

Birational mappings and matrix subalgebra from the chiral Potts model

E. Preissmann,^{1,a)} J.-Ch. Anglès d'Auriac,^{1,b)} and J.-M. Maillard^{2,c)}

¹*Département MCBT, Institut Neel, 25 Av. des Martyrs, BP 166,*

38042 Grenoble Cedex 09, France

²*LPTMC, Tour 24, case 121, 4, Place Jussieu, 75252 Paris Cedex 05, France*

(Received 18 February 2008; accepted 30 October 2008; published online 9 January 2009)

We study birational transformations of the projective space originating from lattice statistical mechanics, specifically from various chiral Potts models. Associating these models with *stable patterns* and *signed patterns*, we give general results which allow us to find *all* chiral q -state spin-edge Potts models when the number of states q is a prime or the square of a prime, as well as several q -dependent family of models. We also prove the absence of monocolored stable signed pattern with more than four states. This demonstrates a conjecture about cyclic Hadamard matrices in a particular case. The birational transformations associated with these lattice spin-edge models show complexity reduction. In particular, we recover a one-parameter family of integrable transformations, for which we give a matrix representation when the parameter has a suitable value. © 2009 American Institute of Physics. [DOI: 10.1063/1.3032564]

I. INTRODUCTION AND PRESENTATION

In a previous publication¹ a set of birational transformations acting on projective spaces of various dimensions has been introduced. These transformations are birational realizations of Coxeter groups. They arise naturally in lattice statistical mechanics in relation with the Yang–Baxter equations for solving vertex models and star-triangle relation for solving spin model.^{2,3} However, it is important to note that these birational symmetries are actually symmetries of the lattice of statistical mechanics models beyond the Yang–Baxter integrable situations: they can be seen as (generically infinite) discrete and nonlinear symmetries of the parameter space of the model and, for instance, of the phase diagram of these lattice models.⁴ These transformations can, in fact, be considered *per se* as discrete dynamical system. The degree complexity (or entropy) of these transformations has been evaluated.^{5–7} An unexpected complexity reduction has been found, and it has been conjectured that the most general Potts model has the *same* complexity as the most general cyclic Potts model. Considering that the most general cyclic chiral Potts model has only q homogeneous parameters while the most general Potts model has q^2 homogeneous parameters, the equality between their respective complexities is not obvious. In this paper we go further and study many particular cyclic spin-edge Potts models and their associated birational transformations. As it is described below finding spin-edge cyclic chiral Potts models for lattice statistical mechanics amounts to finding the so-called stable patterns. This problem turns out to be related to many interesting fields of mathematics: Bose–Mesner algebra,⁸ association schemes,⁹ Hadamard matrices (one of our results demonstrates a particular case of a conjecture about Hadamard matrices^{10,11}), Gauss identity, etc.

A q -state Potts model¹² is completely defined by a lattice and a Boltzmann weight matrix W . The spins, which have q states, are located at the vertices of a graph, with *oriented* edges. The

^{a)}Electronic mail: emmanuel.preissmann@gmail.com.

^{b)}Electronic mail: dauriac@grenoble.cnrs.fr.

^{c)}Electronic mail: maillard@lptmc.jussieu.fr.

Boltzmann weight of a given spin configuration is the product of the Boltzmann weight over all edges, hence named *spin-edge* model. The Boltzmann weight of the edges can be conveniently seen as a matrix: the rows refer to the beginning i of the oriented edge, and the column to the end j . The weight of the oriented edge (i, j) is $W(\sigma_i, \sigma_j)$. The so-called inverse relation^{13,14} implies a functional relation between the partition function of a model associated with a matrix and the model associated with its inverse for the same lattice.

By definition a chiral Potts model is a model for which the entries W_{ij} and W_{ji} are different, i.e., the Boltzmann weight matrix is not symmetric. Of particular interest are the cyclic chiral models for which the Boltzmann weights W_{ij} are functions of $i-j \bmod q$. This class contains, in particular, the integrable chiral Potts models.^{15,16} The global symmetries of the cyclic models have been classified in Ref. 17. The most general cyclic Potts model corresponds to the case where there is no other constraint. It means that the Boltzmann weight matrix W is cyclic. Now we can look for other less general models, obtained by imposing further constraints on the entries of W . The simplest constraints are equalities between some entries of the matrix W , but we will also consider the case where these constraints are “antiequalities,” i.e., we demand that some pairs of entries are opposite. Imposing that two Boltzmann weights that are opposite could appear unphysical but, as it will be explained below, it is mathematically very natural.

However, these constraints need to be compatible with the inversion relation mentioned above, as well as with a Hadamard inverse described below. The aim of this paper is to find such matrices and the associated birational transformations. It is organized as follows: we first recall some definitions and what is already known on this problem. We then generalize the notions used in this framework and gather together the notations we use. The next two sections are devoted to our analytical results. These results are grouped into two sections, depending whether the result is directly of importance from the lattice statistical mechanics point of view or not. In Sec. II we first present our more mathematical results. In contrast, the results corresponding to lattice statistical physics are all given in Sec. III A, while the proofs, together with comments and examples, are given in Sec. III B. The content of Sec. III is more “Potts model oriented” and as far as (Boltzmann weight spin-edge) matrices are concerned, focused on particular subcases of cyclic matrices, with an attempt to perform an exhaustive classification of the interesting spin-edge Potts models. We give *all* chiral Potts models when the number of colors q is a square or the square of a prime. In some cases we also study the degree complexity of the birational transformations canonically associated with these subcases of cyclic matrices. Here also results are gathered in Sec. III A and the proofs in Sec. III B. Then, in Sec. IV, we turn to the cases where we were not able to find analytical results and introduce a computer-aided method which enable us to perform some calculation despite the huge combinatorial of this problem. We then present these results.

As far as applications to spin-edge q -state Potts models are concerned our main results correspond to finding the stable patterns, or in other words, the “interesting lattice statistical mechanics spin-edge models,” when q , the number of states of the q -state Potts model, is a prime or the square of a prime, and providing some first steps for results when the number of states is the product of two primes. We also have, as a by-product, other more specific results, such as a demonstration of a conjecture about Hadamard matrices (for monocolored stable patterns). Beside the rigorous proofs, we give numerous examples, most of them in the appendices. We have tried to be rigorous in the demonstration but pedagogical in the examples. The reader more interested in the “lattice statistical mechanics point of view” can skip the more mathematical Sec. II; in particular, the lemma which are more technical. However, we feel that the results of this section are worthwhile *per se* and can be useful to go further in the classification of the Potts models.

A. Recalls

1. The context

Starting from the lattice statistical mechanics point of view, we consider an anisotropic Potts model on a square lattice with Boltzmann weight matrix W_h for the horizontal edges and W_v for the vertical edges. It has been shown¹³ that if $T(W_h, W_v)$ is the transfer matrix of this model then

$$T(W_h, W_v)T(W_h^{-1}, J(W_v)) = C(W_v)\mathbb{I},$$

where $J(W)$ designates the matrix which entries are the inverse of the entries of W (see below). Transporting this equality to the eigenvalues of T permits to find a functional relation for the partition function of the model. This functional relation induces a constraining symmetry for the phase diagram.

We now adopt a more general point of view and we consider the $q \times q$ matrices projectively as elements of $\mathbb{C}P_{q^2-1}$ (since Boltzmann weight matrices are defined up to a multiplicative constant). Using the same notation as in Ref. 18, we define $K=I \circ J$, where I is the usual matrix inverse $I(M)=M^{-1}$ and J is the Hadamard inverse (inverse of the Hadamard product) defined by $(J(M))_{ij}=1/M_{ij}$. The transformations I and J are two noncommuting involutions, which can be represented polynomially in $\mathbb{C}P_{q^2-1}$. In this representation I replaces each entry of M by its cofactor and J replaces each entry by the product of all other entries. It is clear that K and its inverse $K^{-1}=J \circ I$ are both rational transformations. At each step, the q^2 entries of the matrix M are factorized as products of polynomial with integer coefficients, and the common factors of all the entries are discarded.

2. Degree complexity

A quantity characterizing the complexity is the degree complexity λ .⁵⁻⁷ We simply recall the definition

$$\lambda = \lim_{n \rightarrow \infty} \frac{1}{n} \log d_n,$$

where d_n is the degree of the n th iterate K^n , where K is represented as q homogeneous polynomials of degree d . Without the factorizations $d_n=d^n$ and consequently $\lambda=\log d$. For some transformations one has $d_n \sim \delta^n$ with $\delta < d$, this is called a *complexity reduction*.^{19,20} When the growth of the degree is polynomial, one has $\lambda=0$ and the transformation is integrable.²¹ Finally we define the degree generating function as

$$f(x) = \sum_{n=0}^{\infty} d_n x^n \quad (1)$$

when this series has a positive radius of convergence.

3. (I, J)-stable patterns

We consider a disjoint partition $P=\{E_0, \dots, E_{r-1}\}$ of the indices with $\sqcup_{k=0}^{r-1} E_k = \{(i, j), i, j = 0, \dots, n-1\}$, where the symbol \sqcup denotes the disjoint union, we call r the number of colors, and we consider a matrix M such that

$$(i, j) \in E_k \quad \text{and} \quad (i', j') \in E_k \Rightarrow M_{ij} = M_{i'j'}.$$

A matrix verifying this set of equalities is said to belong to the *pattern* P as in Ref. 1. We are interested in the matrices belonging to the same pattern as their image by K . Therefore we will consider pattern containing at least one invertible matrix (for example, we exclude the pattern where all entries are equal). Obviously the transformation J is compatible with any pattern. Therefore a matrix and its K -image will belong to the same pattern if and only if this matrix and its inverse belong to the same pattern. Such a pattern is called *inverse stable*. The number r of subset of the partition is called the number of colors. The transformation associated with a stable pattern with r colors acts on $\mathbb{C}P_{r-1}$.

