Statistical Physics of Low Density Parity Check Error Correcting Codes

David Saad[1], Yoshiyuki Kabashima[2], Tatsuto Murayama[2] and Renato Vicente[3]

[1]Neural Computing Research Group, Aston University, Birmingham B4 7ET, UK.
[2]Dept. of Comp. Intel. & Syst. Sci., Tokyo Institute of Technology, Yokohama 2268502, Japan.
[3] Dep. de Física Geral, Instituto de Física, Universidade de São Paulo, Caixa Postal 66318, 05315-970 São Paulo - SP, Brazil.

Abstract. We study the performance of Low Density Parity Check (LDPC) error-correcting codes using the methods of statistical physics. LDPC codes are based on the generation of codewords using Boolean sums of the original message bits by employing two randomly-constructed sparse matrices. These codes can be mapped onto Ising spin models and studied using common methods of statistical physics. We examine various regular constructions and obtain insight into their theoretical and practical limitations. We also briefly report on results obtained for irregular code constructions, for codes with non-binary alphabet, and on how a finite system size effects the error probability.

1 Introduction

Modern telecommunication relies heavily on error correcting mechanisms to compensate for corruption due to noise during transmission. The information transmission code rate, measured in the fraction of informative transmitted bits, plays a crucial role in determining the speed of communication channels. Rigorous bounds [1] have been derived for the maximal code rate for which codes, capable of achieving arbitrarily small error probability, can be found. However, these bounds are not constructive and most existing practical error-correcting codes are far from saturating them.

Two code families currently achieve the highest information transmission rates for a given corruption level, especially in the high code rate regime. Turbo codes [2] have been introduced less than a decade ago, and were followed by the rediscovery of Low Density Parity Check Codes (LPDC) [3]. The latter have been originally introduced by Gallager [4] in 1962, and abandoned in favour of other codes due to the limited computing facilities of the time. Both codes show excellent performance and recently discovered irregular LDPC constructions nearly saturate Shannon's bound for infinite message size [5].

LDPC codes are generally based on the introduction of random sparse matrices for generating the transmitted codeword as well as for decoding the received corrupted codeword. Two main types of matrices have been studied: regular constructions, where the number of non-zero row/column elements in these matrices

remains fixed; and irregular constructions where it can vary from row to row or column to column. Various decoding methods have been successfully employed; we will mainly refer here to the leading decoding techniques based on Belief Propagation (BP) [6].

Most analyses of LDPC codes have been obtained via methods of information theory, backed up by numerical simulations. These rely on deriving upper and lower bounds for the performance of codes, with or without making assumptions about the code used. These bounds represent a worst case analysis, and may be tight or loose depending on the accuracy and restrictiveness of the assumptions used, and the specific difference between the worst and typical cases.

The statistical physics based analysis takes a different approach, analysing directly the typical case, making use of explicit assumptions about the code used and its macroscopic characteristics. Moreover, using methods adopted from statistical physics of Ising spin systems, one can actually carry out averages over ensembles of codes with the same macroscopic properties to obtain exact performance estimates in the limit of infinitely large systems. Two methods have been used in particular, the replica method and the Bethe approximations [7], that is also linked to the Thouless-Anderson-Palmer (TAP) approach [8] to diluted systems. In this paper we will review recent studies of LDPC codes, using a statistical physics based analysis. We focus on two specific codes, Gallager's original LDPC code [4] and the MN code [3] where messages are represented by binary vectors and are communicated through a Binary Symmetric Channel (BSC) where uncorrelated bit flips appear with probability p.

A Gallager code is defined by a binary matrix $\mathcal{A} = [A \mid B]$, concatenating two very sparse matrices known to both sender and receiver, with B (of dimensionality $(M-N)\times(M-N)$) being invertible - the matrix A is of dimensionality $(M-N)\times N$.

