THE $GL(n,F_p)$ — INVARIANCE OF THE POTTS HAMILTONIAN

MIHAI CARAGIU
Department of Mathematics
Penn State University
218 McAllister Building
University Park, PA 16802 USA

MELLITA CARAGIU
Department of Physics
"Babes-Bolyai" University
Str. M. Kogalniceanu 1
3400 Cluj-Napoca, ROMANIA

(Received June 8, 1995 and in revised form August 8, 1995)

ABSTRACT. After defining a meanfield by arithmetic means, using multiplicative characters of finite fields, its Potts Hamiltonian is exactly computed. Moreover, it proves to be invariant with respect to every change of basis in F_q over the prime field F_p

KEY WORDS AND PHRASES: Finite fields, characters, Hamiltonian invariance
1991 AMS SUBJECT CLASSIFICATION CODES: 11L40, 82B20, 11T24, 51E25.

1. INTRODUCTION

Let us consider the finite field F_q, $q = p^n$, as an n-dimensional vector space over its prime subfield F_p. This is, of course, done by choosing a basis $e = (e_1, e_2, ..., e_2)$ — an (ordered) n-tuple of "vectors" linearly independent over F_p. Then, we can see F_q in a natural way as an n-dimensional hypercubic lattice with size p Every element z of this lattice can be expressed in a unique way as $z = z_1e_1 + .. + z_ne_n$, the coefficients x_i satisfying periodic boundary conditions modulo p (that is, if we substitute $z_i + p$ instead of z_i, the same point z is obtained) That means that the above defined hypercubic lattice can be seen as a discrete model of the n-dimensional torus $T^n = S^1 \times S^1 \times ... \times S^1$ we obtain thus a finite field "wrapped" on a torus.

Suppose now that $r > 1$ is a natural number, and $q \equiv 1 \pmod r$. This happens, for example, if $p \equiv 1 \pmod r$. We may consider then a character (multiplicative) of F_q, that is a surjective morphism of multiplicative groups $f : F_q^* \to U_r$, where U_r is the group of complex r-th roots of unity Then, to every point z of our lattice we associate an r-th root of unity, namely $f(z)$. We obtain thus a discrete analogue for a section of a $U(1)$-bundle over the n-dimensional torus. Also we may see this as a physical field, $f(z)$ being the "spin" attached to site z. Our aim is to study this field using some ideas of statistical mechanics ([1]-basic reference), with the hope of obtaining more information about such pure mathematical entities as characters of finite fields.

2. NEAREST NEIGHBORS

Once we have chosen a basis $e = (e_1, e_2, ..., e_n)$ as above, a natural concept of nearest neighbor sites pops up namely, we say that the sites z and w are e-nearest neighbors, and we denote this by $z \sim w$ (mod e), if the difference $z - w$ belongs to the set $\{e_1, ..., e_n, -e_1, ..., -e_n\}$ Of course, this concept is strongly dependent on the choice of the basis e If we change the basis, it may happen that we obtain a totally different set of nearest neighbor pairs Obviously, if one changes the basis only by permuting the e_i's between themselves, and/or by changing the sign of some of them, the set of nearest neighbor pairs remains the same. Ignoring the action of the symmetric group, this is just $Z/2Z \times ... \times Z/2Z$-invariance, but most of the transformations are not so simple We obtain thus a model for a strange chaotic medium, in which the very idea of nearest neighbor is strongly dependent on the action of $GL(n, F_p)$ — the group which takes care about all base changes in F_q over F_p

3. THE MEANFIELD AND ITS POTTS HAMILTONIAN

We return now to our field f defined on F_q, viewed as an n-dimensional lattice wrapped on T^n We need, in one way or another, to prove that this is a representative field from the randomness point of view, i.e., that it is a "meanfield", in the physical use of the term. This follows from a result [2] about the distribution of the values taken by a multiplicative character of F_q. Namely, let us consider an integer $k < p$. To every z in F_q, we can associate a function $h_z : \{0, 1, ..., k-1\}^n \to U_r$, given as follows

$$h_z(a_1, ..., a_n) := f(z + a_1 e_1 + ... + a_n e_n)\,.$$

The functions h_z can be seen as a means of testing the local state of the field in the e-neighborhood of z represented by a hypercube of size k, with the point z as one of its corners: namely, h_z is only one out of a total of r^{k^n} functions $h : \{0, 1, ..., k-1\}^n \to U_r$. The main result in [2] states that all the functions h have an "almost equal" probability of occurrence as an h_z.

Namely, if we denote by N_h the number of those z in F_q for which $h_z = h$ (k is fixed), we have the following estimate, where we have denoted k^n by b:

$$N_h = (q+1)/r^b + 0(b.q^{1/2})\,, \quad \text{when } q \text{ is large}\,.$$

The proof uses the Lang-Weil estimates applied to an appropriate algebraic curve, whose genus is computed using the Riemann-Hurwitz formula.

Moreover, the constant implied by 0 is smaller than 1.

Now, we can assume that our field is indeed a meanfield, in the most natural sense We are thus ready to define its Potts Hamiltonian:

$$H = \sum_{z \sim w (\text{mod } e)} \delta_{(f(z), f(w))}$$

where $\delta_{(i,j)}$ is 1 if $i = j$ and 0 otherwise (we assume that the elementary energy of interaction [1] is $J = 1$). By definition, it seems that H is dependent on both the basis e and the character choice Of course $GL(n, F_p)$ acts as well on the Hamiltonian H, by an action induced by its action on the basis e (on which the neighbor system is strongly dependent). However, we shall see that the action of $GL(n, F_p)$ on the Hamiltonian is trivial.

4. THE $GL(n, F_p)$-INVARIANCE

We prove now the following theorem.

THEOREM. H does not depend on the choice of the basis e, nor on the character f.