4. Cyclic matrices

Consider the set of $q \times q$ cyclic matrix M_c with entries $M_c(i, j)$ such that

$$M_c(i, j) = M_c(0, i - j \bmod q). \quad (2)$$

The corresponding model of lattice statistical mechanics is the cyclic chiral Potts model.^{15,16} Chiral refers to the fact that $M_c(i, j)$ is not necessarily equal to $M_c(j, i)$ (the lattice has an orientation) and cyclic refers to the fact that one restricts to cyclic Boltzmann weight matrices. The corresponding pattern is inverse stable and also matrix-product stable (see next Sec. I B). Since a cyclic matrix is fully determined by its first row, the transformation K can be represented in $\mathbb{C}P_{q-1}$. It is found that complexity reduction does occur for cyclic matrices and the complexity is the largest root of $x^2 + (2 - (q-2)^2)x + 1$.²² From numerical analysis it has been conjectured that this value for the algebraic complexity is the same as for arbitrary matrices without any constraint on the entries. Another inverse-stable pattern is provided by cyclic and symmetric matrices. In that case the complexity reduction is even bigger and the complexity is the root of largest modulus of $x^2 + (2 - (p-1)^2)x + 1$, where $p = \lfloor q/2 \rfloor + 1$ where $\lfloor \cdot \rfloor$ denotes the integer part. One aim of this paper is to find some subspaces where further complexity reduction takes place.²³

B. Generalizations

1. Product stability

A pattern is said to be product stable if the product of two matrices belonging to this pattern also belongs to this pattern. Using the Cayley–Hamilton theorem, one can express the inverse of a matrix M as a linear combination of its $q-1$ first powers. Therefore product stability implies inverse stability. We are going to present examples where the reciprocal proposition is wrong. From now on we call P -stable a pattern which is product stable, I -stable a pattern which is inverse stable, and $I\bar{P}$ -stable a pattern which is inverse stable but not product stable. An obvious example is the symmetric matrices which are inverse stable (the inverse of a symmetric matrix is symmetric) but are not product stable (the matrix product of two symmetric matrices is not necessarily symmetric).

2. Generalization of the notion of pattern: Signed patterns

We generalize the notion of pattern and look for a set of r independent $q \times q$ matrices M_i such that

$$K \left(\sum_{i=0}^{r-1} x_i M_i \right) = \sum_{i=0}^{r-1} y_i M_i.$$

Let us introduce the characteristic function χ which associates with each set of indices E the matrix $\chi(E)$ defined by

$$(\chi(E))_{ij} = \begin{cases} 1 & (i, j) \in E \\ 0 & (i, j) \notin E. \end{cases}$$

The patterns defined in the previous paragraph correspond to

$$M_k = \chi(E_k). \quad (3)$$

For reasons explained below, we also consider the more general case of matrices with entries 0, 1, or -1 ,

$$M_k = \chi(E_k^+) - \chi(E_k^-). \quad (4)$$

We call the partition $\{E_0^+, E_0^-, \dots, E_{r-1}^+, E_{r-1}^-\}$ a *signed pattern* and r the number of colors. The algebra generated by these matrices is J -stable. The notion of “signed patterns” simply corresponds to the notion of patterns defined by equalities between entries *up to a sign*.

3. Stability of signed patterns

A product-stable set of matrices with entries 0 or 1 and which sums up to the all one entry matrix is called an *association scheme*.⁹ It is an algebra. If the matrices are also symmetric, then it is a *Bose–Mesner algebra*.⁸

The problem we address in this paper can be summarized as finding r $q \times q$ matrices M_i with entry 0, 1, -1 verifying

$$\sum_{i=1}^r |(M_i)_{jk}| = 1 \quad \forall j, k$$

and

$$\left(\sum_{i=1}^r x_i M_i \right) \left(\sum_{i=1}^r y_i M_i \right) = \sum_{i=1}^r z_i M_i \quad (5)$$

for P -stability and

$$\left(\sum_{i=1}^r x_i M_i \right)^{-1} = \sum_{i=1}^r z_i M_i \quad (6)$$

when the inverse of $\sum_{i=1}^r x_i M_i$ exists for I -stability. From the definition, the matrices induced by a P -stable pattern form an algebra. But the matrices induced by I -stable patterns do not always (in contrast with the problem studied in Ref. 17).

Note that if a set of matrices $\{M_i\}$ defines an algebra, so does the set $\{P_\sigma^{-1} M_i P_\sigma\}$, where σ is a permutation of $\{0, \dots, q-1\}$ and P the associated permutation matrix $(P_\sigma)_{ij} = \delta_{i, \sigma(j)}$. However, if M is a cyclic matrix, $P_\sigma^{-1} M P_\sigma$ is not necessarily a cyclic matrix.

C. Notations and definitions

- (i) From now on we will restrict ourselves to cyclic matrices. As far as notations are concerned, we identify a cyclic matrix and its first row seen as a vector in $\mathbb{C}P_{q-1}$. Let $\mathbf{v} \in \mathbb{C}^q$ be a vector, we use the notation $\text{Cy}(\mathbf{v})$ to denote the $q \times q$ matrix

$$(\text{Cy}(\mathbf{v}))_{ij} = v_{i-j}$$

and $\text{Diag}(\mathbf{v})$ to denote the $q \times q$ matrix

$$(\text{Diag}(\mathbf{v}))_{ij} = v_i \delta_{ij}.$$

δ is a Kronecker symbol.

- (ii) As already mentioned in Sec. I, the discrete Fourier transform plays a crucial role for stability of cyclic matrices. We therefore define the matrix $U = (\omega^{ij})$, where $\omega = \exp(2\pi/q)l$, and use the notation

$$\hat{\mathbf{x}} = U\mathbf{x}$$

to denote the Fourier transform of the vector $\mathbf{x} \in \mathbb{C}^q$. We note the relation

$$U^* \times \text{Cy}(\mathbf{x}) \times U = q \text{Diag}(\hat{\mathbf{x}}), \quad (7)$$

which will be useful. For the reader familiar with lattice statistical mechanics, U is the generalization of the Kramers–Wannier duality, however, it is *not* a transformation of order 2, but of order 4.

- (iii) When patterns are *explicitly* given, we use a straightforward representation: we put in a bracket the entries of the first row. An example is given with the comments in Appendix A.
- (iv) The subspace spanned by the set of vectors $\{\mathbf{v}(i)\}_{i=1 \dots r}$ with complex coefficients is denoted

$$\bigoplus_{1 \leq i \leq r} \mathbb{C}\mathbf{v}(i).$$

- (v) We use arithmetic modulo q , \mathbb{Z}_q^* is the set of elements of \mathbb{Z}_q which are invertible, and if d is a divisor of q (noted $d|q$), one introduces

$$\mathbb{Z}(q, d) = \{k \in \mathbb{Z}_q \mid \gcd(k, q) = d\}.$$

- (vi) We will also use the convolution product (noted \star) and the Hadamard product (noted \cdot) between two vectors of \mathbb{C}^q defined, respectively, by

$$(\mathbf{u} \star \mathbf{v})_i = \sum_{j=0}^{q-1} u_j v_{i-j},$$

$$(\mathbf{u} \cdot \mathbf{v})_i = u_i v_i.$$

It is straightforward to see that $\text{Cy}(\mathbf{u})\text{Cy}(\mathbf{v}) = \text{Cy}(\mathbf{u} \star \mathbf{v})$. With these notations, Eq. (7) reads

$$\widehat{\mathbf{u} \star \mathbf{v}} = q \hat{\mathbf{u}} \cdot \hat{\mathbf{v}}.$$

We note $\mathbf{u}^{\star n}$ the convolution product of \mathbf{u} with itself n times. By convention $\mathbf{u}^{\star 0} = \chi(\{0\})$. Keeping in mind that diagonalization of the cyclic matrices requires the discrete Fourier transform equation (7), the previous relation amounts to writing that the eigenvalues of the product of two cyclic matrices are the product of the eigenvalues. With these notations a partition $\mathcal{E} = \{E_1, \dots, E_r\}$ is P -stable if $\forall a_i, b_i, \exists c_i$ such that

$$\sum_i a_i \chi(E_i) \star \sum_i b_i \chi(E_i) = \sum_i c_i \chi(E_i),$$

the partition $\mathcal{E} = \{E_1, \dots, E_r\}$ is I -stable if $\forall a_i, \exists c_i$ such that

$$\sum_i a_i \chi(E_i) \star \sum_i c_i \chi(E_i) = (1, 0, \dots, 0)$$

corresponding to the matrix inversion of a cyclic matrix.

- (vii) A set of disjoint subsets $\mathcal{E} = \{E_0 = \{0\}, E_1, \dots, E_k\}$ of $\{0, \dots, q-1\}$ is *convenient* if $\forall (n_1, \dots, n_k) \in \mathbb{N}^k \forall l \in [0, k]$,

$$\forall i, j \in E_l \quad (\chi(E_1)^{\star n_1} \star \dots \star \chi(E_k)^{\star n_k})_i = (\chi(E_1)^{\star n_1} \star \dots \star \chi(E_k)^{\star n_k})_j.$$

By a slight abuse of notation a set E such that $\{\{0\}, E\}$ is convenient is also called convenient. In that case one has

$$\forall n > 0, \quad \forall i, j \in E \quad (\text{Cy}(\chi(E))^n)_{0,i} = (\text{Cy}(\chi(E))^n)_{0,j}. \tag{8}$$

Actually, since any power of a $q \times q$ M can be expressed as linear combination of the first $q-1$ powers with the help of the Cayley–Hamilton theorem, one needs to verify Eq. (8) only for $0 < n \leq q-1$.

Intuitively, a convenient set of disjoint subsets can be seen as a possible “beginning” of a stable pattern. Indeed it verifies some *necessary* conditions such that it can be extended to a stable pattern. In particular, each set of a stable partition is convenient. This will be used in Sec. IV. Note that if \mathcal{E} is a partition then it is P -stable.

(viii) An *admissible* set is a subset E of $\{0, \dots, q-1\}$,

$$E = \bigsqcup_{d \in D} di_d H_d, \tag{9}$$

where D is a subset of the divisors of q , H_d is a subgroup of $\mathbb{Z}_{q/d}^*$, and $\text{gcd}(di_d, q) = d \forall d \in D$. We will show below that the union in Eq. (9) is indeed a disjoint union and that the admissible sets are, in fact, the *only* possible sets in a stable pattern.

(ix) For I a finite set, $\mathbf{x} = (x_i)_{i \in I}$, we note $\mathcal{P}_{\mathbf{x}, I} = \{A_1, \dots, A_r\}$ the partition of I such that $x_i = x_j$ if and only if i and j are in a same A_k . Actually the A_k 's are the preimages of the application $i \rightarrow x_i$. When the set $I = \{1, \dots, q\}$ we do not specify it and note simply $\mathcal{P}_{\mathbf{x}}$. For example, for $q=4$ $\mathcal{P}_{(x_1, x_2, x_1, x_1)} = \{\{1, 3, 4\}, \{2\}\}$.

(x) Finally if E is a group, $F < E$ means that F is a subgroup of E .

