Papers

On polynomial invariants of linear codes
Alexander Barg

Cluster expansions in dilute systems: application to satisfiability problems and spin glasses
G. Semerjian, L.F. Cugliandolo (clusters.ps)

Codes on graphs: normal realizations
G. David Forney Jr. (CGNR.ps)

Codes on graphs: news and views
G. David Forney Jr. (CISS−GDF.ps)

Links on Codes

David MacKay Links on Codes
(this gives data files, software, performance curves, etc.)

David MacKay Home Page

Jonathan Yedidia Home Page

Robert J. McEliece Home Page

David Saad: Publications http://www.ncrg.aston.ac.uk

Radford Neal − LDPC software package
http://www.cs.toronto.edu/~radford/ldpc.software.html

Some references on the cond−mat data base on the physicists' work on Error Correcting Codes

Statistical Mechanics and error−correction Codes
Nicolas Sourlas

Comments: Proceedings of the Marseille Satellite Colloquium "Mathematical Results in Stat. Mechanics"
Subj−class: Statistical Mechanics

Abstract
I will show that there is a deep relation between error−correction codes and certain mathematical models of spin glasses. In particular minimum error probability decoding is equivalent to finding the ground state of the corresponding spin system. The most probable value of a symbol is related to the magnetization at a different temperature. Convolutional codes correspond to one−dimensional spin systems and Viterbi's decoding algorithm to the transfer matrix algorithm of Statistical Mechanics. A particular spin−glass model, which is exactly soluble, corresponds to an ideal code, i.e. a code which allows error−free communication if the rate is below channel capacity.

Finite−connectivity systems as error−correcting codes
Renato Vicente, David Saad, Yoshiyuki Kabashima

Comments: 32 pages, 12 figures, to appear in PRE
Subj−class: Disordered Systems and Neural Networks

Abstract

We investigate the performance of parity check codes using the mapping onto Ising spin systems proposed by Sourlas. We study codes where each parity check comprises products of K bits selected from the original digital message with exactly C checks per message bit. We show, using the replica method, that these codes saturate Shannon's coding bound for $K\to\infty$ when the code rate K/C is finite. We then examine the finite temperature case to asses the use of simulated annealing methods for decoding, study the performance of the finite K case and extend the analysis to accommodate different types of noisy channels. The connection between statistical physics and belief propagation decoders is discussed and the dynamics of the decoding itself is analyzed. Further insight into new approaches for improving theÊ code performance is given.

Error−Correcting Codes That Nearly Saturate Shannon's Bound
Ido Kanter, David Saad

Comments: 4 pages, 3 figures, submitted to Phys. Rev. Lett.
Subj−class: Disordered Systems and Neural Networks

Abstract

Gallager−type error−correcting codes that nearly saturate Shannon's bound are constructed using insight gained from mapping the problem onto that of an Ising spin system. The performance of the suggested codes is evaluated for different code rates in both finite and infinite message length.

Typical Performance of Gallager−type Error−Correcting Codes
Yoshiyuki Kabashima, Tatsuto Murayama, David Saad

Comments: 6 pages, latex, 1 figure
Subj−class: Disordered Systems and Neural Networks

Abstract

The performance of Gallager's error−correcting code is investigated via methods of statistical physics. In this approach, the transmitted codeword comprises products of the original message bits selected by two randomly−constructed sparse matrices; the number of non−zero row/column elements in these matrices constitutes a family of codes. We show

that Shannon's channel capacity is saturated for many of the codes while slightly lower performance is obtained for others which may be of higher practical relevance. Decoding aspects are considered by employing the TAP approach which is identical to the commonly used belief−propagation−based decoding.

Statistical Physics of Irregular Low−Density Parity−Check Codes
Renato Vicente, David Saad, Yoshiyuki Kabashima

Comments: 20 pages, 9 figures, revised version submitted to JPA
Subj−class: Disordered Systems and Neural Networks
Journal−ref: J. Phys. A 33 (2000) 6527−6542

Abstract

Low−density parity−check codes with irregular constructions have been recently shown to outperform the most advanced error−correcting codes to date. In this paper we apply methods of statistical physics to study the typical properties of simple irregular codes. We use the replica method to find a phase transition which coincides with Shannon's coding bound when appropriate parameters are chosen. The decoding by belief propagation is also studied using statistical physics arguments; the theoretical solutions obtained are in good agreement with simulations. We compare the performance of irregular with that of regular codes and discuss the factors that contribute to the improvement in performance.

The statistical mechanics of turbo codes
A.Montanari, N.Sourlas

Comments: 23 pages, 6 figures: Fig.2 has been replaced (in the preceeding version it was identical to Fig.1)
Report−no: LPTENS 99/29
Subj−class: Disordered Systems and Neural Networks; Statistical Mechanics

Abstract

The "turbo codes", recently proposed by Berrou et. al. are written as a disordered spin Hamiltonian. It is shown that there is a threshold Theta such that for signal to noise ratios v^2 / w^2 > Theta, the error probability per bit vanishes in the thermodynamic limit, i.e. the limit of infinitely long sequences. The value of the threshold has been computed for two particular turbo codes. It is found that it depends on the code. These results are compared with numerical simulations.

