Properties of Sparse Random Matrices over Finite Fields

Roberto C. Alamino and David Saad

Neural Computing Research Group, Aston University, Birmingham B4 7ET, UK

PACS numbers: 02.10.Yn, 02.70.-c, 05.10.-a

Abstract. Typical properties of sparse random matrices over finite (Galois) fields are studied, in the limit of large matrices, using techniques from the physics of disordered systems. We present results for the average kernel dimension, the number of matrices for a given distribution of entries, and average dimension of the eigenvector spaces and the distribution of the eigenvalues. The significance of these results to error-correcting codes and random graphs is also discussed.

1. Introduction

Random matrices are ubiquitous in many branches of the natural sciences and mathematics ranging from biology to computer science, nuclear physics and quantum chaos. Activity in the area has been recently boosted by the application of techniques originated in the statistical mechanics of disordered systems [1, 2, 3, 4, 5, 6]. These techniques have been used to analyse ensemble properties, including variational techniques and the replica method, have proved to be valuable tools in several of these approaches. Most of the research concentrates on real matrices, while the restriction to matrices over $GF(q)$ considered here makes the solution of the problem more involved. Random matrices over $GF(q)$ are specially important in coding theory [7] where, for instance, linear codes are defined by the kernel of the so-called parity-check matrix: each kernel vector defines a codeword to which the original message vector is mapped by a linear operation, in the form of a product with a generator matrix. Well known examples include the Hadamard codes, where properties of the kernel and rank play an important role [8], and low-density parity-check codes (LDPC), which provide the best performance to date in many noise regimes; parity-check matrices are constructed using a special case of the sparse matrices studied here. Although the most studied and applied case of LDPC codes is of binary codes over $GF(2)$ there is a significant body of work, of both practical and theoretical nature [9], on codes over more general finite fields showing an improvement in performance with respect to the binary version. A statistical physics based analysis of LDPC codes over $GF(q)$ has been reported, for instance, in [10].

In addition to being an interesting applied problem, properties of these matrices are of great interest from the pure mathematical point of view and a number of papers have already addressed related questions, in different instances, with a mathematical rigorous approach [11, 12, 13].

Here, we analyse key typical properties of sparse random matrices over $GF(q)$, namely the average dimension of their kernel, the average dimension of the eigenvector spaces, the eigenvalue distributions and the number of matrices for a given connectivity distribution, all in the case of *large matrices*. When the $M \times N$ matrices are large, keeping $N \to \infty$ with $\eta = M/N$ constant, the problem can be mapped into a system of interacting "spins" by a very useful group homomorphism, and the powerful methodology developed for the study of disordered spin lattices in condensed matter physics can then be used, under some assumptions, to obtain the required properties.

In section 2, we generalise a usual statistical physics mapping of systems over the binary field $GF(2)$ to spin system by means of a group homeomorphism in such a way that it can be efficiently applied to any $GF(q)$ allowing for the calculation in sections 3 and 5 of kernel and eigenspace properties, respectively, to be carried out. Making use of these techniques, the number of matrices for a given distribution of non-zero elements is then obtained for various connectivity profiles, in section 6. In section 4 we discuss the importance of the results to LDPC error-correcting codes and in section 7 to general

random graphs. We present a final discussion of the results in section 8.

2. Generalised Mapping of $GF(q)$ onto Spin Systems

A Galois field $GF(q)$ is a finite field with q elements, i.e., a set of q elements $\{0, ..., q-1\}$, which we symbolise by integers for convenience, which is a commutative group under addition $\oplus : GF(q) \to GF(q)$, defined as integer addition *mod* q, and with a monoid structure with respect to a commutative multiplication operation $\otimes : GF(q) \to GF(q)$. The field also includes the zero element '0' and the multiplicative identity '1'. The additional requirement that both multiplication and addition have the algebraic distributive property restricts the number of elements to $q = p^n$, where p is a prime number and n an integer.

In statistical physics applications to information theory, it is usually convenient to map binary vectors with entries from the set $\{0, 1\}$, into what we call "spin" vectors with entries from the set $\{\pm 1\}$. Given an entry $v \in \{0, 1\}$, this mapping is usually accomplished either by the transformation $\sigma(v) = 2v - 1$ or by $\sigma(v) = (-1)^v$. Note that these two transformations are different in the sense that in the former, 0 is mapped to -1 and 1 is mapped to 1, while in the latter the order is reversed. The second mapping is much more convenient as it represents a homeomorphism between representations of $GF(2)$. A further advantage, which we show below, is that this map can also be generalised to any $GF(q)$ allowing the straightforward use of statistical physics techniques to a wide range of problems over Galois fields.

The main fact to be noted is that, under the operation of addition $\oplus$, $GF(q)$ is homeomorphic to the cyclic group of order q and therefore has a representation as the complex q-th roots of unity with the group homeomorphism $\sigma : GF(q) \to \mathbb{C}$ given by

$$\sigma(v) = \exp\left(\frac{2\pi i}{q} v\right), \tag{1}$$

such that for every $v_1, v_2 \in GF(q)$

$$\begin{aligned} \sigma(v_1 \oplus v_2) &= \exp\left[\frac{2\pi i}{q}(v_1 \oplus v_2)\right] \\ &= \exp\left[\frac{2\pi i}{q}(v_1 + v_2)\right] \\ &= \sigma(v_1)\sigma(v_2). \end{aligned} \tag{2}$$

This mapping has a clear geometric interpretation where $2\pi v/q$ is an angle in the unit circle, such that each element of the Galois field is being mapped onto a spin variable "pointing" in one of q possible directions. Let us denote the inverse of an element v under addition by $-v$ such that $v \oplus (-v) = 0$. Then we also have

$$\sigma(v \oplus (-v)) = \sigma(0) = 1 \Rightarrow \sigma(-v) = [\sigma(v)]^{-1}, \tag{3}$$

$$\sigma(v \oplus (-u)) = \sigma(v)\sigma(-u) = \sigma(v)[\sigma(u)]^{-1}. \tag{4}$$

In several applications, including the ones studied in this paper, it turns out to be necessary to use constraints in the form of Kroenecker deltas like

$$\delta(v,u) = \delta(v \oplus (-u), 0). \tag{5}$$

Using the above mapping, one can write any constraint of this type in a generalised way as

$$\delta(v,u) = \frac{1}{q}\prod_{m=1}^{q-1}\left[1 - \exp\left(-\frac{2\pi i}{q}m\right)\exp\left(\frac{2\pi i}{q}v\right)\exp\left(-\frac{2\pi i}{q}u\right)\right]. \tag{6}$$

Also based on this representation, we can now define the k-point functions of the spins by

$$m_k \equiv \frac{1}{N}\sum_{j=1}^{N}\sigma_1^j\cdots\sigma_k^j, \tag{7}$$

where the lower indices represent k different spin configurations $\boldsymbol{\sigma}_1, ..., \boldsymbol{\sigma}_k$. Note that we are now working with the spin variables already mapped onto the complex field $\mathbb{C}$ and therefore the operations of multiplication and addition correspond to the usual ones on $\mathbb{C}$. The first two k-point functions, namely m_1 and m_2, correspond to the magnetisation of the spin system and its overlap between two configurations, respectively.

