}}_i \in \Delta^{d-1}$ and $\boldsymbol{B}_i$ are the posterior estimates of $\boldsymbol{x}_i^*$ and its variance, i.e., after thresholding. The algorithm can be initialized in a "non-informative" way by setting $\hat{\boldsymbol{x}}_i^0 = \boldsymbol{\pi}, \boldsymbol{B}_i^0 = \mathrm{Diag}(\boldsymbol{\pi}) - \boldsymbol{\pi}\boldsymbol{\pi}^\top$ for all $i = 1, \ldots, n$, and $\boldsymbol{\omega}_a^{-1} = \boldsymbol{0}$ and $\boldsymbol{V}_a^{-1} = \boldsymbol{I}$ for all $a = 1, \cdots, m$ for example. We defer the details of the derivation to Appendix B.

2.2 State Evolution

State Evolution (SE) [DMM09, BLM12], known as the cavity method in statistical physics [MPV90], allows us to exactly characterize the asymptotic behavior of AMP at each time step t, by tracking the evolution in time of the relevant *order parameters* of the algorithm. More precisely, let

$$\boldsymbol{M}_{t,n} := \frac{1}{n} \sum_{i=1}^{n} \hat{\boldsymbol{x}}_i^t \boldsymbol{x}_i^{*\top}, \quad \text{and} \quad \boldsymbol{Q}_{t,n} := \frac{1}{n} \sum_{i=1}^{n} \hat{\boldsymbol{x}}_i^t \hat{\boldsymbol{x}}_i^{t\top}.$$

The matrix $\boldsymbol{M}_{t,n}$ tracks the average alignment of the estimates with the true solution, and $\boldsymbol{Q}_{t,n}$ their average covariance structure. The SE equations relate the values of these order parameters at $t+1$ to those at time t in the limit $n \to \infty$, $m/n \to \kappa$. We let $\boldsymbol{M}_t$ and

$\boldsymbol{Q}_t$ denote the respective limits of $\boldsymbol{M}_{t,n}$ and $\boldsymbol{Q}_{t,n}$, which we assume exist in this "replica-symmetric" regime, and let $\boldsymbol{D} = \mathrm{Diag}(\boldsymbol{\pi})$. The SE equations read

$$\begin{aligned}
\boldsymbol{M}_{t+1} &= \sum_{r=1}^{d} \pi_r \, \mathbb{E}_{\boldsymbol{g}} \left[\boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}_t^{\frac{1}{2}} \boldsymbol{g}, \kappa^{-1} \boldsymbol{R}_t) \right] \cdot \boldsymbol{e}_r^\top , \\
\boldsymbol{Q}_{t+1} &= \sum_{r=1}^{d} \pi_r \, \mathbb{E}_{\boldsymbol{g}} \left[\boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}_t^{\frac{1}{2}} \boldsymbol{g}, \kappa^{-1} \boldsymbol{R}_t) \cdot \boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}_t^{\frac{1}{2}} \boldsymbol{g}, \kappa^{-1} \boldsymbol{R}_t)^\top \right], \\
\boldsymbol{X}_t &= \kappa^{-1} (\boldsymbol{D} - \boldsymbol{M}_t - \boldsymbol{M}_t^\top + \boldsymbol{Q}_t), \\
\boldsymbol{R}_t &= \mathrm{Diag}(\boldsymbol{Q}_t \mathbf{1}) - \boldsymbol{Q}_t,
\end{aligned}$$

with $\boldsymbol{g} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{I})$. The matrix $\kappa \boldsymbol{X}_t$ is the covariance matrix of the error of the estimates output by AMP at time t, and $\boldsymbol{R}_t$ can be interpreted as the average covariance matrix of the estimates themselves. Note that the parameter α has disappeared from the characterization by the SE equations, just as in the information theoretic study [ERK+16].

The full derivation of these equations is relegated to Appendix C. The main hypothesis behind the derivation, which we *do not* rigorously verify, is that the variables $\boldsymbol{z}_i^t$ are asymptotically Gaussian, centered about $\boldsymbol{x}_i^*$ and with covariance $\boldsymbol{X}_t$: the measure $\frac{1}{n} \sum_{i=1}^n \delta_{\boldsymbol{z}_i^t - \boldsymbol{x}_i^*}$ converges weakly to $\mathcal{N}(\mathbf{0}, \boldsymbol{X}_t)$. We refer to [BM11, BLM12] for rigorous results, the assumptions of which do not apply to this setting. It is an interesting problem to prove the exactness of the SE equations in this setting.

2.3 Simplification of SE

Here we simplify the system of SE equations above to a single iteration. This crucially relies on the following Proposition:

Proposition 1. *If $\boldsymbol{M}_0 = \boldsymbol{Q}_0$, then for all t we have*

(i) $\boldsymbol{M}_t = \boldsymbol{Q}_t$. In particular, $\boldsymbol{M}_t$ is a symmetric PSD matrix, and $\boldsymbol{M}_t \mathbf{1} = \boldsymbol{\pi}$.

(ii) $\boldsymbol{R}_t = \kappa \boldsymbol{X}_t = \boldsymbol{D} - \boldsymbol{M}_t$.

The proof of the above proposition is deferred to Appendix A. We pause to make a few remarks. The assumption of the Proposition could be enforced for example by setting the initial estimates of AMP as $\hat{\boldsymbol{x}}_i^0 = \boldsymbol{\pi}$ for all i. This yields $\boldsymbol{M}_0 = \boldsymbol{Q}_0 = \boldsymbol{\pi}\boldsymbol{\pi}^\top$, and hence $\boldsymbol{X}_0 = \kappa^{-1}(\boldsymbol{D} - \boldsymbol{\pi}\boldsymbol{\pi}^\top)$. The statements in the Proposition —together referred to as the *Nishimori identities* in the statistical physics literature [ZK16]— simplify the SE equations to a single iteration on $\boldsymbol{X}_t$. To succinctly present this simplification, for $r \in \{1, \cdots, d\}$, and $\boldsymbol{X} \succeq \mathbf{0}$, we let

$$\boldsymbol{\eta}_r(\boldsymbol{X}) := \boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}^{\frac{1}{2}} \boldsymbol{g}, \boldsymbol{X}) \in \Delta^{d-1}.$$

Then, the SE equations can be seen to boil down to the single equation

$$\boldsymbol{X}_{t+1} = \kappa^{-1} f(\boldsymbol{X}_t), \tag{4}$$

where, recalling that $\boldsymbol{g} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{I})$, we define

$$f(\boldsymbol{X}) := \boldsymbol{D} - \sum_{r=1}^{d} \pi_r \, \mathbb{E}_{\boldsymbol{g}} \left[\boldsymbol{\eta}_r(\boldsymbol{X}) \boldsymbol{\eta}_r(\boldsymbol{X})^\top \right] \tag{5}$$

$$= \boldsymbol{D} - \sum_{r=1}^{d} \pi_r \, \mathbb{E}_{\boldsymbol{g}} \left[\boldsymbol{\eta}_r(\boldsymbol{X}) \right] \cdot \boldsymbol{e}_r^\top, \tag{6}$$

$$= \sum_{r=1}^{d} \pi_r \, \mathbb{E}_{\boldsymbol{g}} \left[(\boldsymbol{e}_r - \boldsymbol{\eta}_r(\boldsymbol{X})) \cdot (\boldsymbol{e}_r - \boldsymbol{\eta}_r(\boldsymbol{X}))^\top \right], \tag{7}$$

where equations (5) and (6) correspond to substituting the value of $\boldsymbol{Q}_t$ and $\boldsymbol{M}_t$ into statement (ii) of the above proposition, while the last equality (7) is just a consequence of the first two, (5) and (6). Furthermore, via elementary algebra, the coordinates of the vector $\boldsymbol{\eta}_r(\boldsymbol{X})$ can written as

$$\left(\boldsymbol{\eta}_r(\boldsymbol{X})\right)_s = \frac{\pi_s \exp\left(-\boldsymbol{g}^\top \boldsymbol{X}^{-\frac{1}{2}} (\boldsymbol{e}_r - \boldsymbol{e}_s) - \frac{1}{2} \left\| \boldsymbol{X}^{-\frac{1}{2}} (\boldsymbol{e}_r - \boldsymbol{e}_s) \right\|_{\ell_2}^2 \right)}{Z_r(\boldsymbol{X})}, \tag{8}$$

with

$$Z_r(\boldsymbol{X}) := \sum_{s=1}^{d} \pi_s \exp\left(-\boldsymbol{g}^\top \boldsymbol{X}^{-\frac{1}{2}} (\boldsymbol{e}_r - \boldsymbol{e}_s) - \frac{1}{2} \left\| \boldsymbol{X}^{-\frac{1}{2}} (\boldsymbol{e}_r - \boldsymbol{e}_s) \right\|_{\ell_2}^2 \right).$$

2.4 The mean squared & 0-1 errors

We can measure the performance of AMP by the mean squared error of the estimates $\{\hat{\boldsymbol{x}}_i^t\}_{i=1}^n$:

$$\mathsf{MSE}_{t,n} = \frac{1}{n} \sum_{i=1}^{n} \left\| \hat{\boldsymbol{x}}_i^t - \boldsymbol{x}_i^* \right\|_{\ell_2}^2.$$

Since $\hat{\boldsymbol{x}}_i^t \in \Delta^{d-1}$, an alternative measure of performance would be the expected 0-1 distance between a random category drawn from the multinomial $\hat{\boldsymbol{x}}_i$ and the true category $\boldsymbol{x}_i^*$, then averaged over $i = 1, \cdots, n$. This error would be written as

$$\begin{aligned} \frac{1}{n} \sum_{i=1}^{n} \sum_{r=1}^{d} \hat{x}_{ir}^t (1 - \boldsymbol{e}_r^\top \boldsymbol{x}_i^*) &= 1 - \frac{1}{n} \sum_{i=1}^{n} \hat{\boldsymbol{x}}_i^{t\top} \boldsymbol{x}_i^* \\ &= 1 - \operatorname{trace}(\boldsymbol{M}_{t,n}) = \operatorname{trace}\left(\boldsymbol{D} - \boldsymbol{M}_{t,n}\right). \end{aligned}$$

On the other hand, the MSE in the large n limit reads

$$\begin{aligned} \mathsf{MSE}_t := \lim_{n \to \infty} \mathsf{MSE}_{t,n} &= \operatorname{trace}\left(\boldsymbol{Q}_t - \boldsymbol{M}_t - \boldsymbol{M}_t^\top + \boldsymbol{D} \right), \\ &= \operatorname{trace}\left(\boldsymbol{D} - \boldsymbol{M}_t \right), \end{aligned}$$

so the two notions of error coincide in the limit. Note that the MSE at each step t can be deduced from SE iterate at time t: $\mathsf{MSE}_t = \kappa \operatorname{trace}(\boldsymbol{X}_t)$.

3 Analysis of the State Evolution dynamics

In this section we present our main results on the convergence of the SE iteration (4) to a fixed point, and the location of the phase transition thresholds in three special cases. We start by analyzing the SE map f and present some important generic results.

3.1 Analysis of the SE map f

From expression (7), we see that the map f sends the positive semi-definite (PSD) cone $\mathbb{S}_+^{d\times d}$ to itself. As written, f is only defined for invertible matrices $\boldsymbol{X}$, but it could be extended by continuity to singular matrices: if $\boldsymbol{e}_r - \boldsymbol{e}_s$ is in the null space of $\boldsymbol{X}$, we declare that $\exp(-\frac{1}{2}\|\boldsymbol{X}^{-\frac{1}{2}}(\boldsymbol{e}_r - \boldsymbol{e}_s)\|^2) = 0$. This convention is consistent with the limiting value of a sequence $\left\{ \exp(-\frac{1}{2}\|\boldsymbol{X}_n^{-\frac{1}{2}}(\boldsymbol{e}_r - \boldsymbol{e}_s)\|^2)\right\}_{n\geq 0}$ where $\left\{\boldsymbol{X}_n\right\}_{n\geq 0}$ is a sequence of invertible matrices approaching $\boldsymbol{X}$. This also has an interpretation based on an analogy with electrical circuits, which we discuss shortly. This extension will be also denoted by f. It is continuous over the $\mathbb{S}_+^{d\times d}$, and we have $f(\boldsymbol{0}) = \boldsymbol{0}$. Now, we state an important property of f, namely that it is monotone:

Proposition 2. *The map f is order-preserving on $\mathbb{S}_+^{d\times d}$; i.e., for all $\boldsymbol{X}, \boldsymbol{Y} \succeq \boldsymbol{0}$, if $\boldsymbol{X} \preceq \boldsymbol{Y}$ then $f(\boldsymbol{X}) \preceq f(\boldsymbol{Y})$.*

The proof of this Proposition is conceptually simple but technical, and is thus deferred to Appendix A. Next, we adopt a combinatorial view of the structure of the SE dynamics. This will help us identity subspaces of $\mathbb{S}_+^{d\times d}$ that are left invariant by f. Note that the definition of f involves $\boldsymbol{X}^{-\frac{1}{2}}$ acting on $\mathrm{span}(\boldsymbol{1})^\perp$. Additionally, it is easy to verify that for all $\boldsymbol{X} \in \mathbb{S}_+^{d\times d}$, $f(\boldsymbol{X})\boldsymbol{1} = \boldsymbol{0}$, and $f(\boldsymbol{X})_{rs} \leq 0$ for all $r \neq s$. Therefore, without loss of generality, we can restrict the study of the state evolution iteration to the set

$$\mathcal{A} := \left\{ \boldsymbol{X} \in \mathbb{S}_+^{d\times d},\ \boldsymbol{X}\boldsymbol{1} = \boldsymbol{0},\ X_{rs} \leq 0\ \forall (r,s) \text{ s.t. } r \neq s \right\},$$

since it is invariant under the dynamics. The set $\mathcal{A}$ can be seen as the set of Laplacian matrices of weighted graphs on d vertices (every edge (r,s) is weighted by $-X_{rs}$ for $\boldsymbol{X} \in \mathcal{A}$). Hence f can be seen as a transformation on weighted graphs. This transformation enjoys the following invariance property:

Proposition 3. *For all $\boldsymbol{X} \in \mathcal{A}$, f preserves the connected component structure of the graph represented by $\boldsymbol{X}$; i.e, two distinct connected components of the graph whose Laplacian matrix is $\boldsymbol{X}$ remain distinct when transformed by f.*