PROOF. First, we may note that one may extend the definition of the character to the whole field by $f(0) := 0$ As a physical interpretation one may consider either the spin 0 at the site $z = 0$, or, maybe better, one may consider in fact a field theory on a punctured torus.

The proof is actually very simple. First, let us consider an apparently more general situation if a is an arbitrary element of F_q^*, we count first the number of those z in F_q for which the character takes the same values at z and $z+a$

If $f(z) = f(z+a)$, then obviously z, $z+a$ are non-zero, and $(z+a)/z = y$ is an r-th power in $F_q^* - \{1\}$ Thus, y can take a number of $(q-r-1)/r$ values, and for every such y, z is uniquely determined

Thus we have found $(q-r-1)/r$ possible values of z with the character taking the same values at z and $z+a$. Take now $a = e_1, e_2, ..., e_n$ In each of these n directions, the number of e-nearest neighbor pairs to which the same spin is assigned is $(q-r-1)/r$ It follows that the total energy or Potts Hamiltonian is exactly given by

$$H = n(q-r-1)/r\,.$$

This computation, in fact, proves the $GL(n, F_p)$-invariance, because, as one can see, the above relation for H does not depend on e or on f.

REMARK 1. The same invariance property holds also (if one takes $r = 2$) for the Ising Hamiltonian [1].

REMARK 2. One may work also with more general extensions of finite fields and obtain in a similar way a concept of e-nearest neighbor for every basis of F_{q^n} over F_q but the prime field F_p is more suitably to be taken as a base field, due to its interpretation as a linear spatial array

REMARK 3. For $n = 1$, the change of basis is, in fact, a rescaling. Thus, we get, in this particular case, the "scale-invariance" of the Potts Hamiltonian. If one chooses another scale e, the elements of the F_p^* are reordered as $e, 2e..., (p-1)e$, and the worst that can happen is the interchange of quadratic residues and nonresidues.

5. FURTHER COMMENTS

The most natural step forward would be to define a partition function Z.

It is known [1] that all the information about a statistical system is hidden in the partition function Our hope is to define an appropriate Z in order to get, via its analytic properties, new insights concerning this strange connection between the arithmetic of finite fields and field theory.

Recall that in order to define Z, we need a set of states. Then, we attach a Boltzmann weight [1] to every state in this set. Z will be the sum of all these weights. Hopefully, in the case of a field associated with a character f of F_q^* the Boltzmann weight has a simple form:

$$W(f) = \exp(-\beta n(q-r-1)/r)$$

where r is the order of f, n the dimension of the space, and β a parameter playing the role of inverse temperature. Note that q is the lattice volume

In order to obtain a proper Z, one has to select with great care a set of states satisfying two basic requirements. First, it should not be a "small" set (otherwise the formalism of statistical mechanics will be useless). Second, the selected states must be meaningful from an arithmetical point of view, that is, closely related to the multiplicative characters.

However, the total number of multiplicative characters of F_q is $q-1$, which is rather small even if we fix r, the number of r-valued spin distributions on F_q^* is r^{q-1}. In order to deal with a larger number of states, one may choose to take into account the meanfield property (see section 3). Namely, for every divisor r of $q-1$, we will select a character f_r of order r (we shall call it a "basic state"). By the meanfield property we will agree to consider every such basic state f_r as an average field out of a total number of r^{q-1} r-valued random spin distributions on our punctured torus. Thus, in the expression of Z we have to multiply the Boltzmann weight $W(f_r)$ with a corresponding factor of r^{q-1}. If we restrict, for example, the multiplicity of the spin to a single value r, then for every $q \equiv 1 \pmod r$ we get

$$Z = r^{q-1}W(f_r) = \exp((q-1)\log r - \beta n(q-1-r)/r)\,.$$

One may note that the function $G(\beta) := -\lim_q (\log Z)/\beta q$ — that is, the so-called Gibbs free energy density (in thermodynamical limit) presents in this case a sign change at $\beta = (r/n)\log r$

On the other hand, if the multiplicity of r of the spin is unrestricted, that is if r can be every divisor of $q-1$, the partition function will be given by a sum over the divisors of $q-1$, namely

$$Z = \sum_{r|q-1} r^{q-1}W(f_r)\,.$$

More generally, one may consider some special class of divisors of $q-1$. Then, the partition function Z will be the associated divisor sum. This could lead us to some deep arithmetical problems

For an explicit selection of new states, without making use of the meanfield approach, one may consider the set of all "$GL(n, F_p)$-gauge invariant functions: $g : F_q^* \to U_r$, that is, functions for which the Potts Hamiltonian is well defined (does not depend on the choice of the basis of F_q over F_p) The partition function can be written then as the sum over all such g of the Boltzmann weights $\exp(-\beta H(g))$, where $H(g)$ is the Hamiltonian associated to the function g

REFERENCES

[1] BAXTER, J., *Exactly Solved Models in Statistical Mechanics*, London, New York, Academic Press, 1982.

[2] CARAGIU, M. and MULLEN, G., L., The distribution of r-th powers in finite fields, Penn State University Preprint, PM 161/1993.

Advances in Operations Research

Advances in Decision Sciences

Journal of Applied Mathematics

Algebra

Journal of Probability and Statistics

The Scientific World Journal

International Journal of Differential Equations

Hindawi

Submit your manuscripts at
http://www.hindawi.com

International Journal of Combinatorics

Advances in Mathematical Physics

Journal of Complex Analysis

Journal of Mathematics

Mathematical Problems in Engineering

Abstract and Applied Analysis

Discrete Dynamics in Nature and Society

International Journal of Mathematics and Mathematical Sciences

Journal of Discrete Mathematics

Journal of Function Spaces

International Journal of Stochastic Analysis

Journal of Optimization