As will become evident in what follows, this kind of representation allows a factorisation of terms that simplifies the equations and makes replica calculations simpler.

3. Kernel and Rank

Entries in matrices over $GF(q)$ take values of elements of that finite field, where the usual additions and multiplications involved in their algebra are defined by the corresponding operations over the Galois field.

The kernel of an $M \times N$ matrix A over $GF(q)$ is a linear space with dimension $d_A(0) = \log_q \Omega_A(0)$ where

$$\Omega_A(0) = \sum_{\mathbf{v}}\delta(A\mathbf{v}, 0), \tag{8}$$

is the number of vectors in the kernel, δ is the Kroenecker delta and $\mathbf{v} \in GF(q)^N$.

We term $Ts(0)$ the *average kernel dimension density*, in the limit of large matrices, where we also define the *entropy density*

$$s(0) \equiv \frac{1}{T}\lim_{N\to\infty}\frac{\langle d_A(0)\rangle_A}{N} = \lim_{N\to\infty}\frac{1}{N}\langle \ln \Omega_A(0)\rangle_A, \tag{9}$$

with $1/T = \ln q$ and with the ratio $\eta = M/N$ being a finite positive constant and $\langle\cdot\rangle_A$ denotes an average over the corresponding ensemble of random matrices. Using the replica trick we can write the entropy density as

$$s(0) = \lim_{N\to\infty}\left[\frac{\partial}{\partial n}\ln\langle\Omega_A^n(0)\rangle_A\right]_{n=0}. \tag{10}$$

We focus our analysis on the class of randomly chosen sparse matrices A having exactly K_i non-zero elements in the i-th row with probability $\mathcal{P}(\mathbf{K})$, $\mathbf{K} \equiv (K_1, ..., K_M)$, and C_j elements in the j-th column with probability $\mathcal{P}(\mathbf{C})$, $\mathbf{C} \equiv (C_1, ..., C_N)$, obeying the constraint $\Lambda \equiv \sum_i K_i = \sum_j C_j$, where Λ is the total number of non-zero elements of the matrix. We also consider that the elements of A are sampled from the finite field $GF(q)$ with independent equal probabilities $\mathcal{P}(A_{ij})$.

Using the mapping of $GF(q)$ into spin variables defined in the previous section, the replicated averaged partition function $\mathcal{Z}_n(0) \equiv \langle \Omega_A^n(0) \rangle_A$ can be written as

$$\mathcal{Z}_n(0) = \left\langle \frac{1}{\mathcal{N}} \sum_{\{A_{ij}\}} \left[\prod_{i,j} \mathcal{P}(A_{ij}) \right] \left[\prod_{i=1}^{M} \delta\left(\sum_{j=1}^{N} \chi(A_{ij}), K_i \right) \right] \left[\prod_{j=1}^{N} \delta\left(\sum_{i=1}^{M} \chi(A_{ij}), C_j \right) \right] \times \prod_{a=1}^{n} \left[\sum_{\mathbf{v}_a} \delta(A\mathbf{v}_a, 0) \right] \right\rangle_{\mathbf{K},\mathbf{C},\Lambda}, \tag{11}$$

where the average is over the probability distribution $\mathcal{P}(\mathbf{K}, \mathbf{C}, \Lambda)$ with $\chi(A_{ij}) = 0$ if $A_{ij} = 0$ and 1 otherwise, and the normalisation $\mathcal{N}$ gives the number of matrices which obey the constraints averaged over the distributions of the entries. The replica calculations to obtain the entropy (9) have already been carried out in a previous paper [14] and we will only discuss the important results. One important difference of this approach in comparison to previous similar calculations [15, 16] is that, instead of defining connectivity tensors and summing over them, here and in [14] we sum directly over the matrices entries, which makes possible to include general constraints over the class of random matrices.

Using the rank-nullity theorem, we can define the *free energy density* $f(0)$ as the *average rank density* in the form

$$f(0) \equiv \frac{\langle r(A) \rangle_A}{N} = 1 - Ts(0), \tag{12}$$

which implies that the *internal energy density* of the associated statistical mechanical model should be constrained to be $u = 1$. Defining the inverse temperature $\beta = 1/T$, equation (12) can be written as

$$\beta f(0) = -\frac{1}{N} \left\langle \ln \sum_{\mathbf{v}} e^{-\beta \mathcal{H}(\mathbf{v})} \right\rangle_A, \tag{13}$$

where a formal Hamiltonian can be written as

$$\mathcal{H}(\mathbf{v}) \equiv N - \ln \delta(A\mathbf{v}, 0). \tag{14}$$

The solution given by the replica calculations [14] has the striking property of being *completely independent* of the specific distribution of the individual elements of the matrix $\mathcal{P}(A_{ij})$, depending only on the distribution of $\mathbf{K}$ and $\mathbf{C}$ (and, obviously, that

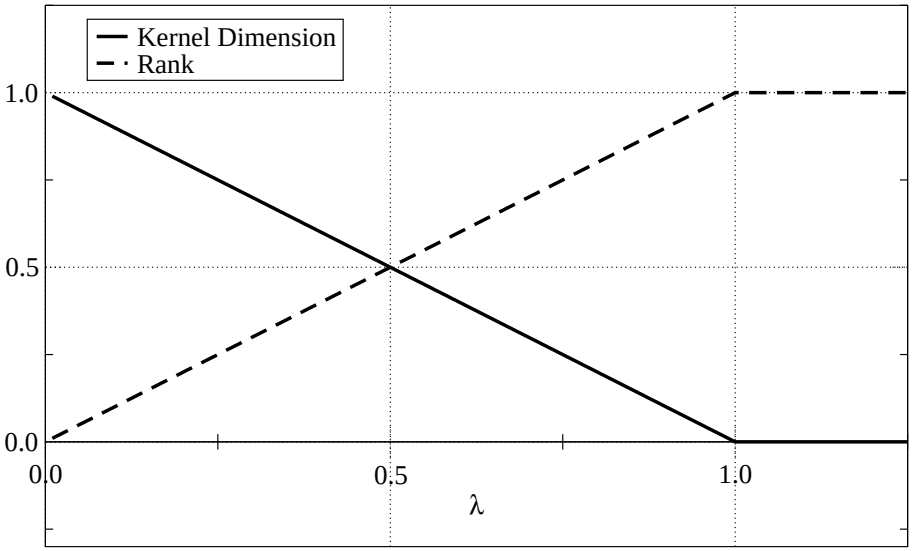


Figure 1. Average kernel dimension density (continuous lines) and average rank density (dashed lines) calculated as solutions to the replica symmetric saddle point equations. The plot shows the thermodynamically favoured analytical solution which is paramagnetic for $0 \leq \eta \leq 1$ and ferromagnetic for $\eta > 1$.

of Λ). Analytical solutions cannot be obtained in general and we must rely on numerical methods to obtain them. However, there exists two straightforward analytical solutions, the paramagnetic and ferromagnetic states. The paramagnetic solution gives the average kernel density as $Ts(0) = 1 - \eta = 1 - M/N$ independently of the order q of the finite field used, and the ferromagnetic solution gives simply $Ts(0) = 0$. Figure 1 shows a plot of the thermodynamically dominant solutions for varying η. We see that the paramagnetic solution dominates until $\eta = 1$, after which it becomes unphysical and the correct solution is given by the ferromagnetic one.