II. ANALYTICAL RESULTS PERTAINING TO MATHEMATICS

In this paragraph we express the inverse stability and the product stability for the pattern and the signed pattern in terms of matrix subalgebra and list mathematical results which are used in Sec. III. We also present results interesting *per se* and likely to be useful to go further in the classification of the lattice models.

A. List of the results

1. Pattern stability as matrix subalgebra

- The pattern $\mathcal{E} = \{E_i\}$ is product stable if and only if there exists a partition $\mathcal{F} = \{F_j\}$ such that

$$\bigoplus_{1 \leq i \leq r} \widehat{\text{C}\chi(E_i)} = \bigoplus_{1 \leq j \leq r} \text{C}\chi(F_j). \tag{10}$$

- The pattern $\mathcal{E} = \{E_i\}$ is inverse stable if and only if there exists a partition $\mathcal{F} = \{F_j^+, F_j^-\}$ such that

$$\bigoplus_{1 \leq i \leq r} \widehat{\text{C}\chi(E_i)} = \bigoplus_{1 \leq j \leq r} (\text{C}\chi(F_j^+) - \text{C}\chi(F_j^-)). \tag{11}$$

- The signed-pattern $\mathcal{E} = \{E_i^+, E_i^-\}$ is product stable if and only if there exists a partition $\mathcal{F} = \{F_j\}$ such that

$$\bigoplus_{1 \leq i \leq r} (\widehat{\text{C}\chi(E_i^+) - \text{C}\chi(E_i^-)}) = \bigoplus_{1 \leq j \leq r} \text{C}\chi(F_j). \tag{12}$$

- The signed-pattern $\mathcal{E} = \{E_i^+, E_i^-\}$ is inverse stable if and only if there exists a partition $\mathcal{F} = \{F_i^+, F_i^-\}$ such that

$$\bigoplus_{1 \leq i \leq r} \mathbb{C}(\widehat{\chi(E_i^+) - \chi(E_i^-)}) = \bigoplus_{1 \leq j \leq r} \mathbb{C}(\chi(F_j^+) - \chi(F_j^-)). \tag{13}$$

2. Stability by multiplication

If \mathcal{E} and \mathcal{F} are two signed patterns verifying Eq. (13) then for any a prime with q ,

$$a\mathcal{E} = \mathcal{E} \quad \text{and} \quad a\mathcal{F} = \mathcal{F}.$$

By $a\mathcal{E} = \mathcal{E}$ we mean $\forall i, \exists k$ such that either $aE_i^+ = E_k^+$ and $aE_i^- = E_k^-$ or $aE_i^+ = E_k^-$ and $aE_i^- = E_k^+$.

3. Admissible subsets

All the sets E_i^\pm or E_i in relations Eqs. (10)–(13) are admissible.

4. Convenient sets: Necessary conditions of stability

This result is mainly useful for the demonstration of the result of Sec. III A 2.

For a partition $\{E_1, \dots, E_r, A\}$ we define a partition $\{F_1, \dots, F_s\}$ such that $\bigoplus_{1 \leq i \leq r} \mathbb{C}\widehat{\chi(E_i)} \subset \bigoplus_{1 \leq j \leq s} \mathbb{C}\chi(F_j)$, with F_j maximal. We define J the subset $\{1, \dots, s\}$ by

$$j \in J \Leftrightarrow (\widehat{\chi(E_i)})_k \neq 0 \quad \forall i \in \{1, \dots, r\}, \quad k \in F_j.$$

Then the set $\{E_1, \dots, E_r\}$ is convenient if and only if

$$\bigoplus_{j \in J} \mathbb{C}\widehat{\chi(F_j)} \subset \left(\bigoplus_{1 \leq i \leq r} \mathbb{C}\chi(E_i) \right) \oplus \left(\bigoplus_{a \in A} \mathbb{C}\chi(\{a\}) \right).$$

5. Subgroup induce product-stable patterns

If H is a subgroup of \mathbb{Z}_q^* (the set of the invertible elements of \mathbb{Z}_q) then H induces a product-stable pattern given by the classes modulo H (i.e., the $\{iH\} \ i \in \mathbb{Z}_q$)

6. Monocolor inverse-stable signed pattern

Except a $q=4$ (and $q=1$) example, there is *no* inverse-stable signed pattern. This result proves a conjecture concerning cyclic Hadamard matrices in the particular case of symmetric matrices.

B. Proof and illustration of the above result

Below we prove and comment on the results mentioned above. We also give examples and illustrations. First we need two assertions.

Assertion 1: Let $V \subset \mathbb{C}^q$ be a vector subspace of dimension r then V is product stable if and only if there exists disjoint subsets F_1, \dots, F_r of $\{1, \dots, q\}$ with $V = \bigoplus_{1 \leq i \leq r} \mathbb{C}\chi(F_i)$.

Assertion 2: Let $V \subset \mathbb{C}^q$ be a vector subspace of dimension r and V^* the (supposed nonempty) subset of vectors of V with all nonzero components, then $(V^*)^{-1} \subset V$ if and only if there exist a partition of $\{1, \dots, q\}$ $F_1^+, F_1^-, \dots, F_r^+, F_r^-$ with

$$V = \bigoplus_{1 \leq i \leq r} \mathbb{C}(\chi(F_i^+) - \chi(F_i^-)).$$

In other words Assertion 1 states that V can be generated by vectors with entries 0 or 1, and Assertion 2 states that V can be generated by vectors with entries 0, 1, or -1 , and such that the absolute value of all the entries of these vectors sum up to the all one entry vector. These assertions are proven by recurrence on the space dimension q .

Proof of Assertion 1: For $q=1$ the assertion is clear. Suppose Assertion 1 is true for dimension $q-1$ and let $V \subset \mathbb{C}^q$ be a product-stable subspace. Let $V \cap (\mathbb{C}^{q-1} \times \{0\}) = W \times \{0\}$, therefore $W = \bigoplus_{1 \leq l \leq s} \mathbb{C}\chi(F_l)$, where the F_l are disjoint subsets of $\{1, \dots, q-1\}$. Let $\mathbf{v} \in V$, we will show that

$i, j \in F_l$ implies $v_i = v_j$. If $v_q = 0$ it is clear. If not, one can always admit $v_q = 1$, then $\mathbf{v} \cdot \mathbf{v} - \mathbf{v} \in W \times \{0\}$ so that $v_i^2 - v_i = v_j^2 - v_j$, which implies $v_i = v_j$ since $v_i + v_j = 1$ is impossible (one can add $\chi(F_l) \times \{0\}$ to \mathbf{v}). So if $\mathbf{v} \in V$ is a vector such that $v_q = 1$, we can admit $v_i = 0$ for $i \in F_l \forall l$. Since $V = (W \times \{0\}) \oplus \mathbb{C}\mathbf{v}$ and $\mathbf{v} \cdot \mathbf{v} = \mathbf{v}$ then all $\mathbf{v} = \chi(F)$, where $F \subset \{1, \dots, q\}$, disjoint of all F_l .

Proof of Assertion 2: Let V satisfying the conditions of Assertion 2 and $\mathbf{v} \in V^*$, such that $v_q = 1$, we define $W = \{\mathbf{w} \in V \mid w_q = 0\}$ and $I = \{i \mid w_i = 0 \forall \mathbf{w} \in W\}$. If $I = \{1, \dots, q\}$ then $W = \mathbb{C}\mathbf{v}$, therefore $\mathbf{v}^{-1} = \mathbf{v}$ which proves the assertion. On the contrary if $I \neq \{1, \dots, q\}$ there exists $\mathbf{w} \in W$ such that $w_i \neq 0$ for all $i \notin I$, this is possible while W is not a finite union of proper subspaces. Let $\mathbf{u} = \lim_{\epsilon \rightarrow 0} (\mathbf{v} + \epsilon^{-1}\mathbf{w})^{-1}$, $u_i = v_i^{-1}$ if $i \in I$ and $u_i = 0$ if $i \notin I$. On another hand $\mathbf{v} - \mathbf{v}^{-1} \in W$ so $v_i = v_i^{-1}$ for $i \in I$, finally $v_i = \pm 1$ for $i \in I$. One has $V = \mathbb{C}\mathbf{u} \oplus W$, and we proceed again with W , keeping only the coordinates not in I .

1. Proof of Sec. II A 1: Pattern stability as matrix subalgebra

Equations (10) and (12) are direct consequences of Assertion 1, taking

$$V = \bigoplus_{1 \leq i \leq r} \mathbb{C}\widehat{\chi(E_i)}.$$

Equations (11) and (13) are direct consequence the Assertion 2. If Eq. (10) holds, then $\{0\} \in \mathcal{E}$ and $\{0\} \in \mathcal{F}$. Indeed if $k \neq 0$ and 0 are in the same F_j and $1 \in E_i$ then $(\widehat{\chi(E_i)})_0 = (\widehat{\chi(E_i)})_k$ is impossible.

We give in Appendix A the exhaustive list of the P -stable, I -stable, and \overline{IP} -stable pattern for $q=8$. The pattern 9 is an illustration of 10, the pattern 5 is an illustration of 12, the pattern 18 is an illustration of 11, and finally pattern 8 is an illustration of 13.

Note that inverse stability is the justification of introducing signed pattern, which could not be justified in the strict framework of lattice statistical mechanics since asking that two Boltzmann weights are opposite is unphysical [however, such opposite entries in the Boltzmann weight matrix occurred in the solution of the $3d$ generalization of the Yang–Baxter equation (tetrahedron equations) by Baxter and Zamolochikov].

In Appendix A we give a detailed nontrivial example of application of Eq. (13).

2. Proof of Sec. II A 2: Stability by multiplication

Let \mathcal{E} and \mathcal{F} be two signed patterns verifying Eq. (13) and $A = \bigoplus_{1 \leq i \leq r} \mathbb{C}(\widehat{\chi(E_i^+)} - \widehat{\chi(E_i^-)}) = \bigoplus_{1 \leq j \leq r} \mathbb{C}(\widehat{\chi(F_j^+)} - \widehat{\chi(F_j^-)})$, therefore for any i , $\widehat{\chi(E_i^+)} - \widehat{\chi(E_i^-)} \in A$. This implies that for any j , $(\widehat{\chi(E_i^+)} - \widehat{\chi(E_i^-)})_k = \epsilon(\widehat{\chi(E_i^-)})_l$ for $k, l \in F_j^+ \cup F_j^-$ with $\epsilon = 1$ if k and l are both in F_j^+ or both in F_j^- , and $\epsilon = -1$ else. Let us introduce the polynomial

$$P(X) = \left(\sum_{e \in E_i^+} X^{ek} - \sum_{e \in E_i^-} X^{ek} \right) - \epsilon \left(\sum_{e \in E_i^+} X^{el} - \sum_{e \in E_i^-} X^{el} \right) \in \mathbb{Q}[X].$$

One has $P(\omega) = 0$, and consequently, using a Galois symmetry argument, $P(\omega^a) = 0$ for a prime with q . Therefore $\widehat{\chi(aE_i^+)} - \widehat{\chi(aE_i^-)} \in A$ and $\bigoplus_{1 \leq i \leq r} \mathbb{C}(\widehat{\chi(E_i^+)} - \widehat{\chi(E_i^-)}) \subset A$. The equality follows by a dimension argument.

