Journal of Statistical Physics, Vol. 96, Nos. 3/4, 1999

Statistical Mechanics Approach to Coding Theory

A. Procacci[1] **and B. Scoppola**[2]

Received March 16, 1999; final April 26, 1999

We propose a method based on cluster expansion to study the optimal code with a given distance between codewords. Using this approach we find the Gilbert–Varshamov lower bound for the rate of largest code.

KEY WORDS: Cluster expansion; coding theory.

1. INTRODUCTION

One of the basic problems in coding theory is to find the largest code of a given length and minimum distance. More precisely, one wants to find the quantity $A(n, d)$ = maximum number of codewords in a binary code of length n with minimum distance d between codewords.

Here the codewords are points in an hypercube $\{0, 1\}^n$, and the distance is the Hamming distance, i.e., the number of different digits between two points.

An important problem in this subject is to find the behaviour of $A(n, d)$ for large n, large d and fixed ratio $d/n = \delta$. Such problem, which is obviously very interesting in the applications to the error-correcting codes, is not completely solved. Upper and lower bounds of the rate of *largest code*, i.e., of the quantity $R = 1/n \log_2 A(n, d)$ are available, but the gap between the two bounds is still large, most of all in certain regions, and the existence of $\lim_{n \to \infty} R$ is still unproved. In particular, the lower bound known so far (*Gilbert–Varshamov lower bound*) is the following classical result (see [G], [V], [MS]):

$$R \geqslant 1 - \frac{1}{n} \ln_2 \sum_{k=0}^{\delta n} \binom{n}{k} \tag{1.1}$$

[1] Departamento de Matematica, ICEx-UFMG, Belo Horizonte, Brazil.

[2] Dipartimento di Matimatica, Università "La Sapienza" di Roma, 00185 Rome, Italy.

0022-4715/99/0800-0907$16.00/0

In this paper we propose an approach to this problem based on the standard expansion used in statistical mechanics of lattice systems. By an estimate based on low density expansion it is possible to find easily the bound (1.1). This suggest that the statistical mechanics approach to this problem may give new results.

2. BASIC NOTATION AND DEFINITIONS

In general, if A is any finite set, we denote by $|A|$ the number of elements of A. Given a finite set A, we define a *graph* g in A as a collection $\{\lambda_1, \lambda_2,..., \lambda_m\}$ of distinct pairs of A. The elements of A are called *vertices* of g. The pairs $\lambda_1, \lambda_2,..., \lambda_m$ are called *links* of the graph g, and given a link $\lambda = \{x_1, x_2\}$ we will denote supp $\lambda = x_1 \cup x_2$. We denote by $|g|$ the number of links in g. Given two graphs g and f we say that $f \subset g$ if each link of f is also a link of g.

A graph $g = \{\lambda_1, \lambda_2,..., \lambda_m\}$ in A is said to be *connected* if for any pair B, C of subsets of A such that $B \cup C = A$ and $B \cap C = \emptyset$, there is a $\lambda_i \in g$ such that supp $\lambda_i \cap B \neq \emptyset$ and supp $\lambda_i \cap C \neq \emptyset$. If g is connected, then necessarily $\bigcup_{i=1}^{m}$ supp $\lambda_i = A$; in this case A is also called the *support* of g and it is denoted by supp g.

We denote by G_A the set of all connected graphs in A.

A *tree* graph τ on $\{1,..., n\}$ is a connected graph such that $|\tau| = n-1$. The set of all the tree graph over $\{1,..., n\}$ will be denoted by T_n.

3. HARD SPHERE LATTICE SYSTEMS.

Let Λ be a finite set and denote its elements (sites) by x. Suppose that a distance $d(x, y)$ is defined in Λ, and, $\forall d > 0$, it exists $V_d > 0$ such that (translational invariance) $\sum_{y \in \Lambda : d(x, y) \leqslant d} 1 = V_d$ independent from x. V_d is the volume of the sphere of radius d and center in $x \in \Lambda$.