In [14], numerical solutions for three different distributions of $\mathbf{K}$, $\mathbf{C}$ and Λ were thoroughly studied and, apart from small variations resulting from particular properties of the distributions, the obtained curves seem to reproduce figure 1.

4. Error Correcting Codes

Low-density parity-check codes are linear codes where the codewords are defined by the kernel of a random sparse matrix, called the parity-check matrix. In most studies of LDPC codes, it is assumed that a parity-check matrix with M rows (parity-checks) and N columns *exactly* defines a code of rate $R = 1 - M/N = 1 - \eta$, which is equivalent to the assertion that the number of codewords (vector in the kernel) is exactly q^{NR}.

The results of the previous section give us a method to rigorously test this assertion. Note that when $M \geq N$, the code rate, in the case of unbiased messages, would be negative, which is unphysical. However, our calculations give a clear interpretation for this case as they show that if $\eta > 1$, the dominant solution is the ferromagnetic one with $Ts = 0$, implying that the matrix is full rank. As the kernel would be only given by

the zero message, this incidentally means that such matrices cannot be used to define a parity-check code due to the lack of redundancy.

However, when $\eta < 1$, the dominant solution is paramagnetic and the typical parity-check matrix defines a code of rate exactly $(N-M)/N$. This is assumed for any parity-check matrix in most calculations in the literature and is confirmed by our results to be true on average; however, it is important to point out that the result is true in the limit of large matrices and is likely to have finite size corrections which may affect practical applications.

The application to error correcting codes also gives support to our conjecture that the dominant solution for $\eta < 1$ is the paramagnetic one and for $\eta \geq 1$ it is the ferromagnetic solution for any distribution. The argument is that the solution of the kernel dimension is mathematically equivalent to the solution of LDPC in channels with infinite noise, which then leads to this behaviour. As already mentioned, the numerical results of [14] seem to support this conjecture, although more careful calculations, varying all the parameters involved must be carried out to confirm this hypothesis more generally.

5. Eigenspaces and Eigenvalues

In the case of square $M \times M$ matrices, which means that $\eta = 1$, we can generalise equation (8) to count the number of vectors in an eigenspace with eigenvalue $\lambda \in \{1, ..., q-1\}$ as

$$\Omega_A(\lambda) = \sum_{\mathbf{v}} \delta(A\mathbf{v}, \lambda\mathbf{v}), \tag{15}$$

with obvious analogous generalisations for the kernel dimension density $d_A(\lambda)$, its average density $Ts(\lambda)$ and all other quantities from section 3 that depend on λ, the free energy now being the dimension of the complementary space to the λ-eigenspace.

The replica calculations are very similar to the particular case of the kernel [14]. However, as there are key differences and in order to keep this paper as self-contained as possible, we reproduce the replica calculations including the appropriate changes to the eigenspace case in Appendix A. The replica symmetric solution, exact for this problem as shown in Appendix B, is therefore (for $\lambda \neq 0$)

$$\begin{aligned} s(\lambda) = &- \ln q - \frac{\alpha}{M} \langle \ln \left[1 + (q-1) x \hat{x} \right] \rangle_{x,\hat{x}} \\ &+ \frac{1}{M\epsilon(\alpha)} \sum_i \left\langle \frac{\alpha^\Lambda}{\Lambda!} \left\langle \ln \left\{ \left[1 + (q-1) \prod_{l=1}^{K_i} x_l \right] \prod_{l=1}^{C_i} \left[1 + (q-1)\hat{x}_l \right] \right. \right. \right. \\ &\left. \left. \left. + \ (q-1) \left(1 - \prod_{l=1}^{K_i} x_l \right) \prod_{l=1}^{C_j} (1 - \hat{x}_l) \right\} \right\rangle_{\mathbf{x},\hat{\mathbf{x}}} \right\rangle_{\mathbf{K},\mathbf{C},\Lambda}, \end{aligned} \tag{16}$$

where now the distributions of the auxiliary fields $\mathbf{x}$ and $\hat{\mathbf{x}}$ are slightly more complicated

than in the kernel case and are given by the saddle point equations

$$\hat{\pi}(\hat{x}) = \frac{1}{\alpha\epsilon(\alpha)} \sum_{i=1}^{M} \left\langle \frac{\alpha^{\Lambda}}{\Lambda!} K_i \times \delta\left(\hat{x} - \left[\prod_{l=1}^{K_i - 1} x_l \right] \frac{\hat{X}^{+}(C_i) - \hat{X}^{-}(C_i)}{\hat{X}^{+}(C_i) + (q-1)\hat{X}^{-}(C_i)} \right) \right\rangle_{\hat{\mathbf{x}},\mathbf{K},\mathbf{C},\Lambda}, \tag{17}$$

$$\pi(x) = \frac{1}{\alpha\epsilon(\alpha)} \sum_{i=1}^{M} \left\langle \frac{\alpha^{\Lambda}}{\Lambda!} C_i \times \delta\left(x - \frac{X^{+}(K_i)\hat{X}^{+}(C_i - 1) - X^{-}(K_i)\hat{X}^{-}(C_i - 1)}{X^{+}(K_i)\hat{X}^{+}(C_i - 1) + (q-1)X^{-}(K_i)\hat{X}^{-}(C_i - 1)} \right) \right\rangle_{\hat{\mathbf{x}},\mathbf{K},\mathbf{C},\Lambda}, \tag{18}$$

$$0 = \left\langle \frac{\alpha^{\Lambda}}{\Lambda!} \left(1 - \frac{\Lambda}{\alpha} \right) \right\rangle_{\mathbf{K},\mathbf{C},\Lambda}, \tag{19}$$

with the following definitions for simplicity

$$\epsilon(\alpha) \equiv \left\langle \frac{\alpha^{\Lambda}}{\Lambda!} \right\rangle_{\mathbf{K},\mathbf{C},\Lambda}, \tag{20}$$

$$\hat{X}^{+}(C) \equiv \prod_{l=1}^{C} [1 + (q-1)\hat{x}_l], \qquad \hat{X}^{-}(C) \equiv \prod_{l=1}^{C} (1 - \hat{x}_l), \tag{21}$$

$$X^{+}(K) \equiv 1 + (q-1) \prod_{l=1}^{K} x_l, \qquad X^{-}(K) \equiv 1 - \prod_{l=1}^{K} x_l. \tag{22}$$

The paramagnetic solution

$$\hat{\pi}(\hat{x}) = \delta(\hat{x}),\ \pi(x) = \delta(x), \tag{23}$$

and the ferromagnetic solution

$$\hat{\pi}(\hat{x}) = \delta(\hat{x} - 1),\ \pi(x) = \delta(x - 1). \tag{24}$$

in terms of the auxiliary fields are the same as for the kernel. Substituting these solutions into equation (16), we see that the paramagnetic solution gives the result $s(\lambda) = 0$ for every value of λ, which must be discarded as the kernel calculation shows that $s(0) = 0$ in the square matrix case. The matrix is therefore diagonalisable and the dimension of the eigenspaces cannot be zero. On the other hand the ferromagnetic solution gives $s(0) = 0$ and $s(\lambda) = \Lambda/M$ for $\lambda \neq 0$, which means that all the non-zero eigenvalues have eigenspaces with the same dimension given by the average value of non-zero entries per row or per column (both must be equal). As Λ scales with M; it gives a finite average dimension density as expected. This result also implies that the eigenvalue distribution is just given by

$$\mathcal{P}(\lambda) = (q-1)^{-1}, \tag{25}$$

for $\lambda \neq 0$, i.e., all eigenvalues have the same probability.