Proof. The proof relies on the concept of *effective resistance*. One can view a graph of Laplacian $\boldsymbol{X} \in \mathcal{A}$ as a network of resistors with resistances $1/(-X_{rs})$. The effective resistance of an edge (r,s) is the resistance of the entire network when one unit of current is injected at r and collected at s (or vice-versa). Its expression is a simple consequence of Kirchhoff's law, and is equal to $R_{rs} := \left\|\boldsymbol{X}^{-1/2}(\boldsymbol{e}_r - \boldsymbol{e}_s)\right\|_{\ell_2}^2$ (see e.g. [Spi]). It is clear that the effective resistance of an edge is finite if and only if both its endpoints belong to the same connected component of the graph, otherwise $R_{rs} = +\infty$, and $(\boldsymbol{\eta}_r(\boldsymbol{X}))_s = 0$. This causes f to "factor" across connected components, and thus acts on them independently. ■

Next, let us look at the limit of $f(t\boldsymbol{X})$ for large t. For $\boldsymbol{X} \in \mathcal{A}$ invertible on $\mathrm{span}(\boldsymbol{1})^\perp$, we have $\lim_{t\to\infty} f(t\boldsymbol{X}) = \boldsymbol{D} - \boldsymbol{\pi}\boldsymbol{\pi}^\top$, since $\boldsymbol{\eta}_r(t\boldsymbol{X}) \to \boldsymbol{\pi}$ almost surely. More generally, if $\boldsymbol{X}$

represents a graph with $\{V_k\}_{1\le k\le K}$ connected components, $(\boldsymbol{\eta}_r(t\boldsymbol{X}))_s \neq 0$ only if r, s are in the same component. Hence, $\boldsymbol{\eta}_r(t\boldsymbol{X}) \to \frac{\boldsymbol{P}_k\boldsymbol{\pi}}{\mathbf{1}^\top \boldsymbol{P}_k\boldsymbol{\pi}}$, where $\boldsymbol{P}_k$ is the orthogonal projector onto the span of the coordinates in V_k where $r \in V_k$, and we have

$$\lim_{t\to\infty} f(t\boldsymbol{X}) = \boldsymbol{D} - \sum_{k=1}^{K} \frac{\boldsymbol{P}_k\boldsymbol{\pi}\boldsymbol{\pi}^\top\boldsymbol{P}_k}{\mathbf{1}^\top\boldsymbol{P}_k\boldsymbol{\pi}} =: \boldsymbol{L}_K. \tag{9}$$

By Propositions 2 and 3 and the limit calculation (9), we deduce that for any partition $\{V_k\}_{1\le k\le K}$ of $\{1,\cdots,d\}$, and all Laplacian matrices $\boldsymbol{X} \succeq \mathbf{0}$ of graphs with connected components $V_1,\cdots,V_K$, we have

$$f(\boldsymbol{X}) \preceq \boldsymbol{L}_K. \tag{10}$$

Indeed, since $\boldsymbol{X} \preceq t\boldsymbol{X}$ for all $t \ge 1$, we have $f(\boldsymbol{X}) \preceq f(t\boldsymbol{X})$ by monotonicity of f. Letting $t \to \infty$ settles the claim. In particular, with $K = 1$, $\boldsymbol{L}_1 = \boldsymbol{D} - \boldsymbol{\pi}\boldsymbol{\pi}^\top$, and for all $\boldsymbol{X} \in \mathcal{A}$ representing a connected graph (i.e. $\operatorname{rank}(\boldsymbol{X}) = d-1$), we have $f(\boldsymbol{X}) \preceq \boldsymbol{D} - \boldsymbol{\pi}\boldsymbol{\pi}^\top$. We are now ready to state the main result of this subsection.

Theorem 4. *Let $\{V_k\}_{1\le k\le K}$ be a partition of $\{1,\cdots,d\}$, and $\boldsymbol{L}_K$ defined as in (9). Let $\boldsymbol{X}_0 \in \mathcal{A}$ with connected components $V_1,\cdots,V_K$, and such that $\boldsymbol{X}_0 \succeq \kappa^{-1}\boldsymbol{L}_K$. If the SE iteration (4) is initialized from $\boldsymbol{X}_0$, then the sequence $\{\boldsymbol{X}_t\}_{t\ge 0}$ is decreasing in the PSD order, i.e., $\boldsymbol{X}_t \preceq \boldsymbol{X}_{t-1}$ for all $t \ge 1$, and converges to a fixed point $\boldsymbol{X}^*$, i.e., $\boldsymbol{X}^* = \kappa^{-1} f(\boldsymbol{X}^*)$.*

Proof. Let $\boldsymbol{X}_0$ satisfy the conditions of the Theorem. Using $\boldsymbol{X}_0 \succeq \kappa^{-1}\boldsymbol{L}_K$ and observation (10), we have $\boldsymbol{X}_1 = \kappa^{-1} f(\boldsymbol{X}_0) \preceq \boldsymbol{X}_0$. By monotonicity of f, we deduce that the SE iterates form a monotone sequence: $\boldsymbol{X}_{t+1} \preceq \boldsymbol{X}_t$ for all $t \ge 0$. Since $\boldsymbol{X}_t \succeq \mathbf{0}$ for all t, then this sequence must have a limit[1] $\boldsymbol{X}^* \succeq \mathbf{0}$. By continuity of f, this limit must satisfy $\boldsymbol{X}^* = \kappa^{-1} f(\boldsymbol{X}^*)$. ∎

We expect that for κ large enough, $\boldsymbol{X}^* = \mathbf{0}$, meaning that $\lim \boldsymbol{M}_t = \boldsymbol{D}$ and $\lim \mathsf{MSE}_t = 0$. This situation corresponds to perfect recovery of the planted solution $\{\boldsymbol{x}_i^*\}_{i=1}^n$ by AMP. We can easily show that this is the case for

$$\kappa > \kappa^* := \sup_{\boldsymbol{X}\in\mathcal{A}} \frac{\lambda_{\max}(f(\boldsymbol{X}))}{\lambda_{\max}(\boldsymbol{X})}. \tag{11}$$

Indeed,

$$\lambda_{\max}(\boldsymbol{X}_{t+1}) = \kappa^{-1}\lambda_{\max}(f(\boldsymbol{X}_t)) \le \frac{\kappa^*}{\kappa}\lambda_{\max}(\boldsymbol{X}_t).$$

If $\kappa > \kappa^*$ then the SE iterates converge to $\mathbf{0}$ for *every* initial point. It is currently unclear to us whether this condition is also necessary. Instead, we consider three special cases and exactly locate the phase transitions thresholds.

3.2 The binary case

In this section we treat the case $d = 2$, which is akin to a noiseless version of the CDMA problem [GV05] or the problem of compressed sensing with binary prior. In this case, the SE

[1] One can see this by observing that $\{\boldsymbol{z}^\top\boldsymbol{X}_t\boldsymbol{z}\}_{t\ge 0}$ is a non-negative monotonically decreasing sequence for all $\boldsymbol{z} \in \mathbb{R}^d$; hence it must have a (non-negative) limit. Then, via the identity $\boldsymbol{y}^\top\boldsymbol{X}_t\boldsymbol{z} = \frac{1}{2}((\boldsymbol{y}+\boldsymbol{z})^\top\boldsymbol{X}_t(\boldsymbol{y}+\boldsymbol{z}) - (\boldsymbol{y}-\boldsymbol{z})^\top\boldsymbol{X}_t(\boldsymbol{y}-\boldsymbol{z}))$, one deduces that $\{\boldsymbol{y}^\top\boldsymbol{X}_t\boldsymbol{z}\}_{t\ge 0}$ has a limit for all $\boldsymbol{y}, \boldsymbol{z} \in \mathbb{R}^d$. These limits define a bi-linear operator which is $(\boldsymbol{y}, \boldsymbol{z}) \mapsto \boldsymbol{y}^\top\boldsymbol{X}^*\boldsymbol{z}$.

iteration becomes one-dimensional. Indeed, we have $\mathcal{A} = \{x\boldsymbol{u}\boldsymbol{u}^\top, x \geq 0\}$, with $\boldsymbol{u} = (1, -1)^\top$. And since this space is invariant under f, the latter can be parameterized by one scalar function $x \mapsto \varphi(x)$, defined by

$$f(x\boldsymbol{u}\boldsymbol{u}^\top) = \varphi(x)\boldsymbol{u}\boldsymbol{u}^\top, \quad \forall x \geq 0.$$

Next, we compute φ. For $\boldsymbol{X} = x\boldsymbol{u}\boldsymbol{u}^\top$, we have $\boldsymbol{X}^{-\frac{1}{2}}\boldsymbol{u} = \frac{1}{\sqrt{2x}}\boldsymbol{u}$. Then, letting $\boldsymbol{\pi} = (p, 1-p)^\top$, using (6) we have

$$\begin{aligned}
\varphi(x) = f(x\boldsymbol{u}\boldsymbol{u}^\top)_{1,1} &= p - p\,\mathbb{E}_{\boldsymbol{g}}\left[\frac{p}{p + (1-p)e^{-\boldsymbol{g}^\top\boldsymbol{u}/\sqrt{2x} - 1/2x}}\right], \\
&= \mathbb{E}_{\boldsymbol{g}}\left[\frac{p(1-p)}{1 - p + pe^{\boldsymbol{g}^\top\boldsymbol{u}/\sqrt{2x} + 1/2x}}\right], \\
&= \mathbb{E}_{g}\left[\frac{p(1-p)}{1 - p + pe^{g/\sqrt{x} + 1/2x}}\right]. \qquad (12)
\end{aligned}$$

Letting $\boldsymbol{X}_t = a_t\boldsymbol{u}\boldsymbol{u}^\top$, for all $t \geq 0$, the SE reduces to

$$a_{t+1} = \kappa^{-1}\varphi(a_t). \qquad (13)$$

The function φ is continuous, increasing on $\mathbb{R}_+$, and bounded (since $\varphi(\infty) = p(1-p) < \infty$). Moreover, $\varphi(0) = 0$. Therefore, the sequence (13) converges to zero for all initial conditions $a_0 > 0$ if and only if $\kappa^{-1}\varphi(x) < x$ for all $x > 0$, i.e.

$$\kappa > \kappa^*_{\text{binary}}(p) := \sup_{x>0}\ \mathbb{E}_g\left[\frac{p(1-p)x^2}{1 - p + p\exp\left(gx + x^2/2\right)}\right].$$

By a change of variables $g + x/2 \to g$, one can also write this threshold as

$$\kappa^*_{\text{binary}}(p) = \sup_{x>0}\ \mathbb{E}_g\left[\frac{p(1-p)x^2e^{-x^2/8}}{pe^{gx/2} + (1-p)e^{-gx/2}}\right]. \qquad (14)$$

If $\kappa < \kappa^*_{\text{binary}}(p)$, then a new stable fixed point $a^* > 0$ appears and the sequence $\{a_t\}_{t\geq 0}$ converges to it for all initial conditions $a_0 \geq a^*$, and the asymptotic MSE of the AMP algorithm is $\lim_{t\to\infty} \mathsf{MSE}_t = a^* \operatorname{trace}(\boldsymbol{u}\boldsymbol{u}^\top) = 2a^*$.

Figure 1 demonstrates the accuracy of the above theoretical predictions — the predicted MSE by State Evolution matches the empirical MSE of AMP on a random instance with $n = 2000$, across the whole range of p and κ.

3.3 The symmetric case

In this section we treat the symmetric case where all types have equal proportions: $\boldsymbol{\pi} = (\frac{1}{d}, \cdots, \frac{1}{d})$, and analyze the SE dynamics. In this situation, the half-line $\{x(\boldsymbol{D} - \boldsymbol{\pi}\boldsymbol{\pi}^\top)\,,\ x \geq 0\}$ is stable under the application of the map f, and the dynamics becomes one-dimensional if initialized on this half-line.

Lemma 5. *Assume $\boldsymbol{\pi} = (\frac{1}{d}, \cdots, \frac{1}{d})$. For all $x > 0$, we have*

$$f\left(x(\boldsymbol{I} - \frac{1}{d}\mathbf{1}\mathbf{1}^\top)\right) = \varphi(x)\left(\boldsymbol{I} - \frac{1}{d}\mathbf{1}\mathbf{1}^\top\right),$$

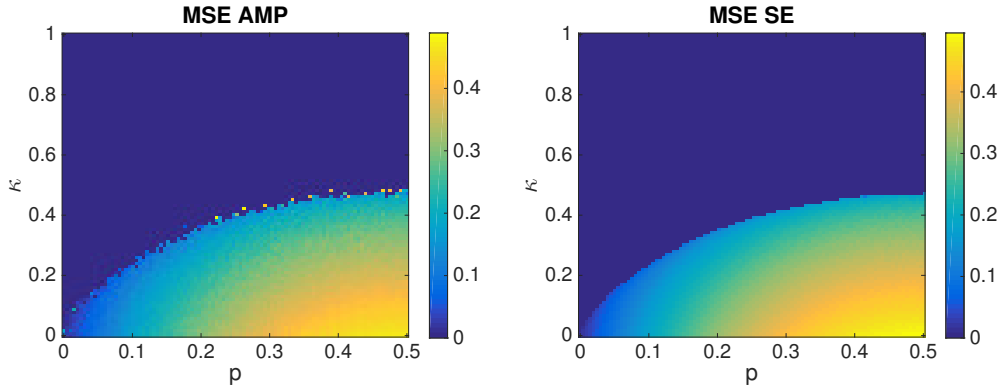

Figure 1. MSE of AMP on a random instance with $n = 2000$ in the binary case (left), and predicted MSE by State Evolution (right) as a function of $p = \pi_1$ and κ. The blue region corresponds to exact recovery. The boundary of this region is traced by the curve $p \mapsto \kappa^*_{\text{binary}}(p)$ in equation (14).

with

$$\varphi(x) = \mathbb{E}_{\boldsymbol{g}}\left[\frac{\exp(g_2/\sqrt{x})}{\exp(g_1/\sqrt{x}+1/x)+\sum_{r=2}^{d}\exp(g_r/\sqrt{x})}\right].$$

Proof. Let $\boldsymbol{P} = (\boldsymbol{I} - \frac{1}{d}\mathbf{1}\mathbf{1}^\top)$, and $\boldsymbol{X} = x\boldsymbol{P}$ with $x > 0$. The matrix $\boldsymbol{P}$ is the orthogonal projector on $\text{span}(\mathbf{1})^\perp$. Therefore, we have

$$\boldsymbol{X}^{-1/2}(\boldsymbol{e}_r - \boldsymbol{e}_s) = (\boldsymbol{e}_r - \boldsymbol{e}_s)/\sqrt{x}.$$