Notice that, applying this result to $a = -1$, one finds that if $E \in \mathcal{E}$ then either $E = -E$ or $-E$ is another set of \mathcal{E} .

3. Proof of Sec. II A 3: Admissible subsets

Let us first recall that an admissible set E of $\{0, \dots, q-1\}$ is a disjoint union

$$E = \bigsqcup_{d \in D} di_d H_d,$$

where D is a subset of the divisors of q , H_d is a subgroup of $\mathbb{Z}_{q/d}^*$, and $\gcd(di_d, q) = d \forall d \in D$.

We first note that the intersection of two admissible sets is an admissible set. This comes from the fact that if d is a divisor of q , H and H' are two subgroups of $\mathbb{Z}_{q/d}^*$, and id and $i'd$ are two elements of $\mathbb{Z}(q, d)$, then either there exists $i''d \in idH \cap i'dH'$ implying that $idH \cap i'dH' = i''d(H \cap H')$ or $idH \cap i'dH' = \emptyset$. We need also the following technical lemma.

Lemma 1: Let $P(X) \in \mathbb{Z}[X]$, if $id \in \mathbb{Z}(q, d)$ then $\{jd \in \mathbb{Z}(q, d) \mid P(\omega^{jd}) = P(\omega^{id})\} = idH$ with $H < \mathbb{Z}_{q/d}^*$ (with a little abuse of notation).

Proof: ω^{id} is a (q/d) th primitive root of unity that we denote ζ . Let k be the inverse of i modulo q/d . The condition $P(\omega^{jd}) = P(\omega^{id})$ becomes $P(\zeta^j) = P(\zeta^{ki})$. But the set $H = \{m \in \mathbb{Z}_{q/d}^* \mid P(\zeta^m) = P(\zeta^i)\}$ is a subgroup of $\mathbb{Z}_{q/d}^*$. Indeed $P(\zeta^m) = P(\zeta^i)$ does not depend on the particular choice of the primitive root of unity since it amounts to saying that $P(X) - P(X^m)$ is a multiple of the minimal polynomial of ζ and therefore $P(\zeta^m) = P(\zeta^i)$ and $P(\zeta^j) = P(\zeta^i)$ imply $P(\zeta^j) = P(\zeta^m)$ and $P(\zeta^j) = P(\zeta^{m^{-1}})$.

Let us consider Eq. (13). Let $k \in F_j^+$ and define $P_i(X) = \sum_{e \in E_i^+} X^e - \sum_{e \in E_i^-} X^e$. By Eq. (13) one has

$$F_j^+ = \bigcap_{1 \leq i \leq r} \{l \in \mathbb{Z}_q \mid P_i(\omega^l) = P_i(\omega^k)\}$$

if $d = \gcd(q, k)$, then $F_j^+ \cap \mathbb{Z}(q, d) = \bigcap_{1 \leq i \leq r} \{l \in \mathbb{Z}(q, d) \mid P_i(\omega^l) = P_i(\omega^k)\}$ which is an admissible set by the results above, and finally F_j^+ is also admissible.

4. Proof of Sec. II A 4: Convenient sets, necessary conditions of stability

We define the intersection of two partitions $\mathcal{E} = \{E_1, \dots, E_r\}$ and $\mathcal{F} = \{F_1, \dots, F_s\}$ of a finite set I by

$$\mathcal{E} \cap \mathcal{F} = \{E_i \cap F_j \mid 1 \leq i \leq r \ 1 \leq j \leq s\}.$$

Lemma 2: Let $\mathbf{y} \in \mathbb{C}^n$ and $\mathbf{a}(1), \dots, \mathbf{a}(t) \in \mathbb{C}^n$ for $A \in \mathcal{P}_{\mathbf{a}(1)} \cap \dots \cap \mathcal{P}_{\mathbf{a}(t)}$. The two following affirmations (14) and (15) are equivalent (with the convention $0^0 = 1$):

$$\forall (k_1, \dots, k_t) \in \mathbb{N}^t, \quad \sum_{i=1}^n a(1)_i^{k_1} \cdots a(t)_i^{k_t} y_i = 0, \tag{14}$$

$$\forall A \in \mathcal{P}_{\mathbf{a}(1)} \cap \dots \cap \mathcal{P}_{\mathbf{a}(t)}, \quad \sum_{i \in A} y_i = 0. \tag{15}$$

Proof: The proof goes by induction over t . For $t=1$, let us define the sets A_i by $\mathcal{P}_{\mathbf{a}(1), \{1, \dots, n\}} = \{A_1, \dots, A_r\}$ and let b_j be the value of $\mathbf{a}(1)_i$ for i in A_j . Using (14) one has

$$\underbrace{\begin{pmatrix} 1 & \cdots & 1 \\ \cdots & \cdots & \cdots \\ b_1^{r-1} & \cdots & b_r^{r-1} \end{pmatrix}}_B \begin{pmatrix} \sum_{i \in A_1} y_i \\ \vdots \\ \sum_{i \in A_r} y_i \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{16}$$

Since $\det B = \prod_{1 \leq i < j \leq r} (b_i - b_j) \neq 0$ (Vandermonde determinant), $\sum_{i \in A_k} y_i = 0$ for any $1 \leq k \leq r$. This proves the property for $t=1$.

Let us take $t > 1$ and assume the lemma for $t-1$, therefore Eq. (14) is equivalent to

$$\sum_{i \in A} a(t)_i^{k_t} y_i = 0 \quad \forall A \in \mathcal{P}_{\mathbf{a}(1)} \cap \dots \cap \mathcal{P}_{\mathbf{a}(t-1)} \quad \forall k_t \in \mathbb{N},$$

and using the lemma for $t=1$ this is equivalent to

$$\sum_{i \in C} y_i = 0 \quad \forall C \in \mathcal{P}_{\mathbf{a}(t), A}, \quad \text{with } A \in \mathcal{P}_{\mathbf{a}(1)} \cap \dots \cap \mathcal{P}_{\mathbf{a}(t-1)},$$

$$\sum_{i \in C} y_i = 0, \quad C \in \mathcal{P}_{\mathbf{a}(1)} \cap \dots \cap \mathcal{P}_{\mathbf{a}(t)},$$

which completes the proof of the lemma.

We now use this lemma to prove the result (Sec. II A 4. Let $\{E_0, E_1, \dots, E_r, A\}$ be a partition such that $\mathcal{E} = \{E_0, E_1, \dots, E_r\}$ is convenient. For $(k_0, \dots, k_r) \in \mathbb{N}^{r+1}$ one introduces $\mathbf{u} = \chi(E_0)^{*k_0} \dots \chi(E_r)^{*k_r}$. By definition $u_i = u_j$ for i and j in the same E_l . If $\mathbf{v} = \hat{\mathbf{u}} = q^{k_0 + \dots + k_r} \widehat{\chi(E_0)^{k_0} \dots \chi(E_r)^{k_r}}$ this implies $\sum_m v_m \omega^{-im} = \sum_m v_m \omega^{-jm}$ leading to

$$\sum_m (\omega^{-im} - \omega^{-jm}) (\widehat{\chi(E_0)})_m^{k_0} \dots (\widehat{\chi(E_r)})_m^{k_r} = 0.$$

We now use the Lemma 2 with $y_m = \omega^{-im} - \omega^{-jm}$ and $\mathbf{a}(n) = \widehat{\chi(E_n)}$ to get the result.

5. Proof of Sec. II A 5: Subgroups induce product-stable patterns

To show that subgroups induce product-stable pattern, we first note that the class modulo H is indeed a pattern. Let I be a set of representative of the classes modulo H . Let

$$\mathbf{x} = \sum_{i \in I} a_i \chi(iH) \in \bigoplus_{i \in I} \mathbb{C} \chi(iH),$$

then

$$(\hat{\mathbf{x}})_j = \sum_{i \in I} a_i \frac{|iH|}{|H|} \sum_{h \in H} \omega^{ihj},$$

where $|A|$ denotes the cardinality of the set A . Consequently if $j' = tj$ with $t \in H$ then $(\hat{\mathbf{x}})_{j'} = (\hat{\mathbf{x}})_j$, which implies

$$\bigoplus_{i \in I} \widehat{\mathbb{C} \chi(iH)} \subset \bigoplus_{i \in I} \mathbb{C} \chi(iH).$$

The inverse inclusion is shown using inverse Fourier transform.

6. Proof of Sec. II A 6: Monocolor inverse-stable signed-pattern

Let us take $q > 1$ (the case $q = 1$ is obvious). It is readily verified that the monocolor signed pattern $[a, -a, -a, -a]$ is I -stable. We now prove the following lemma which we will need.

Lemma 3: *If $a, b \in \mathbb{N}^*$ $a\mathbb{Z}_{ab}^* = a\mathbb{Z}_b^*$ (by \mathbb{Z}_b^* we mean the elements of \mathbb{Z}_{ab} which are prime with b).*

Proof: Let us introduce the set $C = \{k \in \mathbb{Z}_{ab} \mid \gcd(k, b) = 1\}$, we will prove $a\mathbb{Z}_{ab}^* = aC$. It is clear that $a\mathbb{Z}_{ab}^* \subset aC$. We need to show that if k is prime with b , then one of the $k, k+b, \dots, k+(a-1)b$ is prime with a . Let us write $a = cd$ where the prime factors of b appear only in c . Since $\gcd(b, d) = 1$ then $k, k+b, \dots, k+(d-1)b$ are distinct modulo d , therefore one of them is equal to 1 modulo d , which proves the lemma.

Below we show that there is no other I -stable signed pattern than $[a, -a, -a, -a]$. Let E^+, E^- be an I -stable monocolor signed pattern and $M = \text{Cy}(\chi(E^+) - \chi(E^-))$, the inverse stability can be expressed as $M^2 = tI_q$, where t is some even nonzero integer and I_q is the identity matrix. Applying twice M to the all one entry vector, one gets

$$M^2 = s^2 I_q, \tag{17}$$

with $s = |E^+| - |E^-|$ where we consider, without loss of generality, that $|E^+| > |E^-|$.