6. Number of Matrices

The number of $GF(q)$ matrices given a connectivity profile is of significant interest within the discrete mathematics community. Exact results have been obtained for the case of *finite* binary matrices [17] in the form of a formula that facilitates the calculation of their precise number. Using the same techniques from the previous sections, this number and its average value can be obtained for large $GF(q)$ matrices. For a given number of non-zero elements per row $\mathbf{K} = (K_1, ..., K_M)$ and per column $\mathbf{C} = (C_1, ..., C_N)$, the number of matrices is

$$N_A = \sum_{\{A_{ij}\}} \left[\prod_{i=1}^{M} \delta\left(\sum_{j=1}^{N} \chi(A_{ij}), K_i\right)\right] \left[\prod_{j=1}^{N} \delta\left(\sum_{i=1}^{M} \chi(A_{ij}), C_j\right)\right], \tag{26}$$

where again we are summing directly over the entries of the matrix instead of over a connectivity tensor. The detailed calculations where presented in [14] resulting in

$$N_A = (q-1)^{\Lambda} \frac{\Lambda!}{\prod_i K_i! \prod_j C_j!}, \tag{27}$$

which is just the number of binary matrices with the given non-zero elements profile times a factor $(q-1)^{\Lambda}$ which is the multiplicity of the non-zero entries.

The *average* number of matrices is then

$$\begin{aligned} \bar{N}_A &= \left\langle (q-1)^{\Lambda} \frac{\Lambda!}{\prod_i K_i! \prod_j C_j!} \right\rangle_{\mathbf{K},\mathbf{C},\Lambda} \\ &= \sum_{\mathbf{K}} \sum_{\mathbf{C}} \mathcal{P}(\mathbf{K}|\mathbf{C}) \mathcal{P}(\mathbf{C}) (q-1)^{\sum_j C_j} \frac{\left(\sum_j C_j\right)!}{\prod_i K_i! \prod_j C_j!}, \end{aligned} \tag{28}$$

where the distribution $\mathcal{P}(\mathbf{K}|\mathbf{C})$ includes the constraint $\delta\left(\sum_i K_i, \sum_j C_j\right)$. For a regular matrix, it is easy to see that this number scales as N^{CN} and a more appropriate quantity would be the quenched entropy

$$\Xi \equiv \left\langle \frac{1}{N} \ln N_A \right\rangle = \frac{1}{N} \sum_{\mathbf{K}} \sum_{\mathbf{C}} \mathcal{P}(\mathbf{K}|\mathbf{C}) \mathcal{P}(\mathbf{C}) \ln \left[(q-1)^{\sum_j C_j} \frac{\left(\sum_j C_j\right)!}{\prod_i K_i! \prod_j C_j!} \right], \tag{29}$$

scaling as $\ln N$.

A detailed numerical analysis of these formulas for different distributions is also given in [14]. These studies indicate that if we keep the number of columns constant and increase the ratio η by adding rows, whenever the number of rows is much larger than the number of columns, the average number of matrices becomes independent of both the ratio and number of rows and also suggest that the average number of matrices in these cases is basically defined by the average value of the $\mathbf{C}$ distributions.

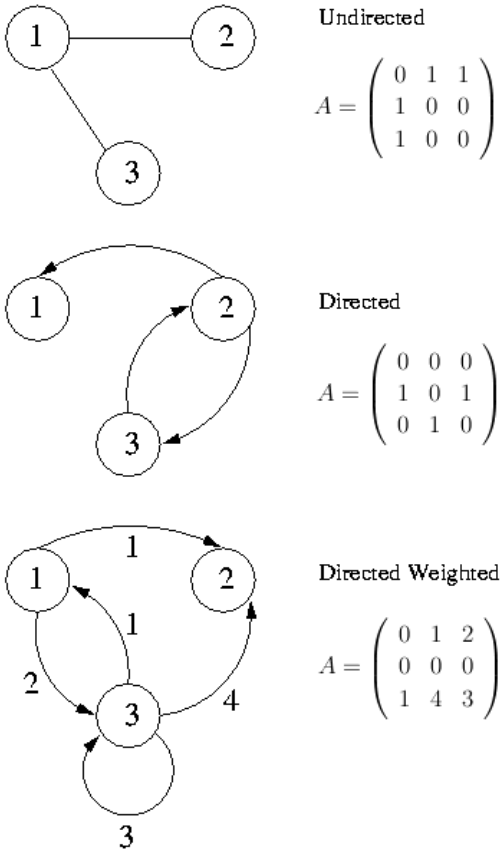
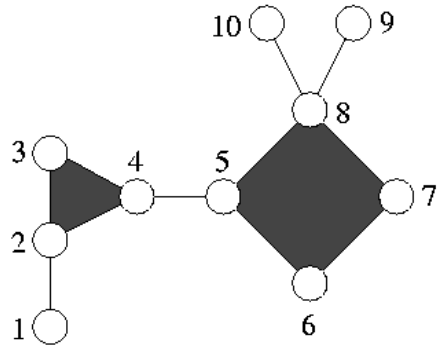


Figure 2. Examples of adjacency matrices. From top to bottom, undirected graphs, directed graphs and directed weighted graphs.

7. Random Graphs

The results of the previous section can be used to obtain the number and average number of generalised sparse random graphs. For usual random graphs, directed or undirected, the adjacency matrix can be written as a binary matrix with a 1 in entry A_{ij} if there is a link from vertex i to vertex j. If in addition each link is given an integer weight, the matrix can be viewed as a $GF(q)$ matrix for the sake of counting the graphs. In figure 2, we give an example of a directed, an undirected and an undirected weighted graph.

Graphs like the ones in figure 2 can be used in statistical physics to describe systems with 2-body interactions, like an Ising model, for instance. However, there exists systems with many-body interactions and we would like to be able to describe them by graphs and matrices as well. With this in mind, we can generalise random graphs in the following way. Instead of only links that connect two vertices, representing an interaction between them, we allow for the existence of polygons connecting $p \geq 3$ vertices with a p-body interaction. This graph construction can then be codified by a binary matrix in which each line represent a group of interacting vertices (spins, for instance) and each



$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Figure 3. Example of a graph with p-spin interactions and its matrix representation.

row carries the label of the vertices. This is the type of representation frequently used in most studies of codes [18]. An example of such a graph is given in figure 3. In fact this is a matrix representation of the tensor whose indices identify the interacting variables.

In this way, we can represent any interacting system as a random $GF(q)$ matrix, which allows us to use the results of the former section to calculate their number or their average number according to our needs.