Encoding refers to the production of a M dimensional binary codeword $\boldsymbol{t} \in \{0,1\}^M$ $(M > N)$ from the original message $\xi \in \{0,1\}^N$ by $\boldsymbol{t} = G^T\boldsymbol{\xi} \pmod 2$, where all operations are performed in the field $\{0,1\}$ and are modulo 2. The generator matrix is $G = [I \mid B^{-1}A] \pmod 2$, where I is the $N \times N$ identity matrix, implying that $AG^T = 0 \pmod 2$ and that the first N bits of $\boldsymbol{t}$ are set to the message $\boldsymbol{\xi}$. In *regular* Gallager codes the number of non-zero elements in each row of A is chosen to be exactly $\hat{K}$. The number of elements per column is then $C = (1-R)\hat{K}$, where the code rate is $R = N/M$ (for unbiased messages). The encoded vector $\boldsymbol{t}$ is then corrupted by noise represented by the vector $\boldsymbol{\zeta} \in \{0,1\}^M$ with components independently drawn with probability $P(\zeta) = (1-p)\delta(\zeta) + p\delta(\zeta-1)$. The received vector takes the form $\boldsymbol{r} = G^T\boldsymbol{\xi} + \boldsymbol{\zeta} \pmod 2$.

Decoding is carried out by multiplying the received message by the matrix $\mathcal{A}$ to produce the *syndrome* vector $\boldsymbol{z} = \mathcal{A}\boldsymbol{r} = \mathcal{A}\boldsymbol{\zeta} \pmod 2$ from which an estimate $\hat{\boldsymbol{\tau}}$ for the noise vector can be produced. An estimate for the original message is then obtained as the first N bits of $\boldsymbol{r} + \widehat{\boldsymbol{\tau}} \pmod 2$. The Bayes optimal estimator (also known as *marginal posterior maximiser*, MPM) for the noise is defined as $\widehat{\tau}_j = \mathrm{argmax}_{\tau_j} P(\tau_j \mid z)$, where $\tau_j \in \{0,1\}$. The performance of this estimator can be measured by the probability of bit error $P_b = 1 - 1/M \ \sum_{j=1}^{M} \delta[\widehat{\tau}_j; \zeta_j]$,

where $\delta[;]$ is Kronecker's delta. Knowing the matrices B and A, the syndrome vector $\boldsymbol{z}$ and the noise level p, it is possible to apply Bayes' theorem and compute the posterior probability

$$P(\boldsymbol{\tau} \mid \boldsymbol{z}) = \frac{1}{Z}\chi\left[\boldsymbol{z} = \mathcal{A}\boldsymbol{\tau} (\text{mod } 2)\right] P(\boldsymbol{\tau}), \tag{1}$$

where $\chi[X]$ is an indicator function providing 1 if X is true and 0 otherwise. To compute the MPM one has to compute the marginal posterior $P(\tau_j \mid \boldsymbol{z}) = \sum_{i \neq j} P(\boldsymbol{\tau} \mid \boldsymbol{z})$, which in general requires $\mathcal{O}(2^M)$ operations, thus becoming impractical for long messages. To solve this problem one can use the sparseness of $\mathcal{A}$ to design algorithms that require $\mathcal{O}(M)$ operations to perform the same task. One of these methods is the probability propagation algorithm, also known as belief propagation (BP) [6].

The MN code has a similar structure, except for the fact that the generator matrix is $G = B^{-1}A$. The randomly-selected sparse matrices A and B are of dimensionality $M \times N$ and $M \times M$ respectively; these are characterized by K and L non-zero unit elements per row and C and L per column respectively. Correspondingly, the code rate becomes $R = N/M = K/C$. Decoding is carried out by taking the product of the matrix B and the received message $\boldsymbol{z} = G^T\boldsymbol{\xi} + \boldsymbol{\zeta}$ (mod 2). The equation

$$\boldsymbol{z} = A\boldsymbol{\xi} + B\boldsymbol{\zeta} = A\boldsymbol{S} + B\boldsymbol{\tau} \pmod 2, \tag{2}$$

is solved via the iterative methods of BP [3] to obtain the most probable Boolean vectors $\boldsymbol{S}$ and $\boldsymbol{\tau}$; the posterior probability (1) becomes slightly more elaborate, including two sets of free variables $\boldsymbol{S}$ and $\boldsymbol{\tau}$ and two priors.

2 Statistical physics

To facilitate the statistical physics analysis we replace the $\{0, 1\}$ representation by the conventional Ising spin $\{1, -1\}$ representation, and mod 2 sums by products [9]. For instance, in Gallager's code, the syndrome vector acquires the form of a multi-spin coupling $\mathcal{J}_\mu = \prod_{j \in \mathcal{L}(\mu)} \zeta_j$ where $j = 1, \cdots, M$ and $\mu = 1, \cdots, (M - N)$. The $\hat{K}$ indices of nonzero elements in the row μ of a matrix $\mathcal{A}$, that is not necessarily a concatenation of two matrices (therefore defining a *non-structured* Gallager code), are given by $\mathcal{L}(\mu) = \{j_1, \cdots, j_{\hat{K}}\}$, and in a column l are the C indices given by $\mathcal{M}(l) = \{\mu_1, \cdots, \mu_C\}$.