Therefore for all $r \neq s$,

$$f(\boldsymbol{X})_{rs} = -\frac{1}{d}\ \mathbb{E}_{\boldsymbol{g}}\left[\frac{\exp\left(-\boldsymbol{g}^\top(\boldsymbol{e}_r - \boldsymbol{e}_s)/\sqrt{x} - 1/x\right)}{1+\sum_{l\neq r}\exp\left(-\boldsymbol{g}^\top(\boldsymbol{e}_r - \boldsymbol{e}_l)/\sqrt{x} - 1/x\right)}\right].$$

By permutation-invariance of the Gaussian distribution, we see that $f(\boldsymbol{X})$ is constant on its off-diagonal entries, hence on its diagonal entries as well since $f(\boldsymbol{X})\mathbf{1} = \mathbf{0}$. Writing $f(\boldsymbol{X}) = \frac{\alpha}{d}\boldsymbol{I} - \frac{\beta}{d}(\mathbf{1}\mathbf{1}^\top - \boldsymbol{I})$, we have $(\alpha + \beta) = d\beta$. Hence, $f(\boldsymbol{X}) = \beta(\boldsymbol{I} - \frac{1}{d}\mathbf{1}\mathbf{1}^\top)$ with

$$\begin{aligned}\beta &= \mathbb{E}_{\boldsymbol{g}}\left[\frac{\exp\left(-\boldsymbol{g}^\top(\boldsymbol{e}_1 - \boldsymbol{e}_2)/\sqrt{x} - 1/x\right)}{1+\sum_{l\neq r}\exp\left(-\boldsymbol{g}^\top(\boldsymbol{e}_1 - \boldsymbol{e}_l)/\sqrt{x} - 1/x\right)}\right],\\ &= \mathbb{E}_{\boldsymbol{g}}\left[\frac{\exp(g_2/\sqrt{x})}{\exp(g_1/\sqrt{x}+1/x)+\sum_{r=2}^{d}\exp(g_r/\sqrt{x})}\right],\end{aligned}$$

as claimed. ∎

Therefore, if the SE iteration is initialized on this half-line: $\boldsymbol{X}_0 = a_0(\boldsymbol{I} - \frac{1}{d}\mathbf{1}\mathbf{1}^\top)$, with $a_0 > 0$, then $\boldsymbol{X}_t = a_t(\boldsymbol{I} - \frac{1}{d}\mathbf{1}\mathbf{1}^\top)$ for all t, with

$$a_{t+1} = \kappa^{-1}\varphi(a_t).$$

Just as in the binary case, the function φ is continuous, increasing and bounded with $\varphi(0) = 0$. Hence, we have convergence to zero for all initial condition $a_0 > 0$ if and only if $\kappa^{-1}\varphi(x) < x$ for all $x > 0$, i.e.

$$\kappa > \kappa^*_{\text{sym}}(d) := \sup_{x>0} \ \mathbb{E}_{\boldsymbol{g}} \left[\frac{x^2 \exp(g_2 x)}{\exp(g_1 x + x^2) + \sum_{r=2}^{d} \exp(g_r x)} \right]. \tag{15}$$

Otherwise, it converges to a non-zero value a^* for all initial conditions $a_0 > a^*$, and the asymptotic MSE of the AMP algorithm is $a^* \operatorname{trace}(\boldsymbol{I} - \frac{1}{d}\mathbf{1}\mathbf{1}^\top) = (d-1)a^*$. Using the change of variables $g_1 + x \to g_1$, one can also write this threshold as

$$\kappa^*_{\text{sym}}(d) = \sup_{x>0} \ \mathbb{E}_{\boldsymbol{g}} \left[\frac{x^2 e^{-x^2/2} \exp((g_1 + g_2)x)}{\sum_{r=1}^{d} \exp(g_r x)} \right].$$

It is not straightforward to read off the magnitude of $\kappa^*_{\text{sym}}(d)$ from the above expression. We provide a table of approximate values for several small values of d:

d	2	3	4	5	6	7	8	9	10
κ^*_{sym}	.47	.39	.34	.30	.27	.24	.22	.21	.20

For larger d, an asymptotic expression for this threshold may be desirable. We prove the following in Appendix A:

Proposition 6. *There exist two constants $0 < c_l < c_u$ such that when d is large enough,*

$$c_l \frac{\log d}{d} \le \kappa^*_{\text{sym}}(d) \le c_u \frac{\log d}{d},$$

Furthermore, one can take $c_l = 1 - o_d(1)$, and $c_u = 2 + o_d(1)$.

3.4 The general case initialized with a matching

Here we consider the SE iteration in arbitrary dimension and with arbitrary proportions of types $\boldsymbol{\pi}$, but we initialize the dynamics from a special point $\boldsymbol{X}_0$ that corresponds to a matching of the vertices $\{1, \cdots, d\}$: each edge present in the matching corresponds to its own connected component. This case reveals an interesting behavior which we suspect is generic regardless of the initialization: the existence of a sequence of thresholds $\kappa^*_1, \kappa^*_2, \cdots$ ruling the behavior of the SE dynamics. Let $\mathcal{M} = \{(i_1, i_2), (i_3, i_4), \cdots, (i_{K-1}, i_K)\}$ be a matching on the set of vertices $\{1, \cdots, d\}$ (not all vertices are necessarily part of the matching), and let $\boldsymbol{X}_0$ be its Laplacian matrix, where edges are weighted by arbitrary positive numbers. By Proposition 3, f "factors" across connected components, thus each edge in the matching will follow its own dynamics independently of the other edges. The edges not initially present in the matching remain inactive forever. For $(r, s) \in \mathcal{M}$, we have $(X_t)_{rr} = (X_t)_{ss} = -(X_t)_{rs} = -(X_t)_{sr}$, and

$$\boldsymbol{X}_t^{-\frac{1}{2}}(\boldsymbol{e}_r - \boldsymbol{e}_s) = \frac{1}{\sqrt{2(X_t)_{rr}}}(\boldsymbol{e}_r - \boldsymbol{e}_s),$$

and therefore, using expression (6) and letting $x = (X_t)_{rr}$,

$$\begin{aligned} f(\boldsymbol{X}_t)_{rr} &= \pi_r - \mathbb{E}_{\boldsymbol{g}} \left[(\boldsymbol{\eta}_r(\boldsymbol{X}_t))_r \right], \\ &= \pi_r \, \mathbb{E}_{\boldsymbol{g}} \left[\frac{\pi_s}{\pi_r e^{(g_r - g_s)/\sqrt{2x} + 1/2x} + \pi_s} \right], \\ &= \pi_r \, \mathbb{E}_{g} \left[\frac{\pi_s}{\pi_r e^{g/\sqrt{x} + 1/2x} + \pi_s} \right]. \end{aligned}$$

Therefore, the SE iteration reduces to

$$(X_{t+1})_{rr} = \kappa^{-1}\,\mathbb{E}_g\left[\frac{\pi_r\pi_s}{\pi_r e^{g/\sqrt{(X_t)_{rr}}+1/2(X_t)_{rr}}+\pi_s}\right],$$

for all vertices $(r,s)\in\mathcal{M}$. Note that this iteration is essentially the same as the one in the binary case (12)-(13), where p becomes π_r and $1-p$ becomes π_s. For each $(r,s)\in\mathcal{M}$, the above iteration converges to the fixed point zero for every initial point if and only if

$$\kappa > \kappa^*_{rs} := \sup_{x>0}\ \mathbb{E}_g\left[\frac{\pi_r\pi_s x^2 e^{-x^2/8}}{\pi_r e^{gx/2}+\pi_s e^{-gx/2}}\right]. \tag{16}$$

Here, we symmetrized the expression just as in the binary case (14). Arranging these thresholds as $\kappa^*_1 > \kappa^*_2 > \cdots$ from largest to smallest we see that the fixed point of the SE iteration gains one non-zero edge at each κ^*_i as κ decreases from some large value to zero. Equivalently, $\boldsymbol{X}^*$ gains a rank one component corresponding to the connected component constituted by that edge. It is an interesting problem to determine the behavior of the SE iteration and locate these thresholds, if they exist, beyond this simple matching case.

4 Conclusion

We presented an algorithm for decoding categorical variables of a signal from randomly pooled observations of it, and characterized its performance it terms of a state evolution equation. The analysis of this evolution revealed phase transition phenomena in the parameters of the problem that happen in the linear regime $m/n \to \kappa$. These algorithmic results, combined with information-theoretic ones [WHLC16, ERK$^+$16] leave a large region in parameter space ($\gamma\frac{n}{\log n} < m < \kappa n$) where the signal is identifiable but AMP fails at recovering it, hinting at a possible computational hardness in this structured signal recovery problem. This could have interesting applications in privacy-related considerations. Further, we proved the convergence of the SE dynamics to a fixed point. The analysis of the properties of this fixed point as a function of the parameters $\kappa, \boldsymbol{\pi}$ in the general case, together with rigorous proof of the exactness of the state evolution equations for this problem are interesting open problems.

Acknowledgment Part of this work was performed when FK and LZ were visiting the Simons Institute for the Theory of Computing at UC Berkeley. FK acknowledges funding from the EU (FP/2007-2013/ERC grant agreement 307087-SPARCS). MJ acknowledges the support of the Mathematical Data Science program of the Office of Naval Research under grant number N00014-15-1-2670.

References

[BLM12] Mohsen Bayati, Marc Lelarge, and Andrea Montanari. Universality in polytope phase transitions and iterative algorithms. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 1643–1647. IEEE, 2012.

[BM11] Mohsen Bayati and Andrea Montanari. The dynamics of message passing on dense graphs, with applications to compressed sensing. *IEEE Transactions on Information Theory*, 57(2):764–785, 2011.

[DMM09] David L Donoho, Arian Maleki, and Andrea Montanari. Message-passing algorithms for compressed sensing. *Proceedings of the National Academy of Sciences*, 106(45):18914–18919, 2009.

[ERK+16] Ahmed El Alaoui, Aaditya Ramdas, Florent Krzakala, Lenka Zdeborová, and Michael I Jordan. Decoding from pooled data: Sharp information-theoretic bounds. *arXiv preprint arXiv:1611.09981*, 2016.

[GV05] Dongning Guo and Sergio Verdú. Randomly spread CDMA: Asymptotics via statistical physics. *IEEE Transactions on Information Theory*, 51(6):1983–2010, 2005.

[MPV90] Marc Mézard, Giorgio Parisi, and Miguel-Angel Virasoro. *Spin glass theory and beyond.* World Scientific Publishing, 1990.

[RFGS12] Sundeep Rangan, Alyson K Fletcher, Vivek K Goyal, and Philip Schniter. Hybrid generalized approximate message passing with applications to structured sparsity. In *IEEE International Symposium on Information Theory Proceedings (ISIT)*, pages 1236–1240, 2012.

[SBC+02] Pak Sham, Joel S Bader, Ian Craig, Michael O'Donovan, and Michael Owen. DNA pooling: a tool for large-scale association studies. *Nature Reviews Genetics*, 3(11):862–871, 2002.

[Spi] Daniel Spielman. Spectral graph theory. `http://www.cs.yale.edu/homes/spielman/561`.

[TAP77] 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.

[WHLC16] I-Hsiang Wang, Shao-Lun Huang, Kuan-Yun Lee, and Kwang-Cheng Chen. Data extraction via histogram and arithmetic mean queries: Fundamental limits and algorithms. In *IEEE International Symposium on Information Theory (ISIT)*, pages 1386–1390, 2016.

[ZK16] Lenka Zdeborová and Florent Krzakala. Statistical physics of inference: Thresholds and algorithms. *Advances in Physics*, 65(5):453–552, 2016.

A Omitted proofs

A.1 Proof of Proposition 1

We proceed by induction. Now assume that $\boldsymbol{M}_{t-1} = \boldsymbol{Q}_{t-1}$ and that $\boldsymbol{R}_{t-1} = \kappa \boldsymbol{X}_{t-1}$. We prove that $\boldsymbol{R}_t = \kappa \boldsymbol{X}_t$ and then that $\boldsymbol{M}_t$ is symmetric and $\boldsymbol{M}_t = \boldsymbol{Q}_t$.

The first step is to show that $\boldsymbol{Q}_t \mathbf{1} = \boldsymbol{\pi}$. By assumption, $\boldsymbol{X}_{t-1} = \kappa^{-1}(\boldsymbol{D} - \boldsymbol{Q}_{t-1}) = \kappa^{-1}\boldsymbol{R}_{t-1}$. Let us define,

$$\eta_{rs} := \boldsymbol{\eta}_r(\boldsymbol{X})_s = \frac{\pi_s \exp\left(-\boldsymbol{g}^\top \boldsymbol{X}^{-1/2}(\boldsymbol{e}_r - \boldsymbol{e}_s) - \frac{1}{2}\left\|\boldsymbol{X}^{-1/2}(\boldsymbol{e}_r - \boldsymbol{e}_s)\right\|_{\ell_2}^2\right)}{Z_r(\boldsymbol{X})}. \tag{17}$$

The sth coordinate of $\boldsymbol{Q}_t\mathbf{1}$ is

$$(\boldsymbol{Q}_t\mathbf{1})_s = \sum_{r=1}^{d} \pi_r \, \mathbb{E}_{\boldsymbol{g}} \left[\left(\boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}_t^{1/2}\boldsymbol{g}, \kappa^{-1}\boldsymbol{R}_t) \right)_s \right] = \sum_{r=1}^{d} \pi_r \, \mathbb{E}_{\boldsymbol{g}} \left[\eta_{rs} \right].$$

Moreover, letting $\boldsymbol{\delta}_{rs} = \boldsymbol{X}_{t-1}^{-1/2}(\boldsymbol{e}_r - \boldsymbol{e}_s)$, we have

$$\begin{aligned}
\mathbb{E}_{\boldsymbol{g}} \left[\eta_{rs} \right] &= \int \frac{\pi_s \exp(-\frac{1}{2}\left\| \boldsymbol{g} + \boldsymbol{\delta}_{rs} \right\|_{\ell_2}^2)}{\sum_{l=1}^{d} \pi_l \exp(-\frac{1}{2}\left\| \boldsymbol{g} + \boldsymbol{\delta}_{rl} \right\|_{\ell_2}^2)} \frac{e^{-\frac{1}{2}\|\boldsymbol{g}\|_{\ell_2}^2}}{(2\pi)^{d/2}} \mathrm{d}\boldsymbol{g}, \\
&\overset{(i)}{=} \int \frac{\exp(-\frac{1}{2}\left\| \boldsymbol{g} \right\|_{\ell_2}^2)}{\sum_{l=1}^{d} \pi_l \exp(-\frac{1}{2}\left\| \boldsymbol{g} + \boldsymbol{\delta}_{rl} \right\|_{\ell_2}^2)} \frac{\pi_s e^{-\frac{1}{2}\|\boldsymbol{g} - \boldsymbol{\delta}_{rs}\|_{\ell_2}^2}}{(2\pi)^{d/2}} \mathrm{d}\boldsymbol{g}, \\
&= \int \frac{\pi_s \exp(-\frac{1}{2}\left\| \boldsymbol{g} + \boldsymbol{\delta}_{sr} \right\|_{\ell_2}^2)}{\sum_{l=1}^{d} \pi_l \exp(-\frac{1}{2}\left\| \boldsymbol{g} + \boldsymbol{\delta}_{sl} \right\|_{\ell_2}^2)} \frac{e^{-\frac{1}{2}\|\boldsymbol{g}\|_{\ell_2}^2}}{(2\pi)^{d/2}} \mathrm{d}\boldsymbol{g}.
\end{aligned}$$