We now prove that $s^2=q$. Indeed using Eq. (13)

$$U^*MU = q \operatorname{diag}(\widehat{\chi(E^+) - \chi(E^-)}),$$

so there exists a constant k and a partition $\{F^+, F^-\}$ of $\{0, \dots, q-1\}$ such that $\widehat{\chi(E^+) - \chi(E^-)} = k(\chi(F^+) - \chi(F^-))$. $s = (\widehat{\chi(E^+) - \chi(E^-)})_0 = k(\chi(F^+) - \chi(F^-))_0$ so $s=k$,

$$\widehat{\chi(E^+) - \chi(E^-)} = s(\chi(F^+) - \chi(F^-)). \tag{18}$$

Define $N = \operatorname{Cy}(\chi(F^+) - \chi(F^-))$ applying again the Fourier transform to Eq. (18), one gets

$$N^2 = \left(\frac{q}{s}\right)^2 I_q,$$

which combined with Eq. (17) yields

$$M^2 = qI_q$$

as stated before.

Applying the equation above to a diagonal term proves that M is symmetric, and therefore Eq. (17) can be written as

$$\widetilde{M}M = qI_q. \tag{19}$$

In other words, M is a so-called¹¹ symmetric Hadamard matrix, see Ref. 24.

Using Eqs. (17) and (19) one gets $q=4u^2$. The example given in the beginning of this paragraph corresponds to $u=1$.

Since $\widehat{\chi(E^+) - \chi(E^-)} = 2\widehat{\chi(E^+) - \chi(\{0, \dots, q-1\})} = 2\widehat{\chi(E^+) - q\chi(\{0\})}$ and using Eq. (18),

$$(\widehat{\chi(E^+)})_i = \pm u \quad \text{for } i \neq 0. \tag{20}$$

Since E^+ is an admissible set (see Sec. II A 3),

$$E^+ = \bigsqcup_{d \in D} di_d H_d,$$

where D is a subset of the divisors of q , $\gcd(di_d, q) = d$, and $H_d < \mathbb{Z}_{q/d}^*$. Using the result of Sec. II A 2 and since $|E^+| \neq |E^-|$ for any $a \in \mathbb{Z}_q^*$, one has $aE^+ = E^+$ yielding $\mathbb{Z}_q^* E^+ = E^+$, in particular, for $d \in D$, $i_d d \mathbb{Z}_q^* \subset E^+$. Using Lemma 3 one has $i_d d \mathbb{Z}_q^* = i_d d \mathbb{Z}_{q/d}^* = d \mathbb{Z}_{q/d}^*$, so that

$$E^+ = \bigsqcup_{d \in D} d \mathbb{Z}_{q/d}^* \tag{21}$$

(in the example shown in the beginning of this section one has $E^+ = \{1, 3\} \sqcup \{2\}$).

At this point we need to use results of number theory. The so-called Moebius function μ (Ref. 25) is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^l & \text{if } n = p_1 \cdots p_l \quad \text{with } p_1 \cdots p_l \text{ distinct primes} \\ 0 & \text{else,} \end{cases}$$

and it has the property that $\sum_{k \in \mathbb{Z}_n^*} \zeta^{k} = \mu(n)$, where $\zeta = \exp(2\pi i/n)$. In our case one gets $\sum_{k \in \mathbb{Z}_{q/d}^*} \omega^{kd} = \mu(q/d)$. We now use Eqs. (20) and (21) and we get

$$\pm u = (\widehat{\chi(E^+)})_1 = \sum_{d \in D} \mu\left(\frac{q}{d}\right).$$

Noting $q = 2^{2a_0} p_1^{2a_1} \cdots p_l^{2a_l}$, where $2, p_1, \dots, p_l$ are distinct prime numbers, one has

$$|\{t|q \text{ such that } \mu(t) = 1\}| = 2^l = |\{t|q \text{ such that } \mu(t) = -1\}|,$$

therefore $u = 2^{a_0-1} p_1^{a_1} \cdots p_l^{a_l} \leq 2^l$, consequently $l=0$ and $a_0=1$, which proves that $q=4$ is the only possible value.

III. ANALYTICAL RESULTS PERTAINING TO STATISTICAL MECHANICS

In this paragraph we express the inverse stability and the product stability for the pattern and the signed pattern in terms of matrix subalgebra and list our analytical results.

A. List of the results

1. q is a prime

When q is a prime number, there is no other product-stable pattern than the patterns induced by the subgroups of \mathbb{Z}_q . Furthermore there is no inverse-stable pattern which is not product stable. Consequently there are $1 + \tau(q-1)$ stable patterns, where $\tau(n)$ is the number of divisors of n .

2. q is the square of a prime or the product of two primes

If q is the square of a prime p , then there are $1 + \tau(p-1) + \tau^2(p-1)$ product-stable patterns. In addition to the class modulo \mathbb{Z}_q described in Sec. II A 5, there exists other product-stable patterns. If P denotes the natural projection from \mathbb{Z}_q on \mathbb{Z}_p , the set of product-stable patterns is

$$\{\{0\}, \mathbb{Z}_q \setminus \{0\}\} \cup \{\alpha L\} \cup \{\{0\}, aP^{-1}(H), bPK\},$$

where

$$\alpha \in \mathbb{Z}_q, \quad L < \mathbb{Z}_q,$$

$$a, b \in \mathbb{Z}_p^*, \quad H, K < \mathbb{Z}_p^*.$$

If $q = p_1 p_2$ is the product of two different prime numbers p_1 and p_2 then the three-color pattern defined by $E_0 = \{0\}$ and $E_1 = \{p_1, 2p_1, \dots, (p_2-1)p_1\}$ is product stable.

3. An integrable one-parameter family of integrable patterns

If $q \neq 2$ is a prime the three-color pattern formed by

$$E_0 = \{0\},$$

$$E_1 = \{i^2, i \in \mathbb{Z}_q^*\}, \tag{22}$$

$$E_2 = \mathbb{Z}_q - E_0 - E_1$$

is product stable. Furthermore if $q = 4k + 1$, then the associated transformation K is integrable.

4. Six families of stable patterns

We give below six families of patterns which are stable for any even q . Two patterns on the same row of the table below are related by discrete Fourier transform.

For product-stable signed pattern,

$$P_1 = [x_0, x_1, \dots, -x_1, \dots, x_1],$$

$$P_2 = [x_0, x_1, -x_1, \dots, x_2, -x_1, \dots, x_1],$$

$$P_3 = [x_0, x_1, x_2, \dots, x_{q/2}, -x_1, \dots, -x_{q/2-1}].$$

For inverse-stable simple pattern,

$$Q_1 = [x_0, \dots, x_0, x_1, x_0, \dots, x_0],$$

$$Q_2 = [x_0, x_1, x_0, \dots, x_0, x_2, x_0, x_1, \dots, x_1],$$

$$Q_3 = [x_0, x_1, x_0, x_2, x_0, x_3, \dots, x_0, x_{q/2}].$$

Patterns P_1 and Q_1 are two-color pattern, P_2 and Q_2 are three-color pattern, and P_3 and Q_3 are $q/2+1$ -color patterns. For pattern P_1 (Q_1) the entry $-x_1$ (x_1) is in position $q/2+1$ (position starting at zero). For patterns P_2 and Q_2 the entry x_2 is also in position $q/2+1$. Note that for P_2 the elements before and after x_2 are x_1 when $q/2$ is even and $-x_1$ when $q/2$ is odd.

B. Proof and illustration of the above results

1. Proof of Sec. III A 1: q is a prime

The key point of this demonstration is the well known fact that (if $a_0, \dots, a_{q-1} \in \mathbb{Q}$)

$$\sum_{i=0}^{q-1} a_i \omega^i = 0 \Leftrightarrow a_0 = \dots = a_{q-1}. \quad (23)$$

Let $\mathcal{E} = \{E_1^+, E_1^-, \dots, E_r^+, E_r^-\}$ and $\mathcal{F} = \{F_1^+, F_1^-, \dots, F_r^+, F_r^-\}$ be two partitions verifying Eq. (13) with $E_1^+, \dots, E_r^+, F_1^+, \dots, F_r^+$ nonempty. We admit $r \geq 2$ since the case $r=1$ occurs only for $q=1$ or $q=4$, as shown in Sec. II A 6. Note that the E 's and the F 's play the same role and can be interchanged.

Let $1 \leq l, m \leq r$, Eq. (13) can be rewritten as

$$\begin{aligned} (\widehat{\chi(E_l^+) - \chi(E_l^-)})_i &= (\widehat{\chi(E_l^+) - \chi(E_l^-)})_j \quad \text{if } i, j \in F_m^+ \text{ or } i, j \in F_m^-, \\ (\widehat{\chi(E_l^+) - \chi(E_l^-)})_i &= -(\widehat{\chi(E_l^+) - \chi(E_l^-)})_j \quad \text{if } i \in F_m^+ \text{ and } j \in F_m^-. \end{aligned} \quad (24)$$

If $0 \in F_1^+$ we will show $F_1^+ = \{0\}$ and $F_1^- = \emptyset$. Suppose, *ab absurdo*, that there exists $i \neq 0$ with $i \in F_1^+ \cup F_1^-$. Using Eq. (24) one gets

$$(\widehat{\chi(E_l^+) - \chi(E_l^-)})_0 = \pm (\widehat{\chi(E_l^+) - \chi(E_l^-)})_i$$

for $l \neq 1$ and $0 \in E_1^+$. So that

$$|E_l^+| - |E_l^-| = \pm \left(\sum_{e \in E_l^+} \omega^{ie} - \sum_{e \in E_l^-} \omega^{ie} \right),$$

which is impossible by Eq. (23), since $0 \notin iE_l^+$ and $iE_l^+ \cap iE_l^- = \emptyset$. The same applies interchanging the E 's and F 's.

We now show that $E_1^- = \dots = E_r^- = F_1^- = \dots = F_r^- = \emptyset$. Recalling that $E_1^+ = \{0\}$ and $E_1^- = \emptyset$, let us suppose that F_l^- is nonempty and $i \in F_l^+, j \in F_l^-$, using Eq. (24) one has $(\widehat{\chi(E_l^+) - \chi(E_l^-)})_i = -(\widehat{\chi(E_l^+) - \chi(E_l^-)})_j$, and consequently $1 = -1$, a contradiction.