The posterior (1) can be written as the Gibbs distribution [10]:

$$P(\boldsymbol{\tau} \mid \mathcal{J}) = \frac{1}{Z} \lim_{\beta \to \infty} \exp\left[-\beta \mathcal{H}_\beta(\boldsymbol{\tau}; \mathcal{J})\right] \tag{3}$$

$$\mathcal{H}_\beta(\boldsymbol{\tau}; \mathcal{J}) = -\sum_{\mu=1}^{M-N} \mathcal{J}_\mu \left(\prod_{j \in \mathcal{L}(\mu)} \tau_j - 1 \right) - \frac{F}{\beta} \sum_{j=1}^{M} \tau_j \ ,$$

where $\mathcal{H}$ the Hamiltonian of the system.

The quantity that one concentrates on, in the statistical physics based analysis, is the *free energy* which is linked to the probability of finding the system in a specific configuration. In the *thermodynamic limit* of infinite system size, which is the main case considered in this work, the state of the system is dominated by configurations with the lowest free energy; finite systems are more likely to be found in configurations with lower free energy, but may also be found in other configurations with some probability.

To investigate the typical properties of a model, we calculate the partition function $\mathcal{Z}(\mathcal{A},\mathcal{J}) = \mathrm{Tr}_{\{\boldsymbol{\tau}\}} \exp[-\beta\mathcal{H}]$ and the free energy $\langle \ln[\mathcal{Z}(\mathcal{A},\mathcal{J})]\rangle_{\mathcal{A},\boldsymbol{\zeta}}$ by averaging over the randomness induced by the specific code matrix $\mathcal{A}$ and the true noise vector $\boldsymbol{\zeta}$. For carrying out these averages we use the replica method [10] or the Bethe approximation [11]; both methods provide the same results.

The replica method makes use of the identity $\langle \ln \mathcal{Z}\rangle = \langle \lim_{n\to 0}\ 1/n\ [\mathcal{Z}^n - 1]\rangle$, by calculating averages over a product of partition function replica. Employing assumptions about replica symmetries and analytically continuing the variable n to zero, one obtains solutions which enable one to determine the state of the system. The Bethe approximation is based on a consistent solution to a tree based expansion for calculating the free energy. Details of the techniques used and of the calculations themselves can be obtained in [7] and in the corresponding papers [10] and [11].

3 Results

Once the free energy for the possible solutions is calculated, one can identify the stable dominant solutions and their overlap m with the true noise/signal vectors. In the case of Gallager's code we monitor $m = 1/M\ \sum_{j=1}^{M} \delta[\widehat{\tau}_j;\zeta_j]$, where $\widehat{\boldsymbol{\tau}}$ is the noise vector MPM estimate. In the case of MN we calculate $m = 1/N\ \sum_{j=1}^{N} \delta[\widehat{S}_j;\xi_j]$, estimating the signal vector $\widehat{\boldsymbol{S}}$.

One observes three types of solutions: perfect retrieval (ferromagnetic solution) $m = 1$; catastrophic failure (paramagnetic solution) $m = 0$; and partial failure (sub-optimal ferromagnetic solution) $0 < m < 1$.

In each case one identifies two main critical noise levels: the spinodal point p_s, the noise level below which only perfect (ferromagnetic) solutions exist; and p_t, the noise level above which the ferromagnetic solution is no longer dominant. The former marks the practical decoding limit, as current practical decoding methods fail above p_s, while the latter marks the theoretical limits of the system.

The results obtained for $R = 1/4$ Gallager code are shown in Fig.1a, where we present the theoretical mean overlap between the actual noise vector $\boldsymbol{\zeta}$ and the estimate $\widehat{\boldsymbol{\tau}}$ as a function of the noise level p, as well as results obtained using BP decoding. In Fig.1b we show the thermodynamic transition for $\hat{K} = 6$ and $R = 1/2$ compare with the theoretical upper bound, Shannon's bound and the theoretical p_s values.