The only non-trivial equality is (i) and it was obtained through a simple change of variable $\boldsymbol{g} + \boldsymbol{\delta}_{rs} \to \boldsymbol{g}$. Therefore,

$$(\boldsymbol{Q}_t\mathbf{1})_s = \pi_s \sum_{r=1}^{d} \mathbb{E}_{\boldsymbol{g}} \left[\frac{\pi_r \exp(-\frac{1}{2}\left\| \boldsymbol{g} + \boldsymbol{\delta}_{sr} \right\|_{\ell_2}^2)}{\sum_{l=1}^{d} \pi_l \exp(-\frac{1}{2}\left\| \boldsymbol{g} + \boldsymbol{\delta}_{sl} \right\|_{\ell_2}^2)} \right] = \pi_s.$$

In addition, the above argument also shows that $\boldsymbol{M}_t$ is symmetric since, for $r, s \in \{1, \cdots, d\}$,

$$(\boldsymbol{M}_t)_{rs} = \pi_s \, \mathbb{E}_{\boldsymbol{g}}[\eta_{sr}].$$

Now we have that $\boldsymbol{R}_t = \boldsymbol{D} - \boldsymbol{Q}_t$, and by symmetry of $\boldsymbol{M}_t$, $\boldsymbol{X}_t = \kappa^{-1}(\boldsymbol{D} - 2\boldsymbol{M}_t + \boldsymbol{Q}_t)$. To complete the proof, it remains to show that $\boldsymbol{M}_t = \boldsymbol{Q}_t$. For $r, s \in \{1, \cdots, d\}$ we have

$$(\boldsymbol{Q}_t)_{rs} = \sum_{l=1}^{d} \pi_l \;\; \mathbb{E}_{\boldsymbol{g}} \left[\eta_{lr} \eta_{ls} \right].$$

Once again, we make the change of variable $\boldsymbol{g} + \boldsymbol{\delta}_{lr} \to \boldsymbol{g}$:

$$\begin{aligned}
(\boldsymbol{Q}_t)_{rs} &= \pi_r \pi_s \sum_{l=1}^{d} \pi_l \;\; \int \frac{\exp(-\frac{1}{2}\left\| \boldsymbol{g} \right\|_{\ell_2}^2) \;\; \exp(-\frac{1}{2}\left\| \boldsymbol{g} + \boldsymbol{\delta}_{rs} \right\|_{\ell_2}^2)}{\left(\sum_{l'=1}^{d} \pi_{l'} \exp(-\frac{1}{2}\left\| \boldsymbol{g} + \boldsymbol{\delta}_{rl'} \right\|_{\ell_2}^2) \right)^2} \frac{e^{-\frac{1}{2}\|\boldsymbol{g} - \boldsymbol{\delta}_{lr}\|_{\ell_2}^2}}{(2\pi)^{d/2}} \mathrm{d}\boldsymbol{g}, \\
&= \pi_r \pi_s \, \mathbb{E}_{\boldsymbol{g}} \left[\frac{\exp(-\frac{1}{2}\left\| \boldsymbol{g} + \boldsymbol{\delta}_{rs} \right\|_{\ell_2}^2)}{\sum_{r'=1}^{d} \pi_{r'} \exp(-\frac{1}{2}\left\| \boldsymbol{g} + \boldsymbol{\delta}_{rl'} \right\|_{\ell_2}^2)} \right], \\
&= (\boldsymbol{M}_t)_{sr}.
\end{aligned}$$

A.2 Proof of Proposition 2

The map f is differentiable at every $\boldsymbol{X} \succeq \mathbf{0}$ invertible on $\mathrm{span}(\mathbf{1})^{\perp}$. Let $\mathbf{0} \preceq \boldsymbol{X} \preceq \boldsymbol{Y}$, and $\boldsymbol{W} : [0,1] \to \mathbb{S}_+^{d \times d}$ defined by $\boldsymbol{W}(t) = (1-t)\boldsymbol{X} + t\boldsymbol{Y}$. We will show that $\frac{\mathrm{d}}{\mathrm{d}t} f(\boldsymbol{W}(t)) \succeq \mathbf{0}$ for all $t \in [0,1]$ and conclude with the fundamental theorem of calculus

$$f(\boldsymbol{Y}) - f(\boldsymbol{X}) = \int_0^1 \frac{\mathrm{d}}{\mathrm{d}t} f(\boldsymbol{W}(t)) \mathrm{d}t.$$

We start by computing the derivative of each entry of $f(\boldsymbol{W}(t))$. Let $r, s \in \{1, \dots, d\}$. We have

$$\frac{\mathrm{d}}{\mathrm{d}t} f(\boldsymbol{W}(t))_{rs} = -\frac{\mathrm{d}}{\mathrm{d}t} \pi_r \, \mathbb{E}\left[(\boldsymbol{\eta}_r(\boldsymbol{W}(t)))_s \right].$$

To prepare for further calculations, let us write

$$\boldsymbol{A}(t) := \boldsymbol{W}(t)^{-1/2} \frac{\mathrm{d}}{\mathrm{d}t} \left(\boldsymbol{W}(t)^{-1/2} \right),$$

and

$$\boldsymbol{B}(t) := \frac{\mathrm{d}}{\mathrm{d}t} \left(\boldsymbol{W}(t)^{-1} \right) = -\boldsymbol{W}(t)^{-1} \cdot \frac{\mathrm{d}}{\mathrm{d}t} \boldsymbol{W}(t) \cdot \boldsymbol{W}(t)^{-1}.$$

We observe by the chain rule of differentiation that

$$\boldsymbol{A}(t) + \boldsymbol{A}(t)^\top = \boldsymbol{B}(t). \tag{18}$$

This identity will be used several times. Now we start computing the derivative. Let

$$\begin{aligned} D_{rs} :&= \pi_s \frac{\mathrm{d}}{\mathrm{d}t} \exp\left(-\boldsymbol{g}^\top \boldsymbol{W}(t)^{-1/2} (\boldsymbol{e}_r - \boldsymbol{e}_s) - \frac{1}{2} \left\| \boldsymbol{W}(t)^{-1/2} (\boldsymbol{e}_r - \boldsymbol{e}_s) \right\|_{\ell_2}^2 \right) \\ &= \pi_s \left(-\boldsymbol{g}^\top \frac{\mathrm{d}}{\mathrm{d}t} \left(\boldsymbol{W}(t)^{-1/2} \right) (\boldsymbol{e}_r - \boldsymbol{e}_s) - \frac{1}{2} (\boldsymbol{e}_r - \boldsymbol{e}_s)^\top \boldsymbol{B}(t) (\boldsymbol{e}_r - \boldsymbol{e}_s) \right) \\ &\quad \times \exp\left(-\boldsymbol{g}^\top \boldsymbol{W}(t)^{-1/2} (\boldsymbol{e}_r - \boldsymbol{e}_s) - \frac{1}{2} \left\| \boldsymbol{W}(t)^{-1/2} (\boldsymbol{e}_r - \boldsymbol{e}_s) \right\|_{\ell_2}^2 \right). \end{aligned}$$

Then,

$$\frac{\mathrm{d}}{\mathrm{d}t} \boldsymbol{\eta}_r(\boldsymbol{W}(t))_s = \frac{D_{rs}}{Z_r(\boldsymbol{W}(t))} - \boldsymbol{\eta}_r(\boldsymbol{W}(t))_s \times \sum_{l=1}^{d} \frac{D_{rl}}{Z_r(\boldsymbol{W}(t))}. \tag{19}$$

Now, by differentiating under the expectation sign, we are lead to process expressions of the form

$$\mathbb{E}_{\boldsymbol{g}} \left[\frac{D_{rs}}{Z_r(\boldsymbol{W}(t))} \right] \quad \text{and} \quad \mathbb{E}_{\boldsymbol{g}} \left[\boldsymbol{\eta}_r(\boldsymbol{W}(t))_s \frac{D_{rl}}{Z_r(\boldsymbol{W}(t))} \right].$$

Here, the Gaussian integration by parts formula

$$\mathbb{E}_g \left[g h(g) \right] = \mathbb{E}_g \left[h'(g) \right]$$

for all univariate differentiable functions h with moderate growth (say polynomial) at infinity, will be used multiple times. Recalling

$$\eta_{rs} = \boldsymbol{\eta}_r(\boldsymbol{W}(t))_s = \frac{\pi_s \exp\left(-\boldsymbol{g}^\top \boldsymbol{W}(t)^{-1/2} (\boldsymbol{e}_r - \boldsymbol{e}_s) - \frac{1}{2} \left\| \boldsymbol{W}(t)^{-1/2} (\boldsymbol{e}_r - \boldsymbol{e}_s) \right\|_{\ell_2}^2 \right)}{Z_r(\boldsymbol{W}(t))},$$

from (17), we have

$$\begin{aligned} \mathbb{E}_{\boldsymbol{g}} \left[\boldsymbol{g}^\top \frac{\mathrm{d}}{\mathrm{d}t} \left(\boldsymbol{W}(t)^{-1/2} \right) (\boldsymbol{e}_r - \boldsymbol{e}_s) \, \eta_{rs} \right] &= \mathbb{E}_{\boldsymbol{g}} \left[(\nabla_{\boldsymbol{g}} \eta_{rs})^\top \frac{\mathrm{d}}{\mathrm{d}t} \left(\boldsymbol{W}(t)^{-1/2} \right) (\boldsymbol{e}_r - \boldsymbol{e}_s) \right] \\ &= -(\boldsymbol{e}_r - \boldsymbol{e}_s)^\top \boldsymbol{A}(t) (\boldsymbol{e}_r - \boldsymbol{e}_s) \;\; \mathbb{E}_{\boldsymbol{g}} \left[\eta_{rs} \right] \\ &\quad + \sum_{l=1}^{d} (\boldsymbol{e}_r - \boldsymbol{e}_l)^\top \boldsymbol{A}(t) (\boldsymbol{e}_r - \boldsymbol{e}_s) \;\; \mathbb{E}_{\boldsymbol{g}} \left[\eta_{rs} \eta_{rl} \right], \end{aligned}$$

and similarly,

$$\mathbb{E}_{\boldsymbol{g}}\left[\boldsymbol{g}^\top \frac{\mathrm{d}}{\mathrm{d}t}\left(\boldsymbol{W}(t)^{-1/2}\right)(\boldsymbol{e}_r-\boldsymbol{e}_l)\,\eta_{rs}\eta_{rl}\right] = -\big((\boldsymbol{e}_r-\boldsymbol{e}_l)^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l) + (\boldsymbol{e}_r-\boldsymbol{e}_s)^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l)\big)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\right] + 2\sum_{r'=1}^{d}(\boldsymbol{e}_r-\boldsymbol{e}_{r'})^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\eta_{rr'}\right].$$

Therefore,

$$\mathbb{E}_{\boldsymbol{g}}\left[\frac{D_{rs}}{Z_r(\boldsymbol{W}(t))}\right] = (\boldsymbol{e}_r-\boldsymbol{e}_s)^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_s)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\right] - \frac{1}{2}(\boldsymbol{e}_r-\boldsymbol{e}_s)^\top \boldsymbol{B}(t)(\boldsymbol{e}_r-\boldsymbol{e}_s)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\right] - \sum_{l=1}^{d}(\boldsymbol{e}_r-\boldsymbol{e}_l)^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_s)\;\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\right].$$

Since $\boldsymbol{A}(t)+\boldsymbol{A}(t)^\top = \boldsymbol{B}(t)$ (identity (18)), the first two terms in the above expression cancel each other, and we are left with

$$\mathbb{E}_{\boldsymbol{g}}\left[\frac{D_{rs}}{Z_r(\boldsymbol{W}(t))}\right] = -\sum_{l=1}^{d}(\boldsymbol{e}_r-\boldsymbol{e}_l)^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_s)\;\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\right].$$

On the other hand, using the identity (18) again,

$$\begin{aligned}\mathbb{E}_{\boldsymbol{g}}\left[\boldsymbol{\eta}_r(\boldsymbol{W}(t))_s\frac{D_{rl}}{Z_r(\boldsymbol{W}(t))}\right] &= \big((\boldsymbol{e}_r-\boldsymbol{e}_l)^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l) + (\boldsymbol{e}_r-\boldsymbol{e}_s)^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l)\big)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\right] \\ &\quad - \frac{1}{2}(\boldsymbol{e}_r-\boldsymbol{e}_l)^\top \boldsymbol{B}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\right] \\ &\quad - 2\sum_{r'=1}^{d}(\boldsymbol{e}_r-\boldsymbol{e}_{r'})^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\eta_{rr'}\right] \\ &= (\boldsymbol{e}_r-\boldsymbol{e}_s)^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\right] \\ &\quad - 2\sum_{r'=1}^{d}(\boldsymbol{e}_r-\boldsymbol{e}_{r'})^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\eta_{rr'}\right].\end{aligned}$$

Now, using the above two formulas, and recalling (19), we have

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}t}\,\mathbb{E}\left[\boldsymbol{\eta}_r(\boldsymbol{W}(t))_s\right] &= -\sum_{l=1}^{d}(\boldsymbol{e}_r-\boldsymbol{e}_l)^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_s)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\right] \\ &\quad - \sum_{l=1}^{d}(\boldsymbol{e}_r-\boldsymbol{e}_s)^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\right] \\ &\quad + 2\sum_{l=1}^{d}\sum_{r'=1}^{d}(\boldsymbol{e}_r-\boldsymbol{e}_{r'})^\top \boldsymbol{A}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\eta_{rr'}\right].\end{aligned}$$