8. Conclusions

The main object of this work was to study some typical properties of sparse random matrices over Galois fields using techniques originated in the statistical physics of disordered systems.

In order to carry on our analysis, we introduced a mapping from Galois matrices to spin systems based on the group homeomorphism between $GF(q)$ under addition mod q (denoted by $\oplus$) and the complex q-th roots of unity. This mapping allows for a direct analogy between the matrices and statistical mechanical systems in the canonical ensemble, making it possible to associate properties like rank and nullity with thermodynamical characteristic functions like the free-energy and entropy.

The key point, which is the calculation of the quenched entropy, was carried out in a set up that allows for further generalisations of the constraints enforced in defining the classes of matrices over which the averaging is done by characterising their connectivity profiles. This quenched average is carried out using the replica approach and we are able to obtain, as a result, the average dimension of the kernel for a general distribution of non-zero entries. Solving the resulting equations numerically, we find that the average kernel density is $1 - M/N$ in all cases studied. We conjecture that this result is always valid. The replica symmetric ansatz was assumed in the calculation and later on proved to be exact in this case with the help of the mapping between matrices and spin systems; this sheds light on the meaning of properties like magnetisation and spin correlation.

The above results have practical relevance in a number of areas, including coding and network modelling. With respect to LDPC codes, the average kernel density result

implies that randomly generated LDPC codes typically define codes of rate exactly $1 - M/N$, an assumption which is generally made but lacks rigorous derivation.

A generalisation of the result for the kernel and rank allowed us to obtain the dimension of each eigenspace and its corresponding eigenvalue distribution.

By using the same mathematical techniques, we were also able to find the total number of large matrices for fixed $\mathbf{K}$ and $\mathbf{C}$, row and column connectivities, respectively, and their average number. We showed then how the matrices could be used to represent not only usual graphs, but also the connectivity profile of graphs representing p-spin interactions. The results obtained for the average number of matrices provide therefore a principled approach to determine the average number of possible graphs with given connectivity distributions of a more general nature than the connectivity profiles examined in this paper.

Extensions and generalisations of the presented framework are under study. A most desired generalisation would be to continuous matrices. The first step in this direction is to study matrices with entries in continuous groups instead of the elements of a finite group, more specifically, U(1) which is a straightforward continuous limit of the cyclic groups.

Acknowledgements

Support from EPSRC grant EP/E049516/1 is gratefully acknowledged. R.C.A. would also like to thank Juan P. Neirotti and Jack Raymond for useful discussions.

References

[1] Mezard, M., Parisi, G., and Zee, A. *Nucl. Phys. B* **559**, 689–701 (1999).
[2] Kanzieper, E. *Nucl. Phys. B* **596**, 548–566 (2001).
[3] Nagao, T. and Tanaka, T. *J. Phys. A* **40**, 4973–4987 (2007).
[4] Biroli, G., Bouchaud, J.-P., and Potters, M. *Europhys. Lett.* **78**, 10001 (2007).
[5] Biroli, G., Bouchaud, J.-P., and Potters, M. *J of Stat. Mech.* , P07019 (2007).
[6] Bohigas, O., de Carvalho, J. X., and Pato, M. P. *Phys. Rev. E* **77**, 011122 (2008).
[7] McEliece, R. *Theory of Information & Coding.* Cambridge University Press, Cambridge, MA, (2002 2nd edition).
[8] Phelps, K. T., Rifà, J., and Villanueva, M. *IEEE Trans. Inf. Theory* **51**, 3931–3937 (2005).
[9] Davey, M. and MacKay, D. *IEEE Communications Letters* **2**, 165 – 167 (1998).
[10] Nakamura, K., Kabashima, Y., and Saad, D. *Eurphys. Lett.* **56**, 610–616 (2001).
[11] Cooper, C. *Random Structures and Algorithms* **16**, 209–232 (2000).
[12] Blömer, J., Karp, R., and Weiz, E. *Random Structures and Algorithms* **10**, 407–419 (1998).
[13] Feng, X. and Zhang, Z. *App. Math. and Comp.* **185**, 689–694 (2007).
[14] Alamino, R. C. and Saad, D. *Phys. Rev. E* **77**, 061123 (2008).
[15] Alamino, R. C. and Saad, D. *J. Phys A: Math. Theor.* **40**, 12259–1279 (2007).
[16] Yano, T., T[]Tanaka, and Saad, D. *J Phys A* **41**(32), 324022 (15pp).
[17] Wang, B.-Y. and Zhang, F. *Discrete Mathematics* **187**, 211–220 (1998).
[18] Gallager, R. *Low-Density Parity-Check Codes, Research monograph series.* Number 21. MIT Press, Cambridge,MA, (1963).

[19] Nishimori, H. *Statistical Physics of Spin Glasses and Information Processing.* Oxford University Press, Oxford, UK, (2001).

Appendix A. Replica Calculations

For the case square matrices ($\eta = 1$) and $\lambda \neq 0$, we can use the integral representation of the Kroenecker delta function in the complex plane such that the averaged replicated kernel size defined in equation (11) is generalised to the size the λ-eigenspace as

$$\begin{aligned}\mathcal{Z}_n(\lambda) = \Bigg\langle \frac{1}{\mathcal{N}} \sum_{\{\mathbf{v}_a\}} \oint DWDZ \sum_{\{A_{ij}\}} \left[\prod_{i,j} \mathcal{P}(A_{ij}) (W_i Z_j)^{\chi(A_{ij})} \right] \\ \times \prod_{i=1}^{M} \prod_{a} \delta \left[\bigoplus_{j=1}^{M} \left(A_{ij} \otimes v_a^j\right), \lambda \otimes v_a^i \right] \Bigg\rangle_{\mathbf{K},\mathbf{C},\Lambda},\end{aligned} \tag{A.1}$$

where $\otimes$ and $\oplus$ indicate respectively multiplication and summation on $GF(q)$ and

$$DWDZ = \left[\prod_{i=1}^{M} \frac{dW_i}{W_i^{K_i+1}} \right] \left[\prod_{j=1}^{M} \frac{dZ_j}{Z_j^{C_j+1}} \right]. \tag{A.2}$$

Using the representation of the Kroenecker delta given in equation (6), the product over replica indices of the delta function can be written as

$$\begin{aligned}&\prod_a \delta \left[\bigoplus_{j=1}^{M} \left(A_{ij} \otimes v_a^j\right), \lambda \otimes v_a^i \right] \\ &= \prod_a \frac{1}{q} \prod_{m=1}^{q-1} \left\{ 1 - \exp\left(-\frac{2\pi i}{q} m\right) \exp\left[-\frac{2\pi i}{q} \left(\lambda \otimes v_a^i\right) \right] \prod_{j=1}^{M} \exp\left[\frac{2\pi i}{q} \left(A_{ij} \otimes v_a^j\right) \right] \right\} \\ &= \frac{1}{q^n} \prod_a \left[1 + \sum_{s=1}^{q-1} F_i(s,a) G(s) \right] \\ &= \frac{1}{q^n} \sum_{r=0}^{n} \sum_{\langle a_1 \cdots a_r \rangle} \sum_{s_1,\ldots,s_r} G(s_1) \cdots G(s_r) F_i(s_1,a_1) \cdots F_i(s_r,a_r),\end{aligned} \tag{A.3}$$

with

$$G(s) \equiv \sum_{\langle m_1 \cdots m_s \rangle} (-1)^s \exp\left(-\frac{2\pi i}{q} m_1\right) \cdots \exp\left(-\frac{2\pi i}{q} m_s\right), \tag{A.4}$$

and

$$F_i(s,a) = \exp\left[-\frac{2\pi i}{q} s \left(\lambda \otimes v_a^i\right) \right] \prod_{j=1}^{M} \gamma_j(s,a,A_{ij}), \tag{A.5}$$

where we defined, for simplicity,

$$\gamma_j(s,a,A_{ij}) \equiv \exp\left[\frac{2\pi i}{q} s \left(A_{ij} \otimes v_a^j\right) \right]. \tag{A.6}$$