Results obtained for MN code with various K, L values are presented in Fig.2. On the left - a schematic description of the free energy surface for various K

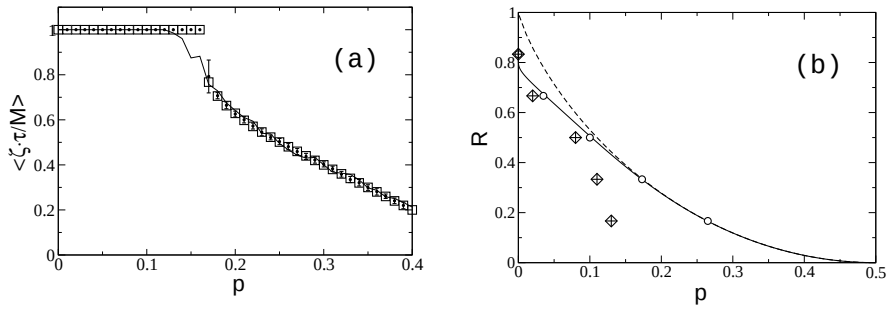

Fig. 1. (a) Mean normalized overlap between the actual noise vector $\boldsymbol{\zeta}$ and decoded noise $\widehat{\boldsymbol{\tau}}$ for $\hat{K}=4$ and $C=3$ (therefore $R=1/4$). Theoretical values (squares), experimental averages over 20 runs for code word lengths $M=5000$ ($\bullet$) and $M=100$ (full line). (b) Transitions for $\hat{K}=6$. Shannon's bound (dashed line), information theory based upper bound (full line) and thermodynamic transition obtained numerically ($\circ$). Theoretical (diamond) and experimental ($+$, $M=5000$ averaged over 20 runs) BP decoding transitions are also shown. In both figures, symbols are chosen larger than the error bars.

values; on the right a description of the existing solutions for each noise value p and their corresponding overlap m.

For unbiased messages with $K\geq 3$ and $L>1$. we obtain both the ferromagnetic and paramagnetic solutions either by applying the TAP approach or by solving the saddle point equations numerically. The former was carried out at the values of F_τ and $F_s=0$) which correspond to the true noise and input bias levels (for unbiased messages $F_s=0$) and thus to Nishimori's condition [12]. The latter is equivalent to having the correct prior within the Bayesian framework [9].

The most interesting quantity to examine is the maximal code rate, for a given corruption process, for which messages can be perfectly retrieved. This is defined in the case of $K\geq 3$ by the value of $R=K/C=N/M$ for which the free energy of the ferromagnetic solution becomes smaller than that of the paramagnetic solution, constituting a first order phase transition. The critical code rate obtained $R_c=1-H_2(p)=1+(p\log_2 p+(1-p)\log_2(1-p))$, coincides with *Shannon's capacity*.

The MN code for $K\geq 3$ seems to offer optimal performance. However, the main drawback is rooted in the co-existence of the stable $m=1,0$ solutions, which implies that from most initial conditions the system will converge to the undesired paramagnetic solution. Studying the ferromagnetic solution numerically shows a highly limited basin of attraction, which becomes smaller as K and L increase, while the paramagnetic solution at $m=0$ *always* enjoys a wide basin of attraction.

Studying the case of $K=2$ and $L>1$, indicates the existence of paramagnetic, ferromagnetic and sub-optimal ferromagnetic solutions depicted in Fig.2b. For corruption probabilities $p>p_s$ one obtains either a dominant paramagnetic solution or a mixture of ferromagnetic ($m=\pm 1$) and paramagnetic ($m=0$) so-