Using identity (18), the sum of the first two terms in the above expression is

$$
\begin{aligned}
&-\sum_{l=1}^{d}(\boldsymbol{e}_r-\boldsymbol{e}_s)^\top \boldsymbol{B}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\right],\\
&=-\sum_{l,r'=1}^{d}(\boldsymbol{e}_r-\boldsymbol{e}_s)^\top \boldsymbol{B}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\eta_{rr'}\right],
\end{aligned}
$$

where we used the fact $\sum_{r'}\eta_{rr'}=1$ in the last expression. Similarly, the third term is equal to

$$
\sum_{l,r'=1}^{d}(\boldsymbol{e}_r-\boldsymbol{e}_{r'})^\top \boldsymbol{B}(t)(\boldsymbol{e}_r-\boldsymbol{e}_l)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\eta_{rr'}\right].
$$

Therefore we obtain

$$
\frac{\mathrm{d}}{\mathrm{d}t}\,\mathbb{E}\left[\boldsymbol{\eta}_r(\boldsymbol{W}(t))_s\right]=\sum_{l,r'=1}^{d}(\boldsymbol{e}_r-\boldsymbol{e}_{r'})^\top \boldsymbol{B}(t)(\boldsymbol{e}_s-\boldsymbol{e}_l)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\eta_{rr'}\right].
$$

The expression we just obtained does not appear to be symmetric in the indices (r,s), but it does become symmetric when multiplied by π_r, thanks to the following identity:

Lemma 7. *Recall the definition of η_{rs} from* (17)*. For all $r,s,l\in\{1,\cdots,d\}$ we have*

$$
\pi_r\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\right]=\sum_{l'=1}^{d}\pi_{l'}\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{l'r}\eta_{l's}\eta_{l'l}\right].
$$

Using the above, we get

$$
\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}t}f(\boldsymbol{W}(t))_{rs}&=-\pi_r\frac{\mathrm{d}}{\mathrm{d}t}\,\mathbb{E}\left[\boldsymbol{\eta}_r(\boldsymbol{W}(t))_s\right],\\
&=-\sum_{l,l',r'=1}^{d}\pi_{l'}(\boldsymbol{e}_r-\boldsymbol{e}_{r'})^\top \boldsymbol{B}(t)(\boldsymbol{e}_s-\boldsymbol{e}_l)\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{l'r}\eta_{l's}\eta_{l'l}\eta_{l'r'}\right],\\
&=-\sum_{l'=1}^{d}\pi_{l'}\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{l'r}\eta_{l's}\cdot(\boldsymbol{e}_r-\boldsymbol{\eta}_{l'})^\top \boldsymbol{B}(t)(\boldsymbol{e}_s-\boldsymbol{\eta}_{l'})\right].
\end{aligned}
$$

This implies that for all $\boldsymbol{z}\in\mathbb{R}^d$

$$
\begin{aligned}
\boldsymbol{z}^\top\frac{\mathrm{d}}{\mathrm{d}t}f(\boldsymbol{W}(t))\boldsymbol{z}&=\sum_{r,s=1}^{d}\frac{\mathrm{d}}{\mathrm{d}t}f(\boldsymbol{W}(t))_{rs}z_rz_s,\\
&=-\sum_{l'=1}^{d}\pi_{l'}\,\mathbb{E}_{\boldsymbol{g}}\left[(\boldsymbol{z}\odot\boldsymbol{\eta}_{l'}-(\boldsymbol{z}^\top\boldsymbol{\eta}_{l'})\boldsymbol{\eta}_{l'})^\top \boldsymbol{B}(t)(\boldsymbol{z}\odot\boldsymbol{\eta}_{l'}-(\boldsymbol{z}^\top\boldsymbol{\eta}_{l'})\boldsymbol{\eta}_{l'})\right],
\end{aligned}
$$

where $\odot$ denote the entry-wise product of two vectors. Since $\boldsymbol{B}(t)=-\boldsymbol{W}(t)^{-1}\cdot\frac{\mathrm{d}}{\mathrm{d}t}\boldsymbol{W}(t)\cdot\boldsymbol{W}(t)^{-1}$ and $\frac{\mathrm{d}}{\mathrm{d}t}\boldsymbol{W}(t)=\boldsymbol{Y}-\boldsymbol{X}\succeq\boldsymbol{0}$, we see that

$$
\boldsymbol{z}^\top\frac{\mathrm{d}}{\mathrm{d}t}f(\boldsymbol{W}(t))\boldsymbol{z}=\sum_{l'=1}^{d}\pi_{l'}\,\mathbb{E}_{\boldsymbol{g}}\left[\left\|(\boldsymbol{Y}-\boldsymbol{X})^{\frac{1}{2}}\boldsymbol{W}(t)^{-1}\left(\boldsymbol{z}\odot\boldsymbol{\eta}_{l'}-(\boldsymbol{z}^\top\boldsymbol{\eta}_{l'})\boldsymbol{\eta}_{l'}\right)\right\|_{\ell_2}^2\right]\geq 0,
$$

hence concluding the general argument. It now remains to prove Lemma 7.

Proof of Lemma 7. The proof relies on a simple change of variables in the expectation. Using (17), and letting $\boldsymbol{\delta}_{rs} = \boldsymbol{W}(t)^{-1/2}(\boldsymbol{e}_r - \boldsymbol{e}_s)$ for all r, s, we have

$$\begin{aligned}
\mathbb{E}_{\boldsymbol{g}}\left[\eta_{l'r}\eta_{l's}\eta_{l'l}\right] &= \pi_r\pi_s\pi_l\,\mathbb{E}_{\boldsymbol{g}}\left[\frac{e^{-\boldsymbol{g}^\top(\boldsymbol{\delta}_{l'r}+\boldsymbol{\delta}_{l's}+\boldsymbol{\delta}_{l'l})-\frac{1}{2}\|\boldsymbol{\delta}_{l'r}\|_{\ell_2}^2-\frac{1}{2}\|\boldsymbol{\delta}_{l's}\|_{\ell_2}^2-\frac{1}{2}\|\boldsymbol{\delta}_{l'l}\|_{\ell_2}^2}}{\left(\sum_{r'=1}^d \pi_{r'}e^{-\boldsymbol{g}^\top\boldsymbol{\delta}_{l'r'}-\frac{1}{2}\|\boldsymbol{\delta}_{l'r'}\|_{\ell_2}^2}\right)^3}\right] \\
&= \pi_r\pi_s\pi_l\,\mathbb{E}_{\boldsymbol{g}}\left[\frac{e^{-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{l'r}\|_{\ell_2}^2-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{l's}\|_{\ell_2}^2-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{l'l}\|_{\ell_2}^2}}{\left(\sum_{r'=1}^d \pi_{r'}e^{-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{l'r'}\|_{\ell_2}^2}\right)^3}\right] \\
&= \pi_r\pi_s\pi_l\int_{\mathbb{R}^d}\frac{e^{-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{l'r}\|_{\ell_2}^2-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{l's}\|_{\ell_2}^2-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{l'l}\|_{\ell_2}^2}}{\left(\sum_{r'=1}^d \pi_{r'}e^{-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{l'r'}\|_{\ell_2}^2}\right)^3}\,\frac{e^{-\frac{1}{2}\|\boldsymbol{g}\|_{\ell_2}^2}}{(2\pi)^{d/2}}\,\mathrm{d}\boldsymbol{g}.
\end{aligned}$$

We make the change of variables $\boldsymbol{g} + \boldsymbol{\delta}_{l'r} \to \boldsymbol{g}$. The term $\|\boldsymbol{g}+\boldsymbol{\delta}_{l'r}\|_{\ell_2}^2$ becomes $\|\boldsymbol{g}\|_{\ell_2}^2$, $\|\boldsymbol{g}+\boldsymbol{\delta}_{l's}\|_{\ell_2}^2$ becomes $\|\boldsymbol{g}+\boldsymbol{\delta}_{rs}\|_{\ell_2}^2$, $\|\boldsymbol{g}+\boldsymbol{\delta}_{l'l}\|_{\ell_2}^2$ becomes $\|\boldsymbol{g}+\boldsymbol{\delta}_{rl}\|_{\ell_2}^2$, $\|\boldsymbol{g}\|_{\ell_2}^2$ becomes $\|\boldsymbol{g}+\boldsymbol{\delta}_{rl'}\|_{\ell_2}^2$, and $\|\boldsymbol{g}+\boldsymbol{\delta}_{l'r'}\|_{\ell_2}^2$ becomes $\|\boldsymbol{g}+\boldsymbol{\delta}_{rr'}\|_{\ell_2}^2$ in the denominator. The first term will assume the role of the Gaussian density, and we rewrite the above as an expectation under the Gaussian distribution:

$$\pi_r\pi_s\pi_l\,\mathbb{E}_{\boldsymbol{g}}\left[\frac{e^{-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{rs}\|_{\ell_2}^2-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{rl}\|_{\ell_2}^2-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{rl'}\|_{\ell_2}^2}}{\left(\sum_{r'=1}^d \pi_{r'}e^{-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{rr'}\|_{\ell_2}^2}\right)^3}\right].$$

If the above expression is multiplied by $\pi_{l'}$ and summed over all l', the third term in the numerator cancels with one power of the denominator, and the result is

$$\pi_r\pi_s\pi_l\,\mathbb{E}_{\boldsymbol{g}}\left[\frac{e^{-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{rs}\|_{\ell_2}^2-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{rl}\|_{\ell_2}^2}}{\left(\sum_{r'=1}^d \pi_{r'}e^{-\frac{1}{2}\|\boldsymbol{g}+\boldsymbol{\delta}_{rr'}\|_{\ell_2}^2}\right)^2}\right] = \pi_r\,\mathbb{E}_{\boldsymbol{g}}\left[\eta_{rs}\eta_{rl}\right].$$

■

A.3 Proof of Proposition 6

For $x > 0$, we let

$$\phi_d(x) := \mathbb{E}_{\boldsymbol{g}}\left[\frac{x^2\sum_{r=2}^d e^{g_r\sqrt{\log(d-1)}x}}{e^{g_1\sqrt{\log(d-1)}x}\cdot(d-1)x^2 + \sum_{r=2}^d e^{g_r\sqrt{\log(d-1)}x}}\right].$$

By symmetry in the variables g_r, $r \geq 2$, we can see that

$$\phi_d\left(\frac{x}{\sqrt{\log(d-1)}}\right) = \frac{d-1}{\log(d-1)}\,\mathbb{E}_{\boldsymbol{g}}\left[\frac{x^2\exp(g_2x)}{\exp(g_1x+x^2)+\sum_{r=2}^d\exp(g_rx)}\right].$$

Our claim reduces to exhibiting upper and lower bounds on $\sup_{x>0}\phi_d(x)$ which are asymptotically independent of d. We start with the upper bound. Since, the function $x \to \frac{x}{1+x}$ is

concave on $\mathbb{R}_+$, we have by Jensen's inequality,

$$\begin{aligned}\phi_d(x) &\le \mathbb{E}_{g_1}\left[\frac{x^2\sum_{r=2}^d \mathbb{E}_{g_r:r\ge 2}\left[e^{g_r\sqrt{\log(d-1)}x}\right]}{e^{g_1\sqrt{\log(d-1)}x}\cdot(d-1)^{x^2}+\sum_{r=2}^d \mathbb{E}_{g_r:r\ge 2}\left[e^{g_r\sqrt{\log(d-1)}x}\right]}\right],\\ &= \mathbb{E}_{g_1}\left[\frac{x^2(d-1)^{1+x^2/2}}{e^{g_1\sqrt{\log(d-1)}x}\cdot(d-1)^{x^2}+(d-1)^{1+x^2/2}}\right].\end{aligned}$$

We split the analysis into two cases: $x \le \sqrt{2}+\epsilon$, $x > \sqrt{2}+\epsilon$ for some $\epsilon > 0$. We see that $\phi_d(x) \le x^2$ for all $x > 0$. If $x \le \sqrt{2}+\epsilon$, then $\phi_d(x) \le (\sqrt{2}+\epsilon)^2$. For the remaining case, let $\alpha = \alpha(\epsilon) > 0$ such that $x^2/2 - \alpha x - 1 > 0$ for all $x > \sqrt{2}+\epsilon$. One can find such an α as the solution to the equation $\alpha + \sqrt{\alpha^2+2} = \sqrt{2}+\epsilon$. Next, we let $\mathcal{E}$ be the event that $g_1 \le \frac{1-x^2/2+\alpha x}{x}\sqrt{\log(d-1)}$, and write

$$\begin{aligned}\phi_d(x) \le\ & \mathbb{E}_{g_1}\left[\frac{x^2}{(d-1)^{x^2/2-1}\cdot e^{g_1\sqrt{\log(d-1)}x}+1}\middle|\bar{\mathcal{E}}\right]\Pr(\bar{\mathcal{E}})\\ &+ \mathbb{E}_{g_1}\left[\frac{x^2}{(d-1)^{x^2/2-1}\cdot e^{g_1\sqrt{\log(d-1)}x}+1}\middle|\mathcal{E}\right]\Pr(\mathcal{E}),\end{aligned}$$

Under $\bar{\mathcal{E}}$, we have $-x^2/2 + 1 - g_1 x\sqrt{\log(d-1)} \le -\alpha x$, and the first term in the above expression is upper bounded by

$$x^2(d-1)^{-\alpha x}.$$

On the other hand, we upper bound the conditional expectation in the second term by x^2, and use the fact that $\Pr(\mathcal{E}) \le (d-1)^{-(1-x^2/2+\alpha x)^2/(2x^2)}$. We obtain the upper bound

$$\phi_d(x) \le x^2\left((d-1)^{-\alpha x} + (d-1)^{-(1-x^2/2+\alpha x)^2/(2x^2)}\right),$$

which decays to 0 as $d\to\infty$ uniformly in $x \ge \sqrt{2}+\epsilon$. This proves that

$$\sup_{x>0}\phi_d(x) \le (\sqrt{2}+\epsilon)^2$$

for all d sufficiently large.

Now we turn our attention on the lower bound. Since the function $x \to \frac{x}{1+x}$ is increasing, we have

$$\phi_d(x) \ge \mathbb{E}_{\boldsymbol{g}}\left[\frac{x^2 e^{\max_{r\ge 2} g_r\sqrt{\log(d-1)}x}}{e^{g_1\sqrt{\log(d-1)}x}\cdot(d-1)^{x^2}+e^{\max_{r\ge 2} g_r\sqrt{\log(d-1)}x}}\right].$$

The maximum of finitely many Gaussians concentrates in a sub-Gaussian way: for all $t \ge 0$,

$$\Pr\left(\max_{r\ge 2} g_r - \mathbb{E}[\max_{r\ge 2} g_r] \le -t\right) \le e^{-t^2/2}.$$

We write $\mathbb{E}[\max_{r\ge 2} g_r] = c_d\sqrt{\log(d-1)}$; it is known that $c_d = \sqrt{2}(1-o_d(1))$. Letting $t = \epsilon c_d\sqrt{\log(d-1)}$ for some $\epsilon > 0$, we have

$$\phi_d(x) \ge \mathbb{E}_{g_1}\left[\frac{x^2(d-1)^{(1-\epsilon)c_d x}}{e^{g_1\sqrt{\log(d-1)}x}\cdot(d-1)^{x^2}+(d-1)^{(1-\epsilon)c_d x}}\right]\cdot\left(1-(d-1)^{-\epsilon^2 c_d^2/2}\right).$$

We plug the value $x = (1-\epsilon)c_d$ in the right hand side, and deduce

$$\sup_{x>0} \phi_d(x) \geq \mathbb{E}_{g_1}\left[\frac{(1-\epsilon)^2 c_d^2}{e^{g_1(1-\epsilon)c_d\sqrt{\log(d-1)}}+1}\right] \cdot \left(1-(d-1)^{-\epsilon^2 c_d^2/2}\right).$$

We see that the above converges to the value $(1-\epsilon)^2$ as $d \to \infty$.