We want to study here the statistical mechanics of a gas of sphere in Λ interacting only via an hard core potential, i.e., a pair potential of the form

$$U(x_i, x_j) = \begin{cases} +\infty & \text{if} \quad d(x_i, x_j) \leqslant d \\ 0 & \text{otherwise} \end{cases} \tag{3.1}$$

The grand-canonical partition function Ξ_Λ, for a fixed activity z is given by

$$\Xi_\Lambda = 1 + \sum_{k \geqslant 1} z^k \frac{1}{k!} \sum_{x_1,..., x_k \in \Lambda} e^{-\sum_{1 \leqslant i \leqslant j \leqslant k} U(x_i, x_j)} \tag{3.2}$$

The logarithm of this partition function can be written as a formal series in power of z through a standard Mayer expansion

$$\log \Xi_\Lambda = \sum_{N \geqslant 1} c_N z^N \tag{3.3}$$

where, denoting shortly $U_{ij} = U(x_i, x_j)$

$$c_N = \frac{1}{N!} \sum_{x_1,\ldots,x_N \in \Lambda} \sum_{g \in G_N} \prod_{ij \in g} (e^{-U_{ij}} - 1) \tag{3.4}$$

Since by definition U_{ij} is a non negative potential, we can use the Brydges–Battle–Federbush tree graph identity (in the special case of non negative potentials, see, e.g., [B] and [PdLS]). Namely the following inequality holds:

$$\left| \sum_{g \in G_N} \prod_{ij \in g} (e^{-U_{ij}} - 1) \right| \leqslant \sum_{\tau \in T_N} \prod_{ij \in \tau} |e^{-U_{ij}} - 1|$$

hence we immediately get the bound

$$|c_N| \leqslant \frac{1}{N!} \sum_{\tau \in T_N} \sum_{x_1,\ldots,x_N \in \Lambda} \prod_{ij \in \tau} |e^{-U_{ij}} - 1| \tag{3.5}$$

Since, by (3.1),

$$|e^{-U_{ij}} - 1| = \begin{cases} 1 & \text{if} \quad d(x_i, x_j) \leqslant d \\ 0 & \text{if} \quad d(x_i, x_j) > d \end{cases}$$

we have for any tree $\tau \in T_N$ (exploiting translational invariance)

$$\sum_{x_1,\ldots,x_N \in \Lambda} \prod_{ij \in \tau} |e^{-U_{ij}} - 1| = |\Lambda| \; V_d^{N-1} \tag{3.6}$$

Moreover we have, from Cayley's theorem

$$\sum_{\tau \in T_N} 1 = N^{N-2} \tag{3.7}$$

Then we can write

$$|c_N| \leqslant |\Lambda| \, \frac{N^{N-2}}{N!} \, V_d^{N-1} \tag{3.8}$$

(3.8) shows that the formal series of the logarithm of the gran partition function, is absolutely convergent for any $z < 1/eV_d$.

4. GILBERT–VARSHAMOV LOWER BOUND

We can use the general result of the above section in the following framework: let Λ be the hypercube of dimension n, (hence $|\Lambda| = 2^n$) and $d(x_i, x_j)$ the Hamming distance. Let $d = \delta n$. The close-packing configuration (corresponding to the limit $z \to \infty$ at a fixed volume $|\Lambda| = 2^n$) gives an expected value of the number of particles in the gas equal to $A(n, d)$. In an intermediate configuration, i.e., for finite z, such expected value of the number of particles in the system is given by

$$\bar{N} = z \frac{\partial}{\partial z} \log \Xi_\Lambda = |\Lambda| \sum_{N \geqslant 1} N c_N z^N \tag{4.1}$$

The series in r.h.s. of (4.1) is again analytic for $z < 1/eV_d$, and since U_{ij} is positive one can show that $c_N = (-1)^{N-1} |c_N|$ (using tree graph identity; see also [Ru]) and $c_1 = 1$. Using (3.8), for any $z < 1/eV_d$ we can write

$$\bar{N} \geqslant |\Lambda| \left[z - \sum_{N \geqslant 2} \frac{N^{N-1}}{N!} V_d^{N-1} z^N \right] \geqslant |\Lambda| \, z \left[1 - \sum_{N \geqslant 1} \frac{N^N}{(N+1)!} (zV_d)^N \right]$$

Choosing e.g., $z = 1/4eV_d$ and considering that $N^N/(n+1)! \leqslant e^N$ we have

$$\bar{N}\left(z = \frac{1}{4eV_d}\right) \geqslant |\Lambda| \frac{1}{4eV_d} \left[1 - \sum_{N \geqslant 1} 4^{-N} \right] = |\Lambda| \frac{1}{6eV_d} \tag{4.2}$$