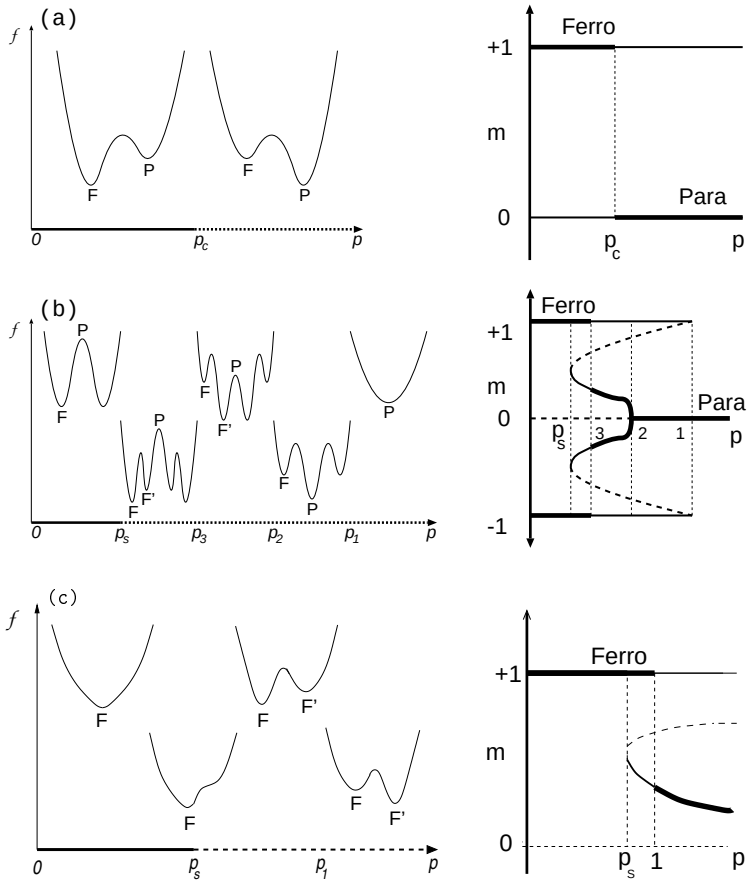

Fig. 2. Left hand figures show a schematic representation of the free energy landscape while figures on the right show the ferromagnetic, sub-optimal ferromagnetic and paramagnetic solutions as functions of the noise rate p; thick and thin lines denote stable solutions of lower and higher free energies respectively, dashed lines correspond to unstable solutions. In all cases considered $L > 1$. (a) $K \geq 3$; the solid line in the horizontal axis represents the phase where the ferromagnetic solution (F, $m = 1$) is thermodynamically dominant, while the paramagnetic solution (P, $m = 0$) becomes dominant for the other phase (dashed line). The critical noise p_c denotes Shannon's channel capacity. (b) $K = 2$; the ferromagnetic solution and its mirror image are the only minima of the free energy over a relatively small noise level (the solid line in the horizontal). The critical point,due to dynamical considerations, is the spinodal point p_s where sub-optimal ferromagnetic solutions (F', $m < 1$) emerge. The thermodynamic transition point p_3, at which the ferromagnetic solution loses its dominance, is below the maximum noise level given by the channel capacity, which implies that these codes do not saturate Shannon's bound even if optimally decoded. (c) $K = 1$; the solid line in the horizontal axis represents the range of noise levels where the ferromagnetic state (F) is the only minimum of the free energy. The sub-optimal ferromagnetic state (F') appears in the region represented by the dashed line. The spinodal point p_s, where F' solution first appears, provides the highest noise value in which convergence to the ferromagnetic solution is guaranteed. For higher noise levels, the system becomes bistable and an additional unstable solution for the saddle point equations necessarily appears. A thermodynamical transition occurs at the noise level p_1 where the state F' becomes dominant.

lutions. Reliable decoding may only be obtained for $p < p_s$, which corresponds to a spinodal point, where a unique ferromagnetic solution emerges at $m = 1$ (plus a mirror solution at $m = -1$). Initial conditions for BP decoding can be chosen randomly, with a slight bias in the initial magnetization. The results obtained point to the existence of a unique pair of global solutions to which the system converges (below p_s) from *all initial conditions*. Similarly, the case of $K = 1,\ L > 1$ presented in Fig.2c shows a dominant ferromagnetic solution below p_s and the emergence of a sub-optimal ferromagnetic solution above it, that becomes dominant at p_1.

The main differences between the results obtained for Gallager and MN codes in the case of unbiased messages are as follows. While Gallager's code allows for sub-optimal practical decoding for any $\hat{K}$ value, it saturates Shannon's bound only in the limit of $\hat{K} \to \infty$. On the other hand, MN codes can *theoretically* saturate Shannon's limit for constructions with $K \geq 3$, which are of no practical value, but they can only achieve suboptimal performance for regular configurations with $K = 1, 2$.

It should be pointed out that these results are valid only in the case of unbiased signal vectors $\boldsymbol{\xi}$. A different picture emerges in the case of biased messages; this includes the emergence of a spinodal point also in the case of $K \geq 3$ MN codes and a decrease in the noise level of the thermodynamic transition to below Shannon's limit.