B Deriving the Approximate Message Passing equations

We divide the derivation of the AMP equations into two parts. First, we write down the Belief Propagation (BP) equations, and simplify them to the "relaxed" BP equations. Then, we show how to transform the relaxed BP equations into the AMP iteration.

B.1 From Belief Propagation (BP) to Relaxed BP

The factor graph G of our model consists of a bipartite graph with the variables $\{\boldsymbol{x}_i,\ 1 \leq i \leq n\}$ on one side of the bipartition and the measurements $\{\boldsymbol{h}_a,\ 1 \leq a \leq m\}$ on the other side. A measurement (or check) node $\boldsymbol{h}_a$ is connected to $k = \alpha n$ variables nodes in expectation chosen uniformly at random (i.e. those such that $A_{ai} = 1$) from all the variable nodes.

We rescale the elements of the sensing matrix $\boldsymbol{A}$ such that A_{ai} has expectation 0 and variance $\frac{\alpha(1-\alpha)}{n}$. This can be done by subtracting the vector $\alpha n \boldsymbol{\pi}$ from each observation $\boldsymbol{h}_a$ and dividing everything by $\sqrt{n}$. Hence, we let

$$\bar{\boldsymbol{h}}_a := (\boldsymbol{h}_a - \alpha n \boldsymbol{\pi})/\sqrt{n},$$

and

$$\overline{\boldsymbol{A}} = (\boldsymbol{A} - \alpha \mathbf{1}_m \mathbf{1}_n^\top)/\sqrt{n}.$$

The linear system $\boldsymbol{h}_a = \sum_{j=1}^n A_{aj}\boldsymbol{x}_j^*$ is equivalent to $\bar{\boldsymbol{h}}_a = \sum_{j=1}^n \overline{A}_{aj}\boldsymbol{x}_j^*$.

We now write the messages of the Belief Propagation algorithm. Let $\vec{E}$ be the set of directed edges of the factor graph with all possible directions, i.e., each edge (i,a) is endowed with both directions $i \to a$ and $a \to i$. Note that $|\vec{E}| = 2km$. The message passing procedure consists of iterating a map $\mathsf{BP} : \left(\Delta^{d-1}\right)^{\vec{E}} \to \left(\Delta^{d-1}\right)^{\vec{E}}$ from some initial guess until (possible) convergence. For convenience, for all $r \in \{1, \cdots, d\}$, any set of messages $\boldsymbol{m} = \{\boldsymbol{m}_{i\to a}\ ,\ \boldsymbol{m}_{a\to i}\ :\ A_{ai} = 1\} \in \left(\Delta^{d-1}\right)^{\vec{E}}$ on G, and any directed edge $a \to i$, we denote the rth coordinate of the d-dimensional message $\boldsymbol{m}_{a\to i}$ by $\boldsymbol{m}_{a\to i}(\boldsymbol{e}_r)$ instead of $(\boldsymbol{m}_{a\to i})_r$, and similarly for the coordinates of $\boldsymbol{m}_{a\to i}$. With this notation in hand, the map BP is defined as follows: We consider a prior distribution on the messages that agrees with the category proportions in the planted solution τ^*, i.e., for every i and r,

$$P(\boldsymbol{x}_i = \boldsymbol{e}_r) = \pi_r$$

This is our "uninformative" prior: under lack of any further information, the algorithm predicts that $\boldsymbol{x}_i = \boldsymbol{e}_r$ with probability π_r for all i and r. Then for all $\boldsymbol{x} \in \{\boldsymbol{e}_1, \cdots, \boldsymbol{e}_d\}$,

$$\mathsf{BP}(\boldsymbol{m})_{i\to a}(\boldsymbol{x}) := \frac{1}{Z_{i\to a}(\boldsymbol{m})} P(\boldsymbol{x}) \prod_{b \in \partial i \setminus a} \boldsymbol{m}_{b\to i}(\boldsymbol{x}), \tag{20}$$

$$\mathsf{BP}(\boldsymbol{m})_{a\to i}(\boldsymbol{x}) := \frac{1}{Z_{a\to i}(\boldsymbol{m})} \sum_{\substack{\boldsymbol{x}_j \in \{\boldsymbol{e}_1,\cdots,\boldsymbol{e}_d\} \\ j \in \partial a \setminus i}} \mathbb{1}\left\{\bar{\boldsymbol{h}}_a = \overline{A}_{ai}\boldsymbol{x} + \sum_{j\neq i} \overline{A}_{aj}\boldsymbol{x}_j\right\} \prod_{j \in \partial a \setminus i} \boldsymbol{m}_{j\to a}(\boldsymbol{x}_j), \tag{21}$$

with $Z_{i\to a}(\boldsymbol{m})$ and $Z_{a\to i}(\boldsymbol{m})$ are the normalizing factors such that $\sum_{r=1}^{d}\mathsf{BP}(\boldsymbol{m})_{i\to a}(\boldsymbol{e}_r) = \sum_{r=1}^{d}\mathsf{BP}(\boldsymbol{m})_{a\to i}(\boldsymbol{e}_r) = 1$. If G was a tree, the map BP would compute the exact posterior distribution of the category assignments $\{\boldsymbol{x}_i \,:\, 1 \le i \le n\}$ given the observations $\{\boldsymbol{h}_a \,:\, 1 \le a \le m\}$. In our case this will only be true when m/n is large enough.

We see that the second equation above has a sum involving d^{k-1} terms, which makes the execution of the BP algorithm intractable. We derive a set of *relaxed* Belief Propagation messages from the above that only require linear-algebraic computations of size polynomial in n and m. Later, we further simplify these equations by leveraging the fact that our factor graph is random and dense, to finally arrive at the Approximate Message Passing iteration.

We now proceed by replacing the indicator in (21) by a Gaussian with small variance $\sigma > 0$, which we then linearize by writing it as the Fourier transform of the standard Gaussian measure (this is also known as the Hubbard-Stratonovich transformation):

$$\begin{aligned}
\mathsf{BP}_\sigma(\boldsymbol{m})_{a\to i}(\boldsymbol{x}) &:= \frac{1}{Z_{a\to i}(\boldsymbol{m})} \sum_{\substack{\boldsymbol{x}_j\in\{\boldsymbol{e}_1,\cdots,\boldsymbol{e}_d\}\\ j\in\partial a\setminus i}} \exp\Big(-\Big\|\bar{\boldsymbol{h}}_a - \sum_{j=1}^{n}\bar{A}_{aj}\boldsymbol{x}_j\Big\|_{\ell_2}^2\Big/2\sigma^2\Big)\prod_{j\in\partial a\setminus i}\boldsymbol{m}_{j\to a}(\boldsymbol{x_j}),\\
&\propto \sum_{\substack{\boldsymbol{x}_j\in\{\boldsymbol{e}_1,\cdots,\boldsymbol{e}_d\}\\ j\in\partial a\setminus i}} \int_{\mathbb{R}^d}\exp\Big(\mathbf{i}\sigma^{-1}\boldsymbol{g}^\top\Big(\bar{\boldsymbol{h}}_a - \sum_{j=1}^{n}\bar{A}_{aj}\boldsymbol{x}_j\Big)\Big)\prod_{j\in\partial a\setminus i}\boldsymbol{m}_{j\to a}(\boldsymbol{x}_j)\gamma_d(\mathrm{d}\boldsymbol{g}),
\end{aligned}$$

where we let γ_d refer to the standard d-dimensional Gaussian measure.

$$\begin{aligned}
&\propto \int_{\mathbb{R}^d}\exp\Big(\mathbf{i}\sigma^{-1}\boldsymbol{g}^\top\big(\bar{\boldsymbol{h}}_a - \bar{A}_{ai}\boldsymbol{x}\big)\Big)\\
&\qquad\times\prod_{j\in\partial a\setminus i}\Big[\sum_{\boldsymbol{x}_j\in\{\boldsymbol{e}_1,\cdots,\boldsymbol{e}_d\}}\exp\big(-\mathbf{i}\sigma^{-1}\bar{A}_{aj}\boldsymbol{g}^\top\boldsymbol{x}_j\big)\,\boldsymbol{m}_{j\to a}(\boldsymbol{x}_j)\Big]\gamma_d(\mathrm{d}\boldsymbol{g}).
\end{aligned}$$

Now, observe that the exponentials in the sum above involve the terms $\bar{A}_{aj}$ which are of order $1/\sqrt{n}$. By expanding the Taylor series of the exponential, one can show

$$\begin{aligned}
\sum_{\boldsymbol{x}_j\in\{\boldsymbol{e}_1,\cdots,\boldsymbol{e}_d\}}\exp(-\mathbf{i}\sigma^{-1}\bar{A}_{aj}\boldsymbol{g}^\top\boldsymbol{x}_j)\,\boldsymbol{m}_{j\to a}(\boldsymbol{x}_j) &= \sum_{r=1}^{d}\exp(-\mathbf{i}\sigma^{-1}\bar{A}_{aj}\boldsymbol{g}^\top\boldsymbol{e}_r)\,\boldsymbol{m}_{j\to a}(\boldsymbol{e}_r)\\
&= \exp\Big(-\mathbf{i}\sigma^{-1}\bar{A}_{aj}\boldsymbol{g}^\top\boldsymbol{m}_{j\to a} - \frac{1}{2}\sigma^{-2}\bar{A}_{aj}^2\boldsymbol{g}^\top\boldsymbol{B}_{j\to a}\boldsymbol{g}\Big)\\
&\quad + \mathcal{O}(1/n^{3/2}),
\end{aligned}$$

where

$$\boldsymbol{B}_{j\to a} = \mathrm{Diag}(\boldsymbol{m}_{j\to a}) - \boldsymbol{m}_{j\to a}\boldsymbol{m}_{j\to a}^\top. \tag{22}$$

Plugging the above expression into the message, we get

$$\begin{aligned}
\mathsf{BP}_\sigma(\boldsymbol{m})_{a\to i}(\boldsymbol{x}) &\approx \frac{1}{Z_{a\to i}(\boldsymbol{m})}\int_{\mathbb{R}^d}\exp\Big(\mathbf{i}\sigma^{-1}\boldsymbol{g}^\top\big(\bar{\boldsymbol{h}}_a - \bar{A}_{ai}\boldsymbol{x}\big)\Big)\\
&\qquad\times\prod_{j\in\partial a\setminus i}\exp\Big(-\mathbf{i}\sigma^{-1}\bar{A}_{aj}\boldsymbol{g}^\top\boldsymbol{m}_{j\to a} - \frac{1}{2}\sigma^{-2}\bar{A}_{aj}^2\boldsymbol{g}^\top\boldsymbol{B}_{j\to a}\boldsymbol{g}\Big)\gamma_d(\mathrm{d}\boldsymbol{g}),\\
&= \frac{1}{Z_{a\to i}(\boldsymbol{m})}\int_{\mathbb{R}^d}\exp\Big(\mathbf{i}\sigma^{-1}\boldsymbol{g}^\top\big(\bar{\boldsymbol{h}}_a - \bar{A}_{ai}\boldsymbol{x}\big)\\
&\qquad - \sum_{j\in\partial a\setminus i}\mathbf{i}\sigma^{-1}\bar{A}_{aj}\boldsymbol{g}^\top\boldsymbol{m}_{j\to a} - \frac{1}{2}\sum_{j\in\partial a\setminus i}\sigma^{-2}\bar{A}_{aj}^2\boldsymbol{g}^\top\boldsymbol{B}_{j\to a}\boldsymbol{g}\Big)\gamma_d(\mathrm{d}\boldsymbol{g}).
\end{aligned}$$

We denote the "average" message and variance that appear in the formula above by

$$\boldsymbol{\omega}_{a\to i} := \sum_{j\in\partial a\setminus i} \overline{A}_{aj}\boldsymbol{m}_{j\to a}, \tag{23}$$

$$\boldsymbol{V}_{a\to i} := \sum_{j\in\partial a\setminus i} \overline{A}^2_{aj}\boldsymbol{B}_{j\to a}. \tag{24}$$

The exponentiated term in the integrand, when combined with the contribution of the Gaussian density, becomes

$$\begin{aligned}\mathbf{i}\sigma^{-1}\boldsymbol{g}^\top\big(\bar{\boldsymbol{h}}_a - \overline{A}_{ai}\boldsymbol{x} - \boldsymbol{\omega}_{a\to i}\big) - \frac{1}{2}\sigma^{-2}\boldsymbol{g}^\top\boldsymbol{V}_{a\to i}\boldsymbol{g} - \frac{1}{2}\left\|\boldsymbol{g}\right\|^2_{\ell_2} \\ = \mathbf{i}\sigma^{-1}\boldsymbol{g}^\top\big(\bar{\boldsymbol{h}}_a - \overline{A}_{ai}\boldsymbol{x} - \boldsymbol{\omega}_{a\to i}\big) - \frac{1}{2}\boldsymbol{g}^\top(\sigma^{-2}\boldsymbol{V}_{a\to i} + \boldsymbol{I})\boldsymbol{g}.\end{aligned}$$

Now, computing the integral yields

$$\mathsf{BP}_\sigma(\boldsymbol{m})_{a\to i}(\boldsymbol{x}) \propto \exp\left(-\frac{1}{2\sigma^2}\left\|(\sigma^{-2}\boldsymbol{V}_{a\to i} + \boldsymbol{I})^{-\frac{1}{2}}\big(\bar{\boldsymbol{h}}_a - \overline{A}_{ai}\boldsymbol{x} - \boldsymbol{\omega}_{a\to i}\big)\right\|^2_{\ell_2}\right),$$

and letting $\sigma \to 0$ yields

$$\mathsf{BP}(\boldsymbol{m})_{a\to i}(\boldsymbol{x}) \propto \exp\left(-\frac{1}{2}\left\|\boldsymbol{V}^{-\frac{1}{2}}_{a\to i}\big(\bar{\boldsymbol{h}}_a - \overline{A}_{ai}\boldsymbol{x} - \boldsymbol{\omega}_{a\to i}\big)\right\|^2_{\ell_2}\right).$$