The partition function becomes

$$\mathcal{Z}_n(\lambda) = \left\langle \frac{1}{\mathcal{N}} \sum_{\{\mathbf{v}_a\}} \oint DZ \prod_{i=1}^{M} \frac{1}{q^n} \sum_{r=0}^{n} \sum_{\langle a_1 \cdots a_r \rangle} \sum_{s_1,\ldots,s_r} G(s_1)\cdots G(s_r) \oint \frac{dW_i}{2\pi i} \frac{1}{W_i^{K_i+1}} \Gamma_i \right\rangle_{\mathbf{K},\mathbf{C},\Lambda}, \tag{A.7}$$

where

$$\begin{aligned}
\Gamma_i &= \exp\left[-\frac{2\pi i}{q} s_1\big(\lambda \otimes v^i_{a_1}\big)\right] \cdots \exp\left[-\frac{2\pi i}{q} s_r\big(\lambda \otimes v^i_{a_r}\big)\right] \\
&\quad \times \prod_j \sum_{A_{ij}} \mathcal{P}(A_{ij}) (W_i Z_j)^{\chi(A_{ij})} \gamma_j(s_1, a_1, A_{ij}) \cdots \gamma_j(s_r, a_r, A_{ij}) \\
&= p^M \exp\left[-\frac{2\pi i}{q} s_1\big(\lambda \otimes v^i_{a_1}\big)\right] \cdots \exp\left[-\frac{2\pi i}{q} s_r\big(\lambda \otimes v^i_{a_r}\big)\right] \\
&\quad \times \prod_j \left[1 + \frac{1}{p} \sum_{h=1}^{q-1} \mathcal{P}(A_{ij} = h) W_i Z_j \gamma_j(s_1, a_1, h) \cdots \gamma_j(s_r, a_r, h)\right],
\end{aligned} \tag{A.8}$$

where we define, for convenience, $p \equiv \mathcal{P}(A_{ij} = 0)$. Let us define a probability distribution over the values of h as

$$\mathcal{P}(h) = \frac{\mathcal{P}(A_{ij} = h)}{1 - p}, \tag{A.9}$$

in such a way that h varies from 1 to $q-1$ and the probability over this range is correctly normalised. Then

$$\begin{aligned}
\Gamma_i &= p^M \exp\left[-\frac{2\pi i}{q} s_1\big(\lambda \otimes v^i_{a_1}\big)\right] \cdots \exp\left[-\frac{2\pi i}{q} s_r\big(\lambda \otimes v^i_{a_r}\big)\right] \\
&\quad \times \prod_j \left[1 + \left(\frac{1-p}{p}\right) W_i Z_j \langle \gamma_j(s_1, a_1, h) \cdots \gamma_j(s_r, a_r, h)\rangle_h\right] \\
&= p^M \exp\left[-\frac{2\pi i}{q} s_1\big(\lambda \otimes v^i_{a_1}\big)\right] \cdots \exp\left[-\frac{2\pi i}{q} s_r\big(\lambda \otimes v^i_{a_r}\big)\right] \sum_{l=0}^{N} \sum_{\langle j_1 \cdots j_l \rangle} \left(\frac{1-p}{p}\right)^l \\
&\quad \times W_i^l Z_{j_1} \cdots Z_{j_l} \langle \gamma_{j_1}(s_1, a_1, h) \cdots \gamma_{j_1}(s_r, a_r, h)\rangle_h \cdots \langle \gamma_{j_l}(s_1, a_1, h) \cdots \gamma_{j_l}(s_r, a_r, h)\rangle_h.
\end{aligned} \tag{A.10}$$

The integrals over the W_i's, acting on the Γ_i's, select the power of W_i to be K_i and

we therefore obtain

$$\begin{aligned}
\mathcal{Z}_n = \Bigg\langle \kappa \sum_{\{\mathbf{v}_a\}} \oint DZ \prod_{i=1}^{M} \Bigg\{ \sum_{r=0}^{n} \sum_{\langle a_1 \cdots a_r \rangle} \sum_{s_1,\ldots,s_r} G(s_1)\cdots G(s_r) \\
\times \exp\left[-\frac{2\pi i}{q} s_1 \big(\lambda \otimes v_{a_1}^i\big) \right] \cdots \exp\left[-\frac{2\pi i}{q} s_r \big(\lambda \otimes v_{a_r}^i\big) \right] \sum_{\langle j_1 \cdots j_{K_i} \rangle} Z_{j_1} \cdots Z_{j_{K_i}} \\
\times \ \langle \gamma_{j_1}(s_1, a_1, h) \cdots \gamma_{j_1}(s_r, a_r, h) \rangle_h \cdots \Big\langle \gamma_{j_{K_i}}(s_1, a_1, h) \cdots \gamma_{j_{K_i}}(s_r, a_r, h) \Big\rangle_h \Bigg\} \Bigg\rangle_{\mathbf{K},\mathbf{C},\Lambda} \\
\approx \Bigg\langle \kappa \sum_{\{\mathbf{v}_a\}} \oint DZ \prod_{i=1}^{M} \Bigg\{ \sum_{r=0}^{n} \sum_{\langle a_1 \cdots a_r \rangle} \sum_{s_1,\ldots,s_r} G(s_1)\cdots G(s_r) \\
\times \exp\left[-\frac{2\pi i}{q} s_1 \big(\lambda \otimes v_{a_1}^i\big) \right] \cdots \exp\left[-\frac{2\pi i}{q} s_r \big(\lambda \otimes v_{a_r}^i\big) \right] \\
\times \ \frac{N^{K_i}}{K_i!} \left[\frac{1}{N} \sum_{j=1}^{N} Z_j \langle \gamma_j(s_1, a_1, h) \cdots \gamma_j(s_r, a_r, h) \rangle_h \right]^{K_i} \Bigg\} \Bigg\rangle_{\mathbf{K},\mathbf{C},\Lambda}
\end{aligned} \tag{A.11}$$

where

$$\kappa = p^{M^2} \left(\frac{1-p}{p} \right)^{\sum_i K_i} \mathcal{N}^{-1} q^{-nM}. \tag{A.12}$$