It has been shown that irregular LDPC constructions can achieve better practical performance (e.g. [5, 13]). In analytical studies, based on the same framework presented here [14] we investigated the position of both critical points p_s and p_t with respect to Shannon's limit and their values in regular constructions. We show that improved irregular constructions correspond to models with higher p_s values while the position of p_t changes only slightly. The possibility of employing the statistical physics based analysis for providing a principled method to optimise the code construction is still an open question.

4 Related studies

We also studied the effect of non-binary alphabet on the performance of LDPC codes [15] as it seems to offer improved performance in many cases [16]. The alphabet used in this study is defined over Galois field $GF(q)$ [17]. Our results show that Gallager codes of this type saturate Shannon's limit as $C \to \infty$ irrespective of the value of q. For finite C, these codes exhibits two different behaviours for $C \geq 3$ and $C = 2$. For $C \geq 3$, we show that the theoretical error correcting ability of these codes is monotonically improving as q increases, i.e., the value of p_t increases with q for a given configuration. The practical decoding limit, determined by the emergence of a suboptimal solution and the value of p_s, decreases with q. On the other hand, $C = 2$ codes exhibit a continuous transition from optimal to sub-optimal solutions at a certain noise level, below which practical BP decoding converges to the (unique) optimal solution. This critical noise level monotonically increases with q and becomes even higher than that of some codes

of connectivity $C \geq 3$, while the optimal decoding performance is inferior to that of $C \geq 3$ codes with the same q value.

The work described so far is limited to the case of infinite message length. In finite systems there is some probability of finding the system in a non-dominant state, what translates to an error probability which vanishes exponentially with the systems size. Significant effort has been dedicated to bounding the *reliability exponent* in the information theory literature [18]; we have also studied the reliability exponent [19] by carrying out direct averages over ensembles of Gallager codes, characterised by finite and infinite $\hat{K}$ values. In the limit of infinite connectivity our result collapses onto the best general random coding exponents reported in the IT literatures, the *random coding exponent* and the *expurgated exponent* for high and low R values respectively. The method provides one of the only tools available for examining codes of finite connectivity, and predicts the tightest estimate of the zero error noise level threshold to date for Gallager codes. It can be easily extended to investigate other linear codes of a similar type and is clearly of high practical significance.

Finally, insight gained from the analysis led us to suggest the potential use of a similar system as a public-key cryptosystem [20]. The cryptosystem is based on an MN code where the matrix G and a corruption level $p < p_s$ play the role of the public key and the matrices used to generate G play the role of the secret key and are known only to the authorised user.

In the suggested cryptosystem, a plaintext represented by an N dimensional Boolean vector $\boldsymbol{\xi} \in (0,1)^N$ is encrypted to the M dimensional Boolean ciphertext $\boldsymbol{J}$ using a predetermined Boolean matrix G, of dimensionality $M \times N$, and a corrupting M dimensional vector $\boldsymbol{\zeta}$, whose elements are 1 with probability p and 0 otherwise, in the following manner $\boldsymbol{J} = G\ \boldsymbol{\xi}\ + \boldsymbol{\zeta}$, where all operations are (mod 2). The corrupting vector $\boldsymbol{\zeta}$ is chosen at the transmitting end. The matrix G, which is at the heart of the encryption/decryption process is constructed by choosing two randomly-selected sparse matrices A $(M \times N)$ and B $(M \times M)$, and a dense matrix D $(N \times N)$, defining $G = B^{-1}AD \pmod 2$. The matrices A and B are similar to those used in other MN constructions; the dense invertible Boolean matrix D is arbitrary and is added for improving the system's security. Authorised decryption follows a similar procedure to decoding corrupted messages in LDPC codes (i.e., using BP), while an unauthorised user will find the decryption to be computationally hard [20].

5 Conclusions

We showed how the methods of statistical physics can be employed to investigate error-correcting codes and related areas, by studying the typical case characteristics of a given system. This approach provides a unique insight by examining macroscopic properties of stochastic systems, carrying out explicit averages over ensembles of codes that share the same macroscopic properties.

The results obtained shed light on the properties that limit the theoretical and practical performance of parity check codes, explain the differences between

Gallager and MN constructions, explores the role of irregularity, finite size effects and non-binary alphabets in LDPC constructions.