So, when q prime, Eq. (13) reduces to Eq. (10) which we write

$$(\widehat{\chi(E_k^+)})_i = (\widehat{\chi(E_k^+)})_j \quad \forall i, j \in F_l, \quad \forall k, l, \tag{25}$$

if $1 \in H \in \mathcal{E}$ and $1 \in K \in \mathcal{F}$ so $\sum_{h \in H} \omega^{ih} = \sum_{h \in H} \omega^{jh}$ for $i, j \in K$. Using Eq. (23), one deduces $iH = jH$. Taking $j=1$ one gets $i \in H$ and therefore $K \subset H$. Interchanging H and K one finds that $K = H$. From $ij^{-1} \in H$ we deduce that the subset of the partition which contains 1 is a subgroup.

Again using Eq. (25) with $l \geq 2$ one has $iE_l^+ = jE_l^+$ for $i, j \in H$, and therefore $E_l^+ = HE_l^+$ and E_l^+ is a union of classes modulo H . On another hand again using Eq. (25)

$$(\widehat{\chi(H)})_i = (\widehat{\chi(H)})_j \quad \forall i, j \in E_l^+,$$

therefore $iH = jH$ and E_l^+ is one class modulo H . This completes the proof (noting $E_1^+ = \{0\} = 0H$).

2. Proof of Sec. III A 2: q is the square of a prime

We consider the case $q = p^2$ with p a prime and note $\omega = \exp(2\pi/q)\iota$ and $\zeta = \exp(2\pi/p)\iota$. We recall that the cyclotomic polynomials of respective orders p and q are

$$\Phi_p(X) = 1 + \dots + X^{p-1},$$

$$\Phi_q(X) = 1 + X^p + \dots + X^{(p-1)p},$$

therefore if $P(X) = \sum_{k=0}^{p-1} a_k X^k$ and $Q(X) = \sum_{k=0}^{p^2-1} b_k X^k$ are two polynomials in $\mathbb{Q}[X]$, then

$$P(\zeta) = 0 \Leftrightarrow a_0 = \dots = a_{p-1}, \tag{26}$$

$$Q(\omega) = 0 \Leftrightarrow (p|(l-m) \Rightarrow b_l = b_m). \tag{27}$$

A minimal polynomial of ω over $\mathbb{Q}[\zeta]$ is $X^p - \zeta$. Finally we note P the natural projection $\mathbb{Z}_q \xrightarrow{P} \mathbb{Z}_p$.

Lemma 4: If $H < \mathbb{Z}_q^*$ then either $H = P^{-1}(K)$ with $K < \mathbb{Z}_p^*$ (in that case H is said to be of type 1) or $h \in H, h' \in H, h \neq h'$ implies $p|(h' - h)$ (in that case H is said to be of type 2).

Proof: Suppose $H < \mathbb{Z}_q^*$ is not of type 2, then there exists $h, h', h' \neq h$ such that $p|(h - h')$, so $h'h^{-1} = 1 + kp$ with $1 \leq k \leq p-1$. Therefore $(1+kp)^l = 1 + klp$ for all l and $1 + p\mathbb{Z}_p \subset H$ and finally $H(1 + p\mathbb{Z}_p) = H$: H is of type 1.

The next lemma is devoted to the determination of $\mathcal{P}_{\widehat{\chi(E)}}$ when $E = iH$ ($p|i$ and $H < \mathbb{Z}_q^*$) or $E = jpK$ ($p|j$ and $K < \mathbb{Z}_p^*$).

Lemma 5: One distinguishes the three following cases:

$$E = jpK, \quad p|j, \quad K < \mathbb{Z}_p^* \Rightarrow \mathcal{P}_{\widehat{\chi(E)}} = \{p\mathbb{Z}_p, \{iP^{-1}(K)|p|i\}\}, \tag{28}$$

$$E = iP^{-1}(K), \quad K < \mathbb{Z}_p^*, \quad p|it \Rightarrow \mathcal{P}_{\widehat{\chi(E)}} = \{\{0\}, \mathbb{Z}_q^*, \{pjK|p|j\}\}, \tag{29}$$

$$E = iH, \quad p|i, \quad H < \mathbb{Z}_q^*, \quad H \text{ of type 2} \Rightarrow \mathcal{P}_{\widehat{\chi(E)}} = \{jH|j \in \mathbb{Z}_q\}. \tag{30}$$

Proof of Eq. (28): If $p|i$ and $p|l$ then

$$(\widehat{\chi(E)})_i = (\widehat{\chi(E)})_l \Leftrightarrow \sum_{k \in K} (\omega^{ijpk} - \omega^{ljpk}) = 0 \Leftrightarrow \sum_{k \in K} (\zeta^{ijk} - \zeta^{ljk}) \stackrel{(1)}{=} 0 \Leftrightarrow iK = lK,$$

on another hand $(\widehat{\chi(E)})_{pt} = |K|$ for any t . The equivalence noted \Leftrightarrow refers to (26) with $H < \mathbb{Z}_q^* p|i$.

Proof of Eq. (29): If $K = \mathbb{Z}_p^*$, then $E = \mathbb{Z}_q^*$ and (29) is verified. We now suppose $K \neq \mathbb{Z}_p^*$. If $p|l$ then $(\widehat{\chi(E)})_l = \sum_{k \in K} \sum_{m=0}^{p-1} \omega^{il(mp+k)} = 0$, on another hand if $p \nmid l$ $(\widehat{\chi(E)})_{pt} = p \sum_{k \in K} \zeta^{itk} \neq 0$ using (26) and $K \neq \mathbb{Z}_p^*$, the value $\sum_{k \in K} \zeta^{itk}$ depends only on K using again (26). Finally $(\chi(E))_0 = p|K|$.

Proof of Eq. (30):

If $p \nmid l$ and $p \nmid j$, the two quantities $(\widehat{\chi(E)})_j = \sum_{h \in H} \omega^{jih}$ and $(\widehat{\chi(E)})_l = \sum_{h \in H} \omega^{ihl}$ are equal if and only if $ijH = ilH$. Indeed let us suppose $(\widehat{\chi(E)})_j = (\widehat{\chi(E)})_l$ then $\forall k \in [1, p-1], |ijH \cap (k+p\mathbb{Z}_p)| = 0$, or 1 since H is of type 2, and if $t \in (ijH \cap (k+p\mathbb{Z}_p)) \setminus (ilH \cap (k+p\mathbb{Z}_p))$ then, using (27), $t+p, \dots, t+(p-1)p$ also belong to $(ijH \cap (k+p\mathbb{Z}_p)) \setminus (ilH \cap (k+p\mathbb{Z}_p))$, a contradiction. On another hand $(\widehat{\chi(E)})_j$ can be seen as a polynomial in ω of degree strictly smaller than p over $\mathbb{Q}[\zeta]$, therefore $(\widehat{\chi(E)})_j \notin \mathbb{Q}[\zeta]$ (see Sec. I A 4). Finally if $p \nmid l$ and $p \nmid j$ the two quantities, $(\widehat{\chi(E)})_{pj} = \sum_{h \in H} \zeta^{ijh} \in \mathbb{Q}[\zeta]$ and $(\widehat{\chi(E)})_{pl} = \sum_{h \in H} \zeta^{ihl} \in \mathbb{Q}[\zeta]$ are equal if and only if $ijP(H) = ilP(H)$ using (26).

Lemma 6: *If E is convenient, admissible, $E \cap \mathbb{Z}_q^* \neq \emptyset$ and $E \cap p\mathbb{Z}_p^* \neq \emptyset$ then $E = \mathbb{Z}_q \setminus \{0\}$.*

Proof: Let us take a set E verifying the conditions of the lemma, since E is admissible then $E = iH \sqcup jpK$ with $H < \mathbb{Z}_q^*$, $K < \mathbb{Z}_p^*$ and $p \nmid i$ and $p \nmid j$. If there is $A \in \mathcal{P}_{\widehat{\chi(E)}}$ with $A = pM \subset p\mathbb{Z}_p^*$ using (*) $(\widehat{\chi(A)})_i = (\widehat{\chi(A)})_{jp}$, therefore $\sum_{m \in M} \omega^{imp} = \sum_{m \in M} \omega^{jmp^2}$, so $\sum_{m \in M} \zeta^{im} = |M|$ which is impossible. Consequently there exists t relatively prime to p such that $t, p \in B \in \mathcal{P}_{\widehat{\chi(E)}}$ and so $(\widehat{\chi(E)})_t = (\widehat{\chi(E)})_p$ which reads

$$\sum_{h \in H} \omega^{iht} + \sum_{k \in K} \zeta^{jkt} = \sum_{h \in H} \zeta^{ih} + \sum_{k \in K} 1. \tag{31}$$

So $\sum_{h \in H} \omega^{iht} \in \mathbb{Q}[\zeta]$ and H cannot be of type 2 since the degree of ω over $\mathbb{Q}[\zeta]$ is p . H is then of type 1, $H = P^{-1}(L)$ where $L < \mathbb{Z}_p^*$. Using (31), $\sum_{k \in K} \zeta^{jkt} = p \sum_{l \in L} \zeta^{il} + |K|$. We use (26) and we note $A_s = \{k \in K | p | jkt - s\}$ and $B_s = \{l \in L | p | jl - s\}$ for $1 \leq s < p$; one deduces $|K| = -A_s + pB_s$ which is possible only if $A_s = B_s = 1 \quad \forall s$, therefore $K = L = \mathbb{Z}_p^*$ and finally $E = \mathbb{Z}_q \setminus \{0\}$.

Remark: *If $\{\{0\}, E, F\}$ is convenient then $\forall A \in \mathcal{P}_{\widehat{\chi(E)}} \cap \mathcal{P}_{\widehat{\chi(F)}}$ one has $(\widehat{\chi(A)})_i = (\widehat{\chi(A)})_j$ if $i, j \in E$ or $i, j \in F$, and so if $\mathcal{P}_{\widehat{\chi(A)}} = \{B_1, \dots, B_r\}$ then $E \subset B_s$ and $F \subset B_t$ for some s and t .*

Proof of Sec. III A 2: We consider below five possible cases of couples (E, E') such that $\{\{0\}E, E'\}$ is convenient. In each case we are going to apply the remark above with a suitable choice of the set A , as well as Lemma 5.