The volume V_d is evidently

$$V_d = \sum_{k=0}^{\delta n} \binom{n}{k} \tag{4.3}$$

Since $A(n, d) \geqslant \bar{N}$ for any $z < \infty$ and recalling that $|\Lambda| = 2^n$ we get

$$A(n, d) \geqslant \bar{N}\left(z = \frac{1}{4eV_d}\right) \geqslant 2^n \frac{1}{6e \sum_{k=0}^{\delta n} \binom{n}{k}} \tag{4.4}$$

and therefore

$$R \geqslant 1 - \frac{1}{n} \log_2 \sum_{k=0}^{\delta n} \binom{n}{k} - \frac{\log_2 6e}{n} \tag{4.5}$$

and this gives (1.1) in the limit $n \to \infty$.

It is interesting to outline that using general results in statistical mechanics (see [LP]) it is also possible to write lower bounds for $\bar{N}$ also outside the radius of convergence of the series (4.1). In particular

$$\bar{N} \geqslant |\Lambda| \frac{z}{1+2c_2 z} \qquad \forall z \tag{4.6}$$

By means of (4.6) and $c_2 = V_d/2$ one can find directly a bound for $A(n, d)$, since

$$A(n, d) = \lim_{z \to \infty} \bar{N} \geqslant \lim_{z \to \infty} \frac{z}{1+2c_2 z} = \frac{|\Lambda|}{V_d} \tag{4.7}$$

and this gives directly (1.1). Note that it is possible to find more refined lower bounds of the density of our lattice gas (see again [LP]), involving subsequent coefficients c_k, but unfortunately such estimates do no affect the exponential dependence of the density from n.

5. CONCLUSIONS

The result of this short letter is simple and straightforward, but it is in some sense unexpected, because it shows how a rough estimate in the low density region of the statistical mechanics model gives a lower bound of the rate of the best code equal to the best lower bound available in information theory. A direct lower bound of the rate is also possible, see (4.7), but the result does not change. Possible developments of this work in order to obtain a rigorous upper bound of the rate of the best codes are more difficult, due to the fact that the "ground state" of the statistical mechanics is unknown. Also classical *a priori* upper bound for $\bar{N}$ (see [LP]) are unuseful, because they are meaningless in the limit $z \to \infty$, and we are forced to study such limit in order to obtain an upper bound for $A(n, d)$. However very interesting developments would be possible (namely the proof of the tightness of Gilbert–Varshamov bound) if the absence of phase transitions for this system could be proved. We have a rough indication in this direction: simple computations seem to show that in the limit $n \to \infty$ the coefficients c_N become of the form $c_N = V_d^{N-1} b_N$, with b_N independent from n, d, and this feature was used by various authors to argue the absence of phase transitions in similar models (e.g. for hard spheres in infinite dimensions).

ACKNOWLEDGMENTS

This problem was suggested to us by Y. Suhov, and we want to thank him also for his encouragements. We had fruitful discussions with

M. Cassandro, A. Pellegrinotti and P. Picco. We thank J. Lebowitz for pointing out the reference [LP] and for interesting suggestions and comments. The work of A.P. was partially supported by CNPq and FAPEMIG, and that of B.S. by CNR, GNFM.

REFERENCES

[B] D. Brydges, *A Short Course on Cluster Expansion*, Les Houches 1984, K. Osterwalder and R. Stora, eds. (North Holland Press, 1986).

[G] E. N. Gilbert, A comparison of signalling alphabets, *Bell Syst. Tech. Jnl.* **31**:504–522 (1952).

[LP] J. L. Lebowitz and J. K. Percus, Integral equations and inequalities in the theory of fluids, *J. Math. Phys.* **4**:1495–1506 (1963).

[MS] F. J. Macwilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Math Library, Vol. 16, 1977).

[PdLS] A. Procacci, B. N. B. de Lima, and B. Scoppola, A remark on high temperature polymer expansion for lattice systems with infinite range pair interactions, *Lett. Math. Phys.* **45**:303–322 (1998).

[Ru] D. Ruelle, *Statistical Mechanics, Rigorous Results* (W. Benjamin inc., 1969).

[V] R. R. Varshamov, Estimate of the number of signals in error correcting codes, *Dokl. Akad. Nauk SSSR* **117**:739–741 (1957).