The Statistical Physics of Regular Low−Density Parity−Check Error−Correcting Codes
Tatsuto Murayama, Yoshiyuki Kabashima, David Saad, Renato Vicente

Comments: 35 pages, 4 figures
Subj−class: Disordered Systems and Neural Networks; Statistical Mechanics

Abstract

A variation of Gallager error−correcting codes is investigated using statistical mechanics. In codes of this type, a given message is encoded into a codeword which comprises Boolean sums of message bits selected by two randomly constructed sparse matrices. The similarity of these codes to Ising spin systems with random interaction makes it possible to assess their typical performance by analytical methods developed in the study of disordered systems. The typical case solutions obtained via the replica method are consistent with those obtained in simulations using belief propagation (BP) decoding. We discuss the practical implications of the results obtained and suggest a computationally efficient construction for one of the more practical configurations.

Turbo codes: the phase transition
Andrea Montanari

Comments: 26 pages, 3 eps figures
Report−no: LPTENS 00/13
Subj−class: Disordered Systems and Neural Networks; Statistical Mechanics

Abstract

Turbo codes are a very efficient method for communicating reliably through a noisy channel. There is no theoretical understanding of their effectiveness. In [1] they are mapped onto a class of disordered spin models. The analytical calculations concerning these models are reported here. We prove the existence of a no−error phase and compute its local stability threshold. As a byproduct, we gain some insight into the dynamics of the decoding algorithm.

Public key cryptography and error correcting codes as Ising models
David Saad, Yoshiyuki Kabashima, Tatsuto Murayama

Comments: 6 pages
Subj−class: Disordered Systems and Neural Networks

Abstract

We employ the methods of statistical physics to study the performance of Gallager type error−correcting codes. In this approach, the transmitted codeword comprises Boolean sums of the original message bits selected by two randomly−constructed sparse matrices. We show that a broad range of these codes potentially saturate Shannon's bound but are limited due to the decoding dynamics used. Other codes show sub−optimal performance but are not

restricted by the decoding dynamics. We show how these codes may also be employed as a practical public−key cryptosystem and are of competitive performance to modern cyptographical methods.

Secure and linear cryptosystems using error−correcting codes
I. Kanter, E. Kanter, L. Ein−Dor

Subj−class: Disordered Systems and Neural Networks
Journal−ref: Europhys. Lett. 51 (15 July), 244 (2000)

Abstract

A public−key cryptosystem, digital signature and authentication procedures based on a Gallager−type parity−check error−correcting code are presented. The complexity of the encryption and the decryption processes scale linearly with the size of the plaintext Alice sends to Bob. The public−key is pre−corrupted by Bob, whereas a private−noise added by Alice to a given fraction of the ciphertext of each encrypted plaintext serves to increase the secure channel and is the cornerstone for digital signatures and authentication. Various scenarios are discussed including the possible actions of the opponent Oscar as an eavesdropper or as a disruptor.

Statistical Mechanics of Low−Density Parity Check Error−Correcting Codes over Galois Fields
Kazutaka Nakamura, Yoshiyuki Kabashima, David Saad

Comments: 7 pages, 1 figure
Subj−class: Statistical Mechanics

Abstract

A variation of low density parity check (LDPC) error correcting codes defined over Galois fields ($GF(q)$) is investigated using statistical physics. A code of this type is characterised by a sparse random parity check matrix composed of C nonzero elements per column. We examine the dependence of the code performance on the value of q, for finite and infinite C values, both in terms of the thermodynamical transition point and the practical decoding phase characterised by the existence of a unique (ferromagnetic) solution. We find different q−dependencies in the cases of C=2 and $C \ge 3$; the analytical solutions are in agreement with simulation results, providing a quantitative measure to the improvement in performance obtained using non−binary alphabets.

The glassy phase of Gallager codes
Andrea Montanari

Comments: 27 pages, 8 eps figures
Report−no: LPTENS 01/19
Subj−class: Disordered Systems and Neural Networks; Statistical Mechanics

Abstract

Gallager codes are the best error−correcting codes to−date. In this paper we study them by using the tools of statistical mechanics. The corresponding statistical mechanics model is a spin model on a sparse random graph. The model can be solved by elementary methods (i.e. without replicas) in a large connectivity limit. For low enough temperatures it presents a completely frozen glassy phase (q_{EA}=1). The same scenario is shown to hold for finite connectivities. In this case we adopt the replica approach and exhibit a one−step replica symmetry breaking order parameter. We argue that our ansatz yields the exact solution of the model. This allows us to determine the whole phase diagram and to understand the performances of Gallager codes.

A review on the methods of statistical physics in optimization problems

Statistical mechanics methods and phase transitions in optimization problems
O.C. Martin, R. Monasson, R. Zecchina

Comments: Review article, 80 pages, uses elsart.cls
Subj−class: Statistical Mechanics; Disordered Systems and Neural Networks

Abstract

Recently, it has been recognized that phase transitions play an important role in the probabilistic analysis of combinatorial optimization problems. However, there are in fact many other relations that lead to close ties between computer science and statistical physics. This review aims at presenting the tools and concepts designed by physicists to deal with optimization or decision problems in an accessible language for computer scientists and mathematicians, with no prerequisites in physics. We first introduce some elementary methods of statistical mechanics and then progressively cover the tools appropriate for disordered systems. In each case, we apply these methods to study the phase transitions or the statistical properties of the optimal solutions in various combinatorial problems. We cover in detail the Random Graph, the Satisfiability, and the Traveling Salesman problems.

References to the physics literature on optimization are provided. We also give our perspective regarding the interdisciplinary contribution of physics to computer science.