- (1) $E = iH$, $p \nmid i$, $H < \mathbb{Z}_q^*$, $E' = jK$, $p \nmid j$, $K < \mathbb{Z}_p^*$, H and K are both of type 2. Using Eq. (30), $\mathcal{P}_{\widehat{\chi(E)}} = \{kH | k \in \mathbb{Z}_q\}$ and $\mathcal{P}_{\widehat{\chi(E')}} = \{kH | k \in \mathbb{Z}_q\}$, so $\mathcal{P}_{\widehat{\chi(E)}} \cap \mathcal{P}_{\widehat{\chi(E')}} = \{k(H \cap K) | k \in \mathbb{Z}_q\}$. Taking $A = H \cap K$, $\mathcal{P}_{\widehat{\chi(A)}} = \{l(H \cap K) | l \in \mathbb{Z}_q\}$, one gets that $E \subset l(H \cap K)$ and $E' \subset m(H \cap K)$ for some l and m which is possible only if $H = K$.
- (2) $E = iH$, $p \nmid i$, $H < \mathbb{Z}_q^*$, H is of type 2 and $E' = jP^{-1}(L)$, $L < \mathbb{Z}_p^*$, $p \nmid j$, $\mathcal{P}_{\widehat{\chi(E')}} = \{\{0\}, \mathbb{Z}_q^*, \{pkL | p \nmid k\}\}$. Taking $A = H \in \mathcal{P}_{\widehat{\chi(E)}} \cap \mathcal{P}_{\widehat{\chi(E')}}$, $jP^{-1}(L) \subset mH$ for some m which is in contradiction with the fact that H is of type 2.
- (3) $E = iH$, $p \nmid i$, $H < \mathbb{Z}_q^*$, H is of type 2 and $E' = jpK$, $K < \mathbb{Z}_p^*$, $\mathcal{P}_{\widehat{\chi(E')}} = \{p\mathbb{Z}_p, \{tP^{-1}(K) | p \nmid t\}\}$. Taking $A = H \cap P^{-1}(K)$ which a subgroup of type 2, $\mathcal{P}_{\widehat{\chi(A)}} = \{s(H \cap P^{-1}(K)) | s \in \mathbb{Z}_q\}$ and therefore $H \subset s(H \cap P^{-1}(K))$ and $pK \subset pt(H \cap P^{-1}(K))$ for some s and t . We deduce that $pH = pK$.
- (4) $E = ipK$, $p \nmid i$, $K < \mathbb{Z}_p^*$ and $E' = jpL$, $p \nmid j$, $L < \mathbb{Z}_q^*$, $\mathcal{P}_{\widehat{\chi(E)}} \cap \mathcal{P}_{\widehat{\chi(E')}} = \{p\mathbb{Z}_p, \{mP^{-1}(K \cap L) | p \nmid m\}\}$. Taking now $A = P^{-1}(K \cap L)$, $\mathcal{P}_{\widehat{\chi(A)}} = \{\{0\}, \mathbb{Z}_q^*, \{pt(K \cap L) | p \nmid t\}\}$, yielding $K = L$.
- (5) $E = iP^{-1}(K)$, $K < \mathbb{Z}_p^*$, $p \nmid i$ and $E' = jP^{-1}(L)$, $L < \mathbb{Z}_p^*$, $p \nmid j$. Taking $A = p(K \cap L) \in \mathcal{P}_{\widehat{\chi(E)}} \cap \mathcal{P}_{\widehat{\chi(E')}} = \{\{0\}, \mathbb{Z}_q^*, \{pt(K \cap L) | p \nmid t\}\}$, $\mathcal{P}_{\widehat{\chi(A)}} = \{p\mathbb{Z}_p, \{mP^{-1}(K \cap L) | p \nmid m\}\}$, one gets $K = L$.

We now take $\mathcal{E} = \{E_1, \dots, E_r\}$ and $\mathcal{F} = \{\mathcal{P}_{\widehat{\chi(aP^{-1}(H))}} = \{\{0\}, \mathbb{Z}_q^*, \{pmH | p \nmid m\}\} F_1, \dots, F_r\}$, verifying Eq. (10). If one of the E_i 's is of the type of Lemma 6, then $\mathcal{E} = \{\{0\}, \mathbb{Z}_q \setminus \{0\}\}$. From now on we consider the case where no E_k is of this type. So all the E_k 's are either iH or jpK or $\{0\}$, with $H < \mathbb{Z}_q^*$ $p \nmid i$ or $K < \mathbb{Z}_p^*$ $p \nmid j$. It is clear that if E, E' (distinct) are in \mathcal{E} , then $\{\{0\}E, E'\}$ is convenient. Suppose there is a set $E_k = iH$ with $H < \mathbb{Z}_q^*$ $p \nmid i$ with H of type 2, then using the three first points above, one gets that the E_l are the class modulo H . Using now the last two points, we see that $\forall E \in \mathcal{E} \setminus \{0\}$ either $E = iP^{-1}(K)$, $p \nmid i$ or $E = jpL$, $p \nmid j$. Thus we have shown that the only possible P -stable patterns are those occurring in Sec. III A 2.

We now verify that these cases are indeed P -stable. Obviously $\{\{0\}, \mathbb{Z}_q \setminus \{0\}\}$ and $\{\alpha L\}$ are

P -stable. Let us now take $\mathcal{E}=\{\{0\}, aP^{-1}(H), bpK\}$ with $H, K < \mathbb{Z}_p^*$ and $a, b \in \mathbb{Z}_p^*$, $\mathcal{P}_{\chi(aP^{-1}(H))} = \{\{0\}, \mathbb{Z}_q^*, \{pmH|p|m\}\}$ and $\mathcal{P}_{\chi(bpK)} = \{pZ_p, \{tP^{-1}K|p|t\}\}$. Note that these two sets are independent of a and b . Showing that \mathcal{E} is product stable amounts to showing that it is convenient. The only possible A in $\mathcal{P}_{\chi(aP^{-1}(H))} \cap \mathcal{P}_{\chi(bpK)}$ are $\{0\}$, pmH , and $tP^{-1}(K)$ with $p|m$ and $p|t$. When $A=pmH$ then $\mathcal{P}_{\chi(A)} = \{pZ_p, \{mP^{-1}(H)|p|m\}\}$, while when $A=tP^{-1}(K)$, $\mathcal{P}_{\chi(A)} = \{\{0\}, \mathbb{Z}_q^*, \{pmHK|p|m\}\}$. In both cases Eq. (10) is verified which completes the proof of Sec. III A 2.

We are now in position to compute the number of stable patterns. We recall that a cyclic group of order n has $\tau(n)$ subgroups so that \mathbb{Z}_q^* has $\tau(p^2-p) = 2\tau(p-1)$ subgroups, but there are as many subgroups of type 1 as subgroups in \mathbb{Z}_p^* , i.e., $\tau(p-1)$, so there are $\tau(p-1)$ subgroups of type 2. Finally $|\{\{0\}, aP^{-1}(H), bpK\}| = (\tau(p-1))^2$, yielding the stated result.

In Appendix B we give as an illustration the example of all stable patterns for $q=25=5^2$.

3. Proof of Sec. III A 3: An integrable one-parameter family of integrable patterns

- Clearly for the pattern defined by Eq. (22).

$$\text{card}(E_1) = \text{card}(E_2) = \frac{q-1}{2}.$$

- If $k \in E_1$ then there exists a such that $k = a^2 \pmod q$, therefore

$$kE_1 = a^2\{i^2 \pmod q\} = E_1,$$

so $\sum_{i \in E_1} w^{ki}$ is independent of $k \forall k \in E_1$. Let us define A and A' ,

$$A \equiv \sum_{i \in E_1} w^{k_1 i}, \quad A' \equiv \sum_{i \in E_2} w^{k_2 i},$$

where $k_1 \in E_1$ and $k_2 \in E_2$. One has $A + A' + 1 = 0$.

Let us recall Gauss's result,²⁶

$$\sum_{j=0}^{q-1} \exp \frac{2i\pi j^2}{q} = \begin{cases} (1+i)\sqrt{q}, & q \equiv 0 \pmod 4 \\ \sqrt{q}, & q \equiv 1 \pmod 4 \\ 0, & q \equiv 2 \pmod 4 \\ i\sqrt{q}, & q \equiv 3 \pmod 4, \end{cases}$$

from which one deduces

$$A = \frac{\epsilon_q \sqrt{q-1}}{2},$$

with

$$\epsilon_q = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 4 \\ i & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

- Finally, the Fourier transform is represented by the 3×3 matrix,

$$F_q = \begin{pmatrix} 1 & \frac{q-1}{2} & \frac{q-1}{2} \\ 1 & \frac{\epsilon_q \sqrt{q}-1}{2} & \frac{-\epsilon_q \sqrt{q}-1}{2} \\ 1 & \frac{-\epsilon_q \sqrt{q}-1}{2} & \frac{\epsilon_q \sqrt{q}-1}{2} \end{pmatrix}. \quad (32)$$

When $q \equiv 1 \pmod{4}$ then $\epsilon_q = 1$, Eq. (32) corresponds to Eqs. (17) and (18) of Ref. 27. We deduce that the integrable mapping discovered in this reference corresponds to a spin-edge model of lattice statistical mechanics when q is a prime number with $q \equiv 1 \pmod{4}$; the pattern is explicitly defined by Eq. (22). The homogeneous expression of the transformation $K: (x, y, z) \rightarrow (X, Y, Z)$ can then easily be found. If one introduces then the inhomogeneous variables $u = y/x$ and $v = z/x$, a K -invariant having a particularly simple form is

$$\Delta = \frac{(u-v)^2}{(2uv - u - v)(u + v - 2)} \left(q + 2 \frac{uv - u - v + 1}{u + v} \right).$$

When $q \equiv -1 \pmod{4}$ then $\epsilon_q = i$ and the corresponding mapping is not integrable. However, a complexity reduction occurs, and using the method developed in Refs. 1 and 28, one finds for the generating function of the degree defined in Eq. (1),

$$f(x) = \frac{1}{(1-x)(1-x-x^2)},$$

leading to a complexity

$$\lambda = \frac{\sqrt{5}-1}{2} \approx 1.618\ 034.$$

4. Mapping of the six families of stable patterns of Sec. III A 4

These results are verified by direct inspection. Using the methodology and notation in Ref. 28, the collineation C , the inverse I , the generic (i.e., arbitrary q) degree generating function f , and therefore the complexity can be computed for P_1 , Q_1 , P_2 , and Q_2 .