We believe that methods developed over the years in the statistical physics community can make a significant contribution also in other areas of information theory. Research in some of these areas, such as CDMA and image restoration is currently underway.

Support by Grants-in-aid, MEXT (13680400) and JSPS (YK), The Royal Society and EPSRC-GR/N00562 (DS) is acknowledged. We would like to acknowledge the contribution of Kazutaka Nakamura and Naoya Sazuka to this research effort.

References

1. Shannon, C.E.: A Mathematical Theory of Communication: Bell Sys. Tech. J., **27** (1948) 379-423, 623-656.
2. Berrou, C. & A. Glavieux: Near Optimum Error Correcting Coding and Decoding - Turbo-codes: IEEE Transactions on Communications **44** (1996) 1261-1271.
3. MacKay, D.J.C.: Good Error-correcting Codes Based on Very Sparse Matrices: IEEE Transactions on Information Theory **45** (1999) 399-431.
4. Gallager, R.G.: Low-density Parity-check Codes: IRE Trans. Info. Theory **IT-8** (1962) 21-28 . Gallager, R.G.: Low-density Parity-Check Codes, MIT Press, Cambridge, MA. (1963).
5. Richardson, T., Shokrollahi, A., Urbanke, R.: Design of Provably Good Low-density Parity-check Codes: IEEE Transactions on Information Theory (1999) in press .
6. Pearl, J.: Probabilistic Reasoning in Intelligent Systems. Morgan Kaufmann, San Francisco (1988).
7. Nishimori, H.: Statistical Physics of Spin Glasses and Information Processing. Oxford University Press, Oxford UK (2001).
8. Thouless, D.J., Anderson, P.W., Palmer, R.G.: Solution of 'Solvable Model of a Spin Glass': Philos. Mag. (1977) **35**, 593-601.
9. Sourlas, N.: Spin-glass Models as Error-correcting Codes: Nature **339** (1989) 693-695.
10. Kabashima, Y., Murayama, T., Saad, D.: Typical Performance of Gallager-type Error-Correcting Codes: Phys. Rev. Lett. **84** (2000) 1355-1358.
11. Vicente, R., Saad, D., Kabashima, Y.: Error-correcting Code on a Cactus - a Solvable Model: Europhys. Lett. **51**, (2000) 698-704.
12. Nishimori, H.: Internal Energy, Specific Heat and Correlation Function of the Bond-random Ising Model: Prog.Theo.Phys. **66** (1981) 1169-1181.
13. Kanter, I., Saad, D.: Error-Correcting Codes That Nearly Saturate Shannon's Bound : Phys. Rev. Lett. **83** (1999) 2660-2663. Kanter, I., Saad, D.: Finite-size Effects and Error-free Communication in Gaussian Channels: Journal of Physics A **33** (2000) 1675-1681.
14. Vicente, R., Saad, D., Kabashima, Y.: Statistical Physics of Irregular Low-Density Parity Check Codes: Jour. Phys. A **33** (2000) 6527-6542.
15. Nakamura, K., Kabashima, Y., Saad, D.:Statistical Mechanics of Low-Density Parity Check Error-Correcting Codes Over Galois Fields: Europhys. Lett. (2001) in press.

16. Davey, M.C., MacKay, D.J.C: Low Density Parity Check Codes Over $GF(q)$: IEEE Comm. Lett., **2** (1998) 165-167.
17. Lidl, R., Niederreiter, H.: Introduction to Finite Fields and their Applications: Cambridge University Press, Cambridge, UK (1994).
18. Gallager, R.G.: Information Theory and Reliable Communication: Weily & Sons, New York (1968).
19. Kabashima, Y., Sazuka, N., Nakamura, K., Saad, D.: Tighter Decoding Reliability Bound for Gallager's Error-Correcting Code: Phys. Rev. E (2001) in press.
20. Kabashima, Y., Murayama, T., Saad, D.: Cryptographical Properties of Ising Spin Systems: Phys. Rev. Lett. **84** (2000) 2030-2033. Saad, D., Kabashima, Y., Murayama, T.: Public Key Cryptography and Error Correcting Codes as Ising Models. In: Sollich, P., Coolen, A.C.C., Hughston, L.P., Streater, R.F. (eds): Disordered and Complex Systems. American Institute of Physics Publishing, Melville, New York (2001) 89-94.