The calculation of $\mathcal{N}$ is similar to the calculation of the number of matrices [14] and we end up with

$$\kappa = \frac{1}{q^{nM} N_A^{(2)}}, \tag{A.13}$$

where $N_A^{(2)}$ is exactly the number of binary matrices ($q = 2$). Introducing the replica overlaps

$$Q_{\langle a_1 \cdots a_r \rangle}^{s_1,\ldots,s_r} \equiv \frac{1}{M} \sum_{j=1}^{M} Z_j \langle \gamma_j(s_1, a_1, h) \cdots \gamma_j(s_r, a_r, h) \rangle_h, \tag{A.14}$$

and the corresponding auxiliary variables $\hat{Q}_{\langle a_1 \cdots a_r \rangle}^{s_1,\ldots,s_r}$ by means of Dirac delta functions, and noting that we are now working with square matrices such that the indices i and j

run through the same set, we can express the partition function as

$$\begin{aligned}
\mathcal{Z}_n = & \int DQD\hat{Q} \exp\Big(-M \sum Q^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle} \hat{Q}^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle}\Big) \\
& \times \Bigg\langle \kappa \frac{M^{\sum_i K_i}}{\prod_i K_i!} \prod_i \sum_{\{v_a\}} \Bigg\{ \sum G(s_1)\cdots G(s_r) \Big(Q^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle}\Big)^{K_i} \\
& \times \exp\left[-\frac{2\pi i}{q} s_1(\lambda \otimes v_{a_1})\right] \cdots \exp\left[-\frac{2\pi i}{q} s_r(\lambda \otimes v_{a_r})\right] \Bigg\} \\
& \times \oint DZ_i \exp\Big[Z_i \sum \hat{Q}^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle} \langle \gamma_i(s_1,a_1,h)\cdots\gamma_i(s_r,a_r,h)\rangle_h\Big] \Bigg\rangle_{\mathbf{K},\mathbf{C},\Lambda} \\
= & \int DQD\hat{Q} \exp\Big(-M \sum Q^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle} \hat{Q}^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle}\Big) \\
& \times \Bigg\langle q^{-nM} \frac{M^{\sum_i K_i}}{(\sum_i K_i)!} \prod_i \sum_{\{v_a\}} \Bigg\{ \sum G(s_1)\cdots G(s_r) \Big(Q^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle}\Big)^{K_i} \\
& \times \exp\left[-\frac{2\pi i}{q} s_1(\lambda \otimes v_{a_1})\right] \cdots \exp\left[-\frac{2\pi i}{q} s_r(\lambda \otimes v_{a_r})\right] \Bigg\} \\
& \times \Big[\sum \hat{Q}^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle} \langle \gamma_i(s_1,a_1,h)\cdots\gamma_i(s_r,a_r,h)\rangle_h\Big]^{C_i} \Bigg\rangle_{\mathbf{K},\mathbf{C},\Lambda}
\end{aligned} \tag{A.15}$$

where

$$DQD\hat{Q} \equiv \left(\prod \frac{dQ\, d\hat{Q}}{2\pi i/M}\right), \tag{A.16}$$

and the summations run over all the allowed values of r, $\langle a_1 \cdots a_r\rangle$ and $s_1, \ldots s_r$.

Under the assumption of replica symmetry in the form

$$Q^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle} = Q_0 \langle x^r \rangle_x, \tag{A.17}$$

$$\hat{Q}^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle} = \hat{Q}_0 \langle \hat{x}^r \rangle_{\hat{x}}, \tag{A.18}$$

where the averages over x and $\hat{x}$ are taken with respect to the field distributions $\pi(x)$ and $\hat{\pi}(\hat{x})$ respectively, we can show by straightforward algebraic manipulations that

$$\sum Q^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle} \hat{Q}^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle} = Q_0 \hat{Q}_0 \langle [1 + (q-1)x\hat{x}]^n \rangle_{x,\hat{x}}, \tag{A.19}$$

$$\begin{aligned}
& \sum G(s_1)\cdots G(s_r) \Big(Q^{s_1,\ldots,s_r}_{\langle a_1 \cdots a_r\rangle}\Big)^{K_i} \exp\left[-\frac{2\pi i}{q} s_1(\lambda \otimes v_{a_1})\right] \cdots \exp\left[-\frac{2\pi i}{q} s_r(\lambda \otimes v_{a_r})\right] = \\
& Q_0^{K_i} \left\langle \prod_{a=1}^{n} \left[1 + \tilde{\omega}(v_a) \prod_{l=1}^{K_i} x_l\right] \right\rangle_{\mathbf{x}},
\end{aligned} \tag{A.20}$$

with

$$\tilde{\omega}(v) \equiv \sum_{s=1}^{q-1} G(s) \exp\left[-i \frac{2\pi s}{q} (\lambda \otimes v)\right], \tag{A.21}$$

and

$$\begin{aligned}\Big[\sum \hat{Q}^{s_1,\ldots,s_r}_{\langle a_1\cdots a_r\rangle}\langle\gamma_i(s_1,a_1,h)\cdots\gamma_i(s_r,a_r,h)\rangle_h\Big]^{C_i} = \\ \hat{Q}_0^{C_i}\left\langle\prod_{a=1}^{n}\prod_{l=1}^{C_i}[1+\omega(v_a,h_l)\hat{x}_l]\right\rangle_{\hat{\mathbf{x}},\mathbf{h}},\end{aligned} \tag{A.22}$$

with

$$\omega(v,h_l)\equiv\sum_{s=1}^{q-1}\exp\left[i\frac{2\pi s}{q}(h_l\otimes v)\right]=\begin{cases} q-1, & \text{if } h_l\otimes v=0,\\ -1, & \text{otherwise.}\end{cases} \tag{A.23}$$

Therefore, we have, for the sum over $\{v_a\}$,

$$\begin{aligned}&\sum_{\{v_a\}}\left\{Q_0^{K_i}\left\langle\prod_{a=1}^{n}\left[1+\tilde{\omega}(v_a)\prod_{l=1}^{K_i}x_l\right]\right\rangle_{\mathbf{x}}\right\}\left\{\hat{Q}_0^{C_i}\left\langle\prod_{a=1}^{n}\prod_{l=1}^{C_i}[1+\omega(v_a,h_l)\hat{x}_l]\right\rangle_{\hat{\mathbf{x}},\mathbf{h}}\right\}\\ &\quad=Q_0^{K_i}\hat{Q}_0^{C_i}\left\langle\left\{\sum_v\left[1+\tilde{\omega}(v)\prod_{l=1}^{K_i}x_l\right]\prod_{l=1}^{C_i}[1+\omega(v,h_l)\hat{x}_l]\right\}^n\right\rangle_{\mathbf{x},\hat{\mathbf{x}},\mathbf{h}}\\ &\quad=Q_0^{K_i}\hat{Q}_0^{C_i}\left\langle\left\{\left[1+(q-1)\prod_{l=1}^{K_i}x_l\right]\prod_{l=1}^{C_i}[1+(q-1)\hat{x}_l]\right.\right.\\ &\quad+\left.\left\{(q-1)+\left[\sum_{v=1}^{q-1}\tilde{\omega}(v)\right]\prod_{l=1}^{K_i}x_l\right\}\left[\prod_{l=1}^{C_i}(1-\hat{x}_l)\right]\right\}^n\Big\rangle_{\mathbf{x},\hat{\mathbf{x}}},\end{aligned} \tag{A.24}$$