On the other hand, by injecting the above formula into the messages from-variable-to-check node (20), the latter can be written as

$$\begin{aligned}\mathsf{BP}(\boldsymbol{m})_{i\to a}(\boldsymbol{x}) &\propto P(\boldsymbol{x})\exp\left(\sum_{b\in\partial i\setminus a} -\frac{1}{2}\left\|\boldsymbol{V}^{-1/2}_{b\to i}(\bar{\boldsymbol{h}}_b - \overline{A}_{bi}\boldsymbol{x} - \boldsymbol{\omega}_{b\to i})\right\|^2_{\ell_2}\right), \\ &\propto P(\boldsymbol{x})\exp\left(-\frac{1}{2}\boldsymbol{x}^\top\left(\sum_{b\in\partial i\setminus a}\overline{A}^2_{bi}\boldsymbol{V}^{-1}_{b\to i}\right)\boldsymbol{x} + \boldsymbol{x}^\top\left(\sum_{b\in\partial i\setminus a}\overline{A}_{bi}\boldsymbol{V}^{-1}_{b\to i}(\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_{b\to i})\right)\right), \\ &\propto P(\boldsymbol{x})\exp(-(\boldsymbol{x} - \boldsymbol{z}_{i\to a})^\top\boldsymbol{\Sigma}^{-1}_{i\to a}(\boldsymbol{x} - \boldsymbol{z}_{i\to a})/2),\end{aligned} \tag{25}$$

where we denoted the average message and variance by

$$\boldsymbol{z}_{i\to a} = \boldsymbol{\Sigma}_{i\to a}\sum_{b\in\partial i\setminus a}\overline{A}_{bi}\boldsymbol{V}^{-1}_{b\to i}(\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_{b\to i}), \tag{26}$$

$$\boldsymbol{\Sigma}^{-1}_{i\to a} := \sum_{b\in\partial i\setminus a}\overline{A}^2_{bi}\boldsymbol{V}^{-1}_{b\to i}. \tag{27}$$

The combination of the equations (22-27) forms the set of *Relaxed Belief Propagation* (RBP)

equations:

$$\begin{cases} \boldsymbol{m}_{i\to a} = \boldsymbol{\eta}(\boldsymbol{z}_{i\to a}, \boldsymbol{\Sigma}_{i\to a}), \\ \boldsymbol{B}_{i\to a} = \mathrm{Diag}(\boldsymbol{m}_{i\to a}) - \boldsymbol{m}_{i\to a}\boldsymbol{m}_{i\to a}^\top, \\ \boldsymbol{z}_{i\to a} = \boldsymbol{\Sigma}_{i\to a} \sum_{b\in\partial i\setminus a} \bar{A}_{bi} \boldsymbol{V}_{b\to i}^{-1}(\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_{b\to i}), \\ \boldsymbol{\Sigma}_{i\to a}^{-1} = \sum_{b\in\partial i\setminus a} \bar{A}_{bi}^2 \boldsymbol{V}_{b\to i}^{-1}, \\ \boldsymbol{\omega}_{a\to i} = \sum_{j\in\partial a\setminus i} \bar{A}_{aj} \boldsymbol{m}_{j\to a}, \\ \boldsymbol{V}_{a\to i} = \sum_{j\in\partial a\setminus i} \bar{A}_{aj}^2 \boldsymbol{B}_{j\to a}, \end{cases} \tag{28}$$

with

$$\boldsymbol{\eta}(\boldsymbol{z}, \boldsymbol{\Sigma}) := \frac{1}{Z(\boldsymbol{z}, \boldsymbol{\Sigma})} \sum_{r=1}^{d} \pi_r \boldsymbol{e}_r \exp\left(-\frac{1}{2}(\boldsymbol{e}_r - \boldsymbol{z})^\top \boldsymbol{\Sigma}^{-1}(\boldsymbol{e}_r - \boldsymbol{z})\right), \tag{29}$$

where $Z(\boldsymbol{z}, \boldsymbol{\Sigma})$ is the normalization constant so that $\mathbf{1}^\top \boldsymbol{\eta}(\boldsymbol{z}, \boldsymbol{\Sigma}) = 1$. The complexity of the iterative version of these equations is of order at most $\mathcal{O}(d^3 nm)$ which is essentially quadratic in n. Next, we further reduce the complexity of the iteration to $\mathcal{O}(d^3(n+m))$ by showing that it suffices to track the average of the incoming messages at each node. This is due to the fact that the factor graph is dense and its edges are independent.

B.2 From Relaxed BP to Approximate Message Passing

Let us now derive the equations of the (more efficient) AMP algorithm. We will define a notion of "total messages" $\boldsymbol{m}_i, \boldsymbol{B}_i$, $\boldsymbol{z}_i$, $\boldsymbol{\Sigma}_i$, $\boldsymbol{\omega}_a$, $\boldsymbol{V}_a$ and relate them to one another. The expressions (23), (24), (26), and (27) defining $\boldsymbol{\omega}_{a\to i}$, $\boldsymbol{V}_{a\to i}$, $\boldsymbol{z}_{i\to a}$ and $\boldsymbol{\Sigma}_{i\to a}$ respectively involve sums over all the neighbors of the node sending the message except the node receiving the message. We first define $\boldsymbol{\omega}_a$, $\boldsymbol{V}_a$ and $\boldsymbol{\Sigma}_i$ by adding this last term:

$$\begin{aligned} \boldsymbol{\omega}_a^t &:= \sum_{j\in\partial a} \bar{A}_{aj} \boldsymbol{m}_{j\to a}^t = \boldsymbol{\omega}_{a\to i}^t + \bar{A}_{ai} \boldsymbol{m}_{i\to a}^t, \\ \boldsymbol{V}_a^t &:= \sum_{j\in\partial a} \bar{A}_{aj}^2 \boldsymbol{B}_{j\to a}^t = \boldsymbol{V}_{a\to i}^t + \bar{A}_{ai}^2 \boldsymbol{B}_{i\to a}^t, \\ \left(\boldsymbol{\Sigma}_i^t\right)^{-1} &:= \sum_{b\in\partial i} \bar{A}_{bi}^2 \left(\boldsymbol{V}_b^t\right)^{-1}. \end{aligned}$$

where we introduced a time index t to track the iteration count. Now we attempt to find a notion of total message $\boldsymbol{z}_i^t$ for $\boldsymbol{z}_{i\to a}^t$ such that the obtained set of equations becomes self consistent. Once $\boldsymbol{z}_i^t$ is found, then we define $\boldsymbol{m}_i^{t+1}$ and $\boldsymbol{B}_i^{t+1}$ as $\boldsymbol{\eta}(\boldsymbol{z}_i^t, \boldsymbol{\Sigma}_i^t)$ and $\mathrm{Diag}(\boldsymbol{\eta}(\boldsymbol{z}_i^t, \boldsymbol{\Sigma}_i^t)) - \boldsymbol{\eta}(\boldsymbol{z}_i^t, \boldsymbol{\Sigma}_i^t)\boldsymbol{\eta}(\boldsymbol{z}_i^t, \boldsymbol{\Sigma}_i^t)^\top$, respectively. Since $\boldsymbol{\Sigma}_{i\to a}^t - \boldsymbol{\Sigma}_i^t = \mathcal{O}(1/n)$ and $\boldsymbol{V}_{a\to i}^t - \boldsymbol{V}_a^t = \mathcal{O}(1/n)$, we have using (26)

$$\begin{aligned} \boldsymbol{z}_{i\to a}^t &= \boldsymbol{\Sigma}_{i\to a}^t \cdot \sum_{b\in\partial i\setminus a} \bar{A}_{bi} \left(\boldsymbol{V}_{b\to i}^t\right)^{-1} (\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_{b\to i}^t), \\ &\simeq \boldsymbol{\Sigma}_i^t \cdot \sum_{b\in\partial i\setminus a} \bar{A}_{bi} \left(\boldsymbol{V}_b^t\right)^{-1} (\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_{b\to i}^t). \end{aligned}$$

Substituting the expression $\boldsymbol{\omega}_{a\to i}^t = \boldsymbol{\omega}_a^t - \overline{A}_{ai}\boldsymbol{m}_{i\to a}^t$ in the above, we get

$$\begin{aligned}\boldsymbol{z}_{i\to a}^t &= \boldsymbol{\Sigma}_i^t \cdot \sum_{b\in\partial i\setminus a} \overline{A}_{bi}\left(\boldsymbol{V}_b^t\right)^{-1}(\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_b^t) + \boldsymbol{\Sigma}_i^t \cdot \sum_{b\in\partial i\setminus a} \overline{A}_{bi}^2\left(\boldsymbol{V}_b^t\right)^{-1}\boldsymbol{m}_{i\to b}^t \\ &\simeq \boldsymbol{\Sigma}_i^t \cdot \sum_{b\in\partial i} \overline{A}_{bi}\left(\boldsymbol{V}_b^t\right)^{-1}(\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_b^t) + \boldsymbol{\Sigma}_i^t \cdot \sum_{b\in\partial i} \overline{A}_{bi}^2\left(\boldsymbol{V}_b^t\right)^{-1}\boldsymbol{m}_{i\to b}^t,\end{aligned}$$

where we also allowed the above sums to run over all neighbors of i since the additional terms are of order $1/\sqrt{n}$ compared to the entire sum which is of order 1. Now we make the assumption that the messages $\boldsymbol{m}_{i\to b}^t$ are approximately equal for all $b \in \partial i$ to a common value $\boldsymbol{m}_i^t$, up to error $1/\sqrt{n}$. This assumption is justified by the fact that the graph is dense with equally strong edge weights, so the messages outgoing from every node are equal, up to first order. This simplifies the second term:

$$\boldsymbol{\Sigma}_i^t \cdot \sum_{b\in\partial i} \overline{A}_{bi}^2\left(\boldsymbol{V}_b^t\right)^{-1}\boldsymbol{m}_{i\to b}^t \simeq \boldsymbol{\Sigma}_i^t \cdot \sum_{b\in\partial i} \overline{A}_{bi}^2\left(\boldsymbol{V}_b^t\right)^{-1}\boldsymbol{m}_i^t = \boldsymbol{m}_i^t.$$

Based on these approximations, we define

$$\boldsymbol{z}_i^t := \boldsymbol{\Sigma}_i^t \cdot \sum_{b\in\partial i} \overline{A}_{bi}\left(\boldsymbol{V}_b^t\right)^{-1}(\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_b^t) + \boldsymbol{m}_i^t.$$

Now we treat $\boldsymbol{\omega}_a^t$. Recall $\boldsymbol{\omega}_a^t = \sum_{j\in\partial a}\overline{A}_{aj}\boldsymbol{m}_{j\to a}^t$, and $\boldsymbol{m}_{j\to a}^t = \boldsymbol{\eta}(\boldsymbol{z}_{j\to a}^{t-1}, \boldsymbol{\Sigma}_{j\to a}^{t-1})$. We write

$$\begin{aligned}\boldsymbol{z}_{j\to a}^{t-1} &= \boldsymbol{\Sigma}_{j\to a}^{t-1} \cdot \sum_{b\in\partial j} \overline{A}_{bj}\left(\boldsymbol{V}_{b\to j}^{t-1}\right)^{-1}(\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_{b\to j}^{t-1}) - \boldsymbol{\Sigma}_{j\to a}^{t-1}\cdot\overline{A}_{aj}\left(\boldsymbol{V}_{a\to j}^{t-1}\right)^{-1}(\bar{\boldsymbol{h}}_a - \boldsymbol{\omega}_{a\to j}^{t-1}), \\ &\simeq \boldsymbol{z}_j^{t-1} - \boldsymbol{\Sigma}_{j\to a}^{t-1}\cdot\overline{A}_{aj}\left(\boldsymbol{V}_a^{t-1}\right)^{-1}(\bar{\boldsymbol{h}}_a - \boldsymbol{\omega}_a^{t-1}).\end{aligned}$$

The second term is negligible compared to the first one, so we develop a first order Taylor approximation of the function $\boldsymbol{\eta}$ in the second term, and obtain

$$\begin{aligned}\boldsymbol{\omega}_a^t &= \sum_{j\in\partial a}\overline{A}_{aj}\boldsymbol{\eta}(\boldsymbol{z}_{j\to a}^{t-1}, \boldsymbol{\Sigma}_{j\to a}^{t-1}), \\ &\simeq \sum_{j\in\partial a}\overline{A}_{aj}\left(\boldsymbol{\eta}(\boldsymbol{z}_j^{t-1}, \boldsymbol{\Sigma}_j^{t-1}) - \frac{\mathrm{d}\boldsymbol{\eta}}{\mathrm{d}\boldsymbol{z}}(\boldsymbol{z}_{j\to a}^{t-1}, \boldsymbol{\Sigma}_{j\to a}^{t-1})\cdot\boldsymbol{\Sigma}_{j\to a}^{t-1}\cdot\overline{A}_{aj}(\boldsymbol{V}_a^{t-1})^{-1}(\bar{\boldsymbol{h}}_a - \boldsymbol{\omega}_a^{t-1})\right), \\ &= \sum_{j\in\partial a}\overline{A}_{aj}\boldsymbol{m}_j^t - \left(\sum_{j\in\partial a}\overline{A}_{aj}^2\frac{\mathrm{d}\boldsymbol{\eta}}{\mathrm{d}\boldsymbol{z}}(\boldsymbol{z}_{j\to a}^{t-1}, \boldsymbol{\Sigma}_{j\to a}^{t-1})\cdot\boldsymbol{\Sigma}_{j\to a}^{t-1}\right)(\boldsymbol{V}_a^{t-1})^{-1}(\bar{\boldsymbol{h}}_a - \boldsymbol{\omega}_{\boldsymbol{a}}^{t-1}).\end{aligned}$$

Based on the expression (29) of $\boldsymbol{\eta}$, one can easily check that

$$\frac{\mathrm{d}\boldsymbol{\eta}}{\mathrm{d}\boldsymbol{z}}(\boldsymbol{z}, \boldsymbol{\Sigma}) = \left(\mathrm{Diag}(\boldsymbol{\eta}(\boldsymbol{z}, \boldsymbol{\Sigma})) - \boldsymbol{\eta}(\boldsymbol{z}, \boldsymbol{\Sigma})\boldsymbol{\eta}(\boldsymbol{z}, \boldsymbol{\Sigma})^\top\right)\cdot\boldsymbol{\Sigma}^{-1},$$

hence

$$\sum_{j\in\partial a}\overline{A}_{aj}^2\frac{\mathrm{d}\boldsymbol{\eta}}{\mathrm{d}\boldsymbol{z}}(\boldsymbol{z}_{j\to a}^{t-1}, \boldsymbol{\Sigma}_{j\to a}^{t-1})\cdot\boldsymbol{\Sigma}_{j\to a}^{t-1} = \sum_{j\in\partial a}\overline{A}_{aj}^2\boldsymbol{B}_{j\to a}^t = \boldsymbol{V}_a^t.$$