where with some amount of algebraic calculations to show that

$$\sum_{v=1}^{q-1}\tilde{\omega}(v)=-(q-1), \tag{A.25}$$

when $\lambda\neq 0$, we can write

$$\mathcal{Z}_n=\int DQD\hat{Q}\,e^{M\tilde{s}}, \tag{A.26}$$

with

$$\tilde{s}=-\frac{1}{M}\ln N_A^{(2)}-n\ln q-Q_0\hat{Q}_0\langle[1+(q-1)x\hat{x}]^n\rangle_{x,\hat{x}}+\frac{1}{M}\ln\Phi, \tag{A.27}$$

where

$$\begin{aligned}\Phi=\left\langle\frac{M^\Lambda}{\Lambda!}Q_0^\Lambda\hat{Q}_0^\Lambda\prod_i\left\langle\left\{\left[1+(q-1)\prod_{l=1}^{K_i}x_l\right]\prod_{l=1}^{C_i}[1+(q-1)\hat{x}_l]\right.\right.\right.\\ \left.\left.\left.+\ (q-1)\left(1-\prod_{l=1}^{K_i}x_l\right)\prod_{l=1}^{C_j}(1-\hat{x}_l)\right\}^n\right\rangle_{\mathbf{x},\hat{\mathbf{x}}}\right\rangle_{\mathbf{K},\mathbf{C},\Lambda}\end{aligned} \tag{A.28}$$

Let us define $\alpha \equiv MQ_0\hat{Q}_0$. For $n \ll 1$, we can consider only the leading contributions in the number of replicas, which gives

$$\ln \Phi = \ln \epsilon(\alpha) + \frac{n}{\epsilon(\alpha)} \sum_i \left\langle \frac{\alpha^\Lambda}{\Lambda!} \langle \ln \{\cdots\} \rangle_{\mathbf{x},\hat{\mathbf{x}}} \right\rangle_{\mathbf{K},\mathbf{C},\Lambda}, \tag{A.29}$$

with

$$\epsilon(\alpha) = \left\langle \frac{\alpha^\Lambda}{\Lambda!} \right\rangle_{\mathbf{K},\mathbf{C},\Lambda}, \tag{A.30}$$

and where $\{\cdots\}$ stands for the expression inside curly brackets in equation (A.28) above.

Substituting the above formulas in $\tilde{s}$ for $n \to 0$, the extremization with respect to Q_0, $\hat{Q}_0$, $\pi(x)$ and $\hat{\pi}(\hat{x})$ leads to the saddle point equations (17), (18) and (19).

Appendix B. Proof of Replica Symmetry

Let us consider the probability distribution inside a specific eigenspace with $\lambda \neq 0$. Then

$$\mathcal{P}(\mathbf{v}|\lambda) = \left[\sum_{\mathbf{v}} \delta(A\mathbf{v}, \lambda\mathbf{v}) \right]^{-1} = q^{-d_A(\lambda)}. \tag{B.1}$$

The distribution of the k-point functions is

$$\begin{aligned} \mathcal{P}(m_k) &= \left\langle \delta\left(m_k - \frac{1}{N} \sum_{j=1}^{N} \sigma_1^j \cdots \sigma_k^j \right) \right\rangle_{\boldsymbol{\sigma}_1,\ldots,\boldsymbol{\sigma}_k} \\ &= q^{-kd_A(\lambda)} \sum_{\mathbf{v}_1,\ldots,\mathbf{v}_k} \delta(A\mathbf{v}_1, \lambda\mathbf{v}_1) \cdots \delta(A\mathbf{v}_k, \lambda\mathbf{v}_k) \\ &\quad \times \delta\left[m_k - \frac{1}{N} \sum_{j=1}^{N} \exp\left(\frac{2\pi i}{q} \big(v_1^j + \cdots + v_k^j \big) \right) \right]. \end{aligned} \tag{B.2}$$

Let us call

$$g(\mathbf{v}_1, ..., \mathbf{v}_k) \equiv \delta\left[m_k - \frac{1}{N} \sum_{j=1}^{N} \exp\left(\frac{2\pi i}{q} \big(v_1^j + \cdots + v_k^j \big) \right) \right], \tag{B.3}$$

and note that $g(\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_k) = g(\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_{k-1} \oplus \mathbf{v}_k, 0)$. Therefore we can write

$$\begin{aligned}
\mathcal{P}(m_k) &= q^{-kd_A(\lambda)} \sum_{\mathbf{v}_1,...,\mathbf{v}_k} \delta(A\mathbf{v}_1, \lambda\mathbf{v}_1) \cdots \delta(A\mathbf{v}_k, \lambda\mathbf{v}_k) g(\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_{k-1} \oplus \mathbf{v}_k, 0) \\
&= q^{-kd_A(\lambda)} \sum_{\mathbf{v}_1,...,\mathbf{v}_k} \delta(A\mathbf{v}_1, \lambda\mathbf{v}_1) \cdots \delta(A\mathbf{v}_k, \lambda\mathbf{v}_k) \sum_{\mathbf{u}} \delta(\mathbf{u}, \mathbf{v}_{k-1} \oplus \mathbf{v}_k) g(\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{u}, 0) \\
&= q^{-kd_A(\lambda)} \sum_{\mathbf{v}_1,...,\mathbf{v}_{k-2},\mathbf{u}} g(\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{u}, 0) \\
&\quad \times \sum_{\mathbf{v}_{k-1}} \delta(A\mathbf{v}_{k-1}, \lambda\mathbf{v}_{k-1}) \sum_{\mathbf{v}_k} \delta(A\mathbf{v}_k, \lambda\mathbf{v}_k) \delta(\mathbf{u}, \mathbf{v}_{k-1} \oplus \mathbf{v}_k) \\
&= q^{-kd_A(\lambda)} \sum_{\mathbf{v}_1,...,\mathbf{v}_{k-2},\mathbf{u}} g(\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{u}, 0) \\
&\quad \times \sum_{\mathbf{v}_{k-1}} \delta(A\mathbf{v}_{k-1}, \lambda\mathbf{v}_{k-1}) \delta(A(\mathbf{u} \oplus (-\mathbf{v}_{k-1})), 0) \\
&= q^{-(k-1)d_A(\lambda)} \sum_{\mathbf{v}_1,...,\mathbf{v}_{k-2},\mathbf{u}} \delta(A\mathbf{u}, \lambda\mathbf{u}) g(\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{u}, 0) \\
&= \left\langle \delta\left(m_k - \frac{1}{N} \sum_{j=1}^{N} \sigma_1^j \cdots \sigma_{k-1}^j \right) \right\rangle_{\boldsymbol{\sigma}_1,...,\boldsymbol{\sigma}_{k-1}} .
\end{aligned} \tag{B.4}$$

Therefore, the distribution of the k-point functions is the same as the $(k-1)$-point functions for any $k > 2$. Therefore, if the magnetisation is zero, all other higher order correlations are also zero and, therefore, there is neither a spin-glass phase nor more complex types of phases but the paramagnetic one. This implies that there is no replica symmetry breaking in the system [19]. The fact that the solution is replica symmetric means that the temperature $T = 1/\ln q$ can be associated with the Nishimori temperature of the system.