We therefore end up with the following approximate message passing procedure:

$$\begin{cases} \boldsymbol{m}_i^{t+1} = \boldsymbol{\eta}(\boldsymbol{z}_i^t, \boldsymbol{\Sigma}_i^t), \\ \boldsymbol{B}_i^{t+1} = \mathrm{Diag}(\boldsymbol{\eta}(\boldsymbol{z}_i^t, \boldsymbol{\Sigma}_i^t)) - \boldsymbol{\eta}(\boldsymbol{z}_i^t, \boldsymbol{\Sigma}_i^t)\boldsymbol{\eta}(\boldsymbol{z}_i^t, \boldsymbol{\Sigma}_i^t)^\top, \\ \boldsymbol{\Sigma}_i^t = \left(\sum_{b \in \partial i} \bar{A}_{bi}^2 \left(\boldsymbol{V}_b^t\right)^{-1} \right)^{-1}, \\ \boldsymbol{z}_i^t = \boldsymbol{m}_i^t + \boldsymbol{\Sigma}_i^t \cdot \sum_{b \in \partial i} \bar{A}_{bi} \left(\boldsymbol{V}_b^t\right)^{-1} (\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_b^t), \\ \boldsymbol{\omega}_a^t = \sum_{j \in \partial a} \bar{A}_{aj} \boldsymbol{m}_j^t - \boldsymbol{V}_a^t \left(\boldsymbol{V}_a^{t-1}\right)^{-1} (\bar{\boldsymbol{h}}_a - \boldsymbol{\omega}_a^{t-1}), \\ \boldsymbol{V}_a^t = \sum_{j \in \partial a} \bar{A}_{aj}^2 \boldsymbol{B}_j^t. \end{cases}$$

This is rearranged to the AMP algorithm displayed in Section 2.1, with the notation $\hat{\boldsymbol{x}}_i^t$ replacing $\boldsymbol{m}_i^t$.

C State Evolution equations

We derive the state evolution equations from the Relaxed Belief Propagation (RBP) equations (28). Let $\boldsymbol{M}_t = \frac{1}{n}\sum_{i=1}^n \boldsymbol{m}_i^t \boldsymbol{x}_i^{*\top}$ and $\boldsymbol{Q}_t = \frac{1}{n}\sum_{i=1}^n \boldsymbol{m}_i^t \boldsymbol{m}_i^{t\top}$. As we argued in the previous section, we can redefine $\boldsymbol{M}_t$ and $\boldsymbol{Q}_t$ by substituting $\boldsymbol{m}_i^t$ by $\boldsymbol{m}_{i\to a}^t$ at the cost of an asymptotically vanishing error. In this section, we drop the time indices to lighten the notation. We expect the variance parameters $\boldsymbol{V}_{a\to i}$ in RBP to be concentrated about a constant:

$$\mathbb{E}[\boldsymbol{V}_{a\to i}] \simeq \sum_{j \neq i} \mathbb{E}[\bar{A}_{aj}^2] \boldsymbol{B}_{j\to a} = \frac{1}{n}\alpha(1-\alpha)\sum_{j\neq i} \boldsymbol{B}_{j\to a} = \alpha(1-\alpha)\boldsymbol{R},$$

with $\boldsymbol{R} := \frac{1}{n}\sum_j \boldsymbol{B}_{j\to a}$. A calculation of the second moment of $\boldsymbol{V}_{a\to i}$ reveals that it is equal to the expectation of $\boldsymbol{V}_{a\to i}$ plus a lower order term. Therefore we can safely assume that the quantities $\boldsymbol{V}_{a\to i}$ are essentially constant and equal to $\alpha(1-\alpha)\boldsymbol{R}$. Next, we deal with $\boldsymbol{\Sigma}_{i\to a}$. By assuming approximate independence of $\bar{A}_{bi}$ and $\boldsymbol{V}_{b\to i}$, we get

$$\mathbb{E}\left[\boldsymbol{\Sigma}_{i\to a}^{-1}\right] = \sum_{b\neq a} \mathbb{E}\left[\bar{A}_{bi}^2\right] \mathbb{E}\left[\boldsymbol{V}_{b\to i}^{-1}\right] = \frac{1}{n}\alpha(1-\alpha)\sum_{b\neq a} \frac{\boldsymbol{R}^{-1}}{\alpha(1-\alpha)} \simeq \kappa \boldsymbol{R}^{-1}.$$

We then make the approximation $\boldsymbol{\Sigma}_{i\to a}^{-1} \simeq \mathbb{E}[\boldsymbol{\Sigma}_{i\to a}^{-1}]$, i.e. $\boldsymbol{\Sigma}_{i\to a} \simeq \kappa^{-1}\boldsymbol{R}$. Next, we turn our attention to $\boldsymbol{z}_{i\to a}$:

$$\begin{aligned} \boldsymbol{z}_{i\to a} &= \boldsymbol{\Sigma}_{i\to a} \cdot \sum_{b\neq a} \bar{A}_{bi} \boldsymbol{V}_{b\to i}^{-1} (\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_{b\to i}) \\ &\simeq \frac{1}{\kappa\alpha(1-\alpha)} \sum_{b\neq a} \bar{A}_{bi} (\bar{\boldsymbol{h}}_b - \boldsymbol{\omega}_{b\to i}). \end{aligned}$$

Now using $\boldsymbol{\omega}_{b\to i} = \sum_{j\neq i} \bar{A}_{bj}\boldsymbol{m}_{j\to b}$ and $\bar{\boldsymbol{h}}_b = \sum_{j=1}^n \bar{A}_{bj}\boldsymbol{x}_j^*$, we get

$$\boldsymbol{z}_{i\to a} \simeq \frac{1}{\kappa\alpha(1-\alpha)} \sum_{b\neq a} \bar{A}_{bi} \left(\sum_{j\neq i} \bar{A}_{bj}(\boldsymbol{x}_j^* - \boldsymbol{m}_{j\to a}) + \bar{A}_{bi}\boldsymbol{x}_i^* \right).$$

The inner sum in the above expression involves n weakly independent terms, so we expect a central limit theorem to hold. Therefore the only relevant quantities are the expectation and the variance of $\boldsymbol{z}$: $\mathbb{E}[\boldsymbol{z}_{i\to a}] = \boldsymbol{x}_i^*$, and

$$\begin{aligned}
\mathbb{E}[(\boldsymbol{z}_{i\to a} - \boldsymbol{x}_i^*)(\boldsymbol{z}_{i\to a} - \boldsymbol{x}_i^*)^\top] &= \frac{1}{(\kappa\alpha(1-\alpha))^2} \sum_{b\neq a}\sum_{j\neq i}\sum_{b'\neq a}\sum_{j'\neq i} \mathbb{E}[\bar{A}_{bi}\bar{A}_{b'i}]\,\mathbb{E}[\bar{A}_{bj}\bar{A}_{bj'}] \\
&\qquad \times (\boldsymbol{x}_j^* - \boldsymbol{m}_{j\to a})(\boldsymbol{x}_j^* - \boldsymbol{m}_{j\to a})^\top \\
&= \frac{1}{(\kappa\alpha(1-\alpha))^2} \sum_{b\neq a}\sum_{j\neq i} \frac{(\alpha(1-\alpha))^2}{n^2} (\boldsymbol{x}_j^* - \boldsymbol{m}_{j\to a})(\boldsymbol{x}_j^* - \boldsymbol{m}_{j\to a})^\top \\
&= \kappa^{-2}\frac{m}{n}\frac{1}{m}\sum_{b\neq a}\frac{1}{n}\sum_{j\neq i}(\boldsymbol{x}_j^* - \boldsymbol{m}_{j\to a})(\boldsymbol{x}_j^* - \boldsymbol{m}_{j\to a})^\top \\
&\simeq \kappa^{-1}(\boldsymbol{D} - \boldsymbol{M} - \boldsymbol{M}^\top + \boldsymbol{Q}),
\end{aligned}$$

with $\boldsymbol{D} = \frac{1}{n}\sum_{i=1}^n \boldsymbol{x}_i^*\boldsymbol{x}_i^{*\top} = \mathrm{Diag}(\boldsymbol{\pi})$. Hence, we define

$$\boldsymbol{X} := \kappa^{-1}(\boldsymbol{D} - \boldsymbol{M} - \boldsymbol{M}^\top + \boldsymbol{Q}).$$

Therefore we have made the assumption that $\boldsymbol{z}_{i\to a} \sim \mathcal{N}(\boldsymbol{x}_i^*, \boldsymbol{X})$. Next, we assume that the $\boldsymbol{z}_{i\to a}$ are "independent enough" that a law of large numbers holds in limit $n\to\infty$, $m/n\to\kappa$:

$$\frac{1}{n}\sum_{i:\boldsymbol{x}_i^*=\boldsymbol{e}_r} \boldsymbol{m}_{i\to a} = \frac{1}{n}\sum_{i:\boldsymbol{x}_i^*=\boldsymbol{e}_r} \boldsymbol{\eta}(\boldsymbol{z}_{i\to a}, \boldsymbol{\Sigma}_{i\to a}) \simeq \pi_r\,\mathbb{E}_{\boldsymbol{g}}\left[\boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}^{\frac{1}{2}}\boldsymbol{g}, \kappa^{-1}\boldsymbol{R})\right],$$

and

$$\frac{1}{n}\sum_{i:\boldsymbol{x}_i^*=\boldsymbol{e}_r} \boldsymbol{m}_{i\to a}\boldsymbol{m}_{i\to a}^\top \simeq \pi_r\,\mathbb{E}_{\boldsymbol{g}}\left[\boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}^{\frac{1}{2}}\boldsymbol{g}, \kappa^{-1}\boldsymbol{R})\cdot\boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}^{\frac{1}{2}}\boldsymbol{g}, \kappa^{-1}\boldsymbol{R})^\top\right],$$

for all $r\in\{1,\cdots,d\}$, with $\boldsymbol{g}\sim\mathcal{N}(\boldsymbol{0},\boldsymbol{I})$. Plugging the above into $\boldsymbol{M}$ and $\boldsymbol{Q}$ yields

$$\begin{aligned}
\boldsymbol{M} &= \frac{1}{n}\sum_{i=1}^n \boldsymbol{\eta}(\boldsymbol{x}_i^* + \boldsymbol{X}^{\frac{1}{2}}\boldsymbol{g}, \kappa^{-1}\boldsymbol{R})\boldsymbol{x}_i^{*\top}, \\
&\simeq \sum_{r=1}^d \pi_r\,\mathbb{E}_{\boldsymbol{g}}\left[\boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}^{\frac{1}{2}}\boldsymbol{g}, \kappa^{-1}\boldsymbol{R})\right]\boldsymbol{e}_r^\top, \\
\boldsymbol{Q} &= \frac{1}{n}\sum_{i=1}^n \boldsymbol{\eta}(\boldsymbol{x}_i^* + \boldsymbol{X}^{\frac{1}{2}}\boldsymbol{g}, \kappa^{-1}\boldsymbol{R})\cdot\boldsymbol{\eta}(\boldsymbol{x}_i^* + \boldsymbol{X}^{\frac{1}{2}}\boldsymbol{g}, \kappa^{-1}\boldsymbol{R})^\top, \\
&\simeq \sum_{r=1}^d \pi_r\,\mathbb{E}_{\boldsymbol{g}}\left[\boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}^{\frac{1}{2}}\boldsymbol{g}, \kappa^{-1}\boldsymbol{R})\cdot\boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}^{\frac{1}{2}}\boldsymbol{g}, \kappa^{-1}\boldsymbol{R})^\top\right].
\end{aligned}$$

Finally, it remains to find an expression for $\boldsymbol{R}$. Recall $\boldsymbol{B}_{i\to a} = \mathrm{Diag}(\boldsymbol{m}_{i\to a}) - \boldsymbol{m}_{i\to a}\boldsymbol{m}_{i\to a}^\top$. Averaging over i and using the assumed concentration of the messages $\boldsymbol{m}_{i\to a}$ yields

$$\begin{aligned}
\boldsymbol{R} = \frac{1}{n}\sum_{i=1}^n \boldsymbol{B}_{i\to a} &\simeq \mathrm{Diag}\left(\sum_{r=1}^d \pi_r\,\mathbb{E}_{\boldsymbol{g}}\left[\boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}^{\frac{1}{2}}\boldsymbol{g}, \kappa^{-1}\boldsymbol{R})\right]\right) - \boldsymbol{Q}, \\
&= \mathrm{Diag}(\boldsymbol{Q}\boldsymbol{1}) - \boldsymbol{Q}.
\end{aligned}$$

To sum up, we get a system of self-consistent equations in $\boldsymbol{M}_t$, $\boldsymbol{Q}_t$, $\boldsymbol{X}_t$ and $\boldsymbol{R}_t$:

$$\begin{cases} \boldsymbol{M}_{t+1} = \sum_{r=1}^{d} \pi_r \, \mathbb{E}_{\boldsymbol{g}} \left[\boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}_t^{\frac{1}{2}} \boldsymbol{g}, \kappa^{-1} \boldsymbol{R}_t) \right] \cdot \boldsymbol{e}_r^\top, \\ \boldsymbol{Q}_{t+1} = \sum_{r=1}^{d} \pi_r \, \mathbb{E}_{\boldsymbol{g}} \left[\boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}_t^{\frac{1}{2}} \boldsymbol{g}, \kappa^{-1} \boldsymbol{R}_t) \cdot \boldsymbol{\eta}(\boldsymbol{e}_r + \boldsymbol{X}_t^{\frac{1}{2}} \boldsymbol{g}, \kappa^{-1} \boldsymbol{R}_t)^\top \right], \\ \boldsymbol{X}_t \quad = \kappa^{-1}(\boldsymbol{D} - \boldsymbol{M}_t - \boldsymbol{M}_t^\top + \boldsymbol{Q}_t), \\ \boldsymbol{R}_t \quad = \mathrm{Diag}(\boldsymbol{Q}_t \mathbf{1}) - \boldsymbol{Q}_t. \end{cases}$$

This set of equations constitute the State Evolution equations.