- For P_1 and Q_1 the mappings are trivial. P_1 leads to a linear mapping with generating function $1/(1-x)$ and Q_1 to a mapping ($K_{Q_2}^2 = -1$),

$$C_{P_1} = \begin{pmatrix} 1 & 1 \\ 1 & 1-q \end{pmatrix}, \quad I_{P_1} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} x_0 + (2-q)x_1 \\ -x_2 \end{pmatrix},$$

$$C_{Q_1} = \begin{pmatrix} 1 & 1 \\ 1 & \epsilon_q \end{pmatrix}, \quad I_{Q_1} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} x_1 \\ -x_2 \end{pmatrix}.$$

- For P_2 and Q_2 , one can also find explicitly the expression of the collineation and of the inverse. The various expressions depend of the parity of $q/2$ (as mentioned q should be even) yielding four mappings all having the same degree generating function

$$f(x) = \frac{1+x}{(1-x)(1-2x)},$$

giving an integer complexity $\lambda = 2$. Introducing $\epsilon_q = (-1)^{q/2}$, the corresponding collineation and inverse are given below,

$$C_{P_2} = \begin{pmatrix} 1 & 2 & 1 \\ \frac{1+\epsilon_q}{2} & \frac{1-\epsilon_q}{2} & -1 \\ 1 & -(q-2) & 1 \end{pmatrix}, \quad I_{P_2} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_0^2 - (q-2)x_1^2 - (q-4)x_0x_1 + \epsilon_q x_0x_2 \\ -(x_0 - \epsilon_q x_2)x_1 \\ -\epsilon_q x_2^2 + \epsilon_q(q-2)x_1^2 + (q-4)x_2x_1 - x_0x_2 \end{pmatrix},$$

$$C_{Q_2}^{\text{even}} = \begin{pmatrix} \frac{q}{2} - 1 & \frac{q}{2} & 1 \\ 1 & 0 & -1 \\ \frac{q}{2} - 1 & -\frac{q}{2} & 1 \end{pmatrix},$$

$$I_{Q_2}^{\text{even}} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} (2q-4)x_0^2 - 2qx_1^2 + 4x_0x_2 \\ -4(x_0 - x_2)x_1 \\ -(q-2)(q-4)x_0^2 + q(q-2)x_1^2 - 4x_2^2 - 4(q-3)x_0x_2 \end{pmatrix},$$

$$C_{Q_2}^{\text{odd}} = \begin{pmatrix} \frac{q}{2} & \frac{q}{2} - 1 & 1 \\ 0 & 1 & -1 \\ \frac{q}{2} & -\frac{q}{2} + 1 & -1 \end{pmatrix}, \quad I_{Q_2}^{\text{odd}} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 4(x_1 - x_2)x_0 \\ 2qx_0^2 + (4-2q)x_1^2 - 4x_1x_2 \\ -q(q-2)x_0^2 + (q-2)(q-4)x_1^2 + 4x_2^2 + 4(q-3)x_1x_2 \end{pmatrix}.$$

The superscript refers to the parity of $q/2$.

IV. NUMERICAL RESULTS

A. Computer-aided method

To study the case where q is neither a prime nor the square of a prime, we use a computer. In principle there is no difficulty since it is “only” a matter of generating the patterns or the signed patterns and check the stability. To test the stability we can use the formulas (10)–(13). However, in practice, this would be tractable only for a very small value of q since the number of patterns grows extremely fast with q .

If a partition $\mathcal{E} = \{E_1, \dots, E_r\}$ is product stable, then for any k , E_k must be such that $i, j \in E_k \Rightarrow (\text{Cy}(\chi(E_k)))_i = (\text{Cy}(\chi(E_k)))_j$. Since the cyclic matrices associated with a stable pattern form an algebra, we see that any subset E_k must be convenient [see Eq. (8)]. This simple remark tells that it is not necessary to generate all possible subset E_k , but only convenient sets: one can first enumerate the 2^q subsets E of $\{0, \dots, q-1\}$ and keep only those which are convenient. The key point here is that a subset E is convenient irrespective of the way the remaining indices are grouped into other subsets. Then, using a tree structure, we can associate convenient subsets to make stable patterns. In order to minimize the tree structure, one can also use the condition on pairs (or more) of index subsets, also deduced from Eq. (8). This procedure applies *mutatis mutandis* to inverse stability when the matrices $\chi(E)$ are invertible. Note that this procedure can also be applied to the search of noncyclic stable patterns.

In the case of cyclic matrix we can go further and avoid the consideration of all possible subsets, retaining only the convenient sets. Indeed using the result of Sec. II A 3 one can generate *directly* the admissible sets. We then consider these sets as “atoms” to be combined to produce the patterns. This can also be implemented using a tree structure. In the results shown below, we did not use this last remark.

TABLE I. Number of P - and $I\bar{P}$ -stable patterns and signed patterns.

q	2	3	4	5	6	7	8
No. of tested pattern	3	11	49	257	1539	10 299	75 905
P -stable pattern	1	2	3	3	7	4	10
P -stable signed pattern	0	0	6	0	3	0	17
$I\bar{P}$ -stable pattern	0	0	2	0	3	0	11
$I\bar{P}$ -stable signed pattern	0	0	2	0	1	0	19
Total	1	2	13	3	14	4	57

B. Results

In Table I we present the number of P -stable and $I\bar{P}$ -stable patterns and signed patterns for $2 \leq q \leq 8$. In Table II we present the number of P -stable patterns for larger values of q . All these numbers have been found using the algorithm presented above. We have verified that for q prime (i.e., $q=2, 3, 5, 7, 11, 13, 17, 19, 23$, and 29), it corresponds to the result of Sec. III A 1, and for q the square of a prime ($q=4, 9$, and 25) to the result of Sec. III A 2. In Table I the first line is the number of convenient sets. The explicit expression of each pattern is not given in the text, but can be downloaded from the site.²⁹ However, the case $q=8$ is given in detail in Appendix A. Finally a MAPLE program to generate all the stable patterns for $q=p^2$ with p prime can be downloaded from Ref. 29.

V. CONCLUSION

In this paper we have shown several results concerning stable patterns in the case of cyclic matrices. The notion of signed pattern arises naturally when one studies $I\bar{P}$ -stability as a consequence of a duality between cyclic matrices and their Fourier transform. We find, in particular, an exact correspondence between $I\bar{P}$ -stable patterns and P -stable signed patterns, which justifies, *a posteriori*, the introduction of signed patterns in this cyclic matrix context. The main results, Eqs. (10)–(13), enable to find all I -stable patterns and signed patterns, when the number of states is a prime or the square of a prime, and to find some, but not all, stable patterns for composite integer values of q . This provides examples of birational transformations of an arbitrary large number of variables. We have computed the complexity of the corresponding transformations in some cases, finding a complexity reduction. In particular, we have recovered a one-parameter family of integrable transformations, for which we have given explicitly the matrix representation when it exists. The case of the monocolour I -stable signed patterns has been solved, demonstrating a conjecture about Hadamard matrices in a particular case. We also present an algorithm to find I -stable patterns. Although this algorithm is exponential, it can be used for not too large values of q .

It would be interesting to generalize our result to arbitrary value of q and to perform a more systematic analysis of the complexity of the associated birational transformation. Finally the same

TABLE II. Number of product-stable patterns.

q	9	10	11	12	13	14	15	16	17
No. of stable patterns	7	10	4	32	6	13	21	37	5
q	18	19	20	21	22	23	24	25	26
No. of stable patterns	42	6	47	28	14	5	172	13	19
q	27	28	29	30	31	37	41	43	49
No. of stable patterns	25	61	7	148	8	9	8	8	21

problem for noncyclic matrices should also be investigated, but it seems to us that it becomes a very complicated task, as a consequence of the loss of the discrete Fourier transform.

APPENDIX A: STABLE PATTERNS FOR $q=8$

We list below the stable patterns for $q=8$. The number before the eight letters between bracket is the arbitrary label of the pattern. The sequence of eight letters designates the first row of the cyclic matrix in the direct space, and the diagonal of the matrix in the Fourier space. When a letter is repeated (negated), this means that the two corresponding entries of the matrix are equal (opposite). For example, the pattern number 10 below corresponds to

$$M_{\text{Fourier}}^{10} = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & b & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -b & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & c & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & b & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -b & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & b \end{pmatrix},$$

$$M_{\text{direct}}^{10} = \begin{pmatrix} a & b & -b & b & c & b & -b & b \\ b & a & b & -b & b & c & b & -b \\ -b & b & a & b & -b & b & c & b \\ b & -b & b & a & b & -b & b & c \\ c & b & -b & b & a & b & -b & b \\ b & c & b & -b & b & a & b & -b \\ -b & b & c & b & -b & b & a & b \\ b & -b & b & c & b & -b & b & a \end{pmatrix},$$

and the cyclic matrix associated with pattern 17 with first row

$$[a \ b \ a \ b \ c \ b \ a \ b]$$

becomes by Fourier transform the diagonal matrix M_{Fourier}^{10} to which one associates in the direct space the cyclic matrix M_{direct}^{10} (see above).

Direct space \rightarrow Fourier space

P -stable pattern \rightarrow P -stable pattern

$$\begin{aligned} 9[a \ b \ c \ d \ e \ b \ f \ d] &\rightarrow 9[a \ b \ c \ d \ e \ b \ f \ d] \\ 15[a \ b \ c \ b \ d \ b \ c \ b] &\rightarrow 15[a \ b \ c \ b \ d \ b \ c \ b] \\ 22[a \ b \ b \ b \ b \ b \ b \ b] &\rightarrow 22[a \ b \ b \ b \ b \ b \ b \ b] \\ 39[a \ b \ c \ d \ e \ d \ c \ b] &\rightarrow 39[a \ b \ c \ d \ e \ d \ c \ b] \\ 48[a \ b \ c \ d \ e \ f \ g \ h] &\rightarrow 48[a \ b \ c \ d \ e \ f \ g \ h] \\ 51[a \ b \ c \ b \ d \ e \ c \ e] &\rightarrow 51[a \ b \ c \ b \ d \ e \ c \ e] \\ 3[a \ b \ c \ b \ d \ b \ e \ b] &\leftrightarrow 53[a \ b \ c \ d \ e \ b \ c \ d] \\ 24[a \ b \ c \ b \ c \ b \ c \ b] &\leftrightarrow 56[a \ b \ b \ b \ c \ b \ b \ b] \end{aligned}$$

Direct space \rightarrow Fourier space

$\bar{I}P$ -stable pattern \rightarrow P -stable signed-pattern

$$\begin{aligned} 4[a \ a \ a \ a \ b \ a \ a \ a] &\rightarrow 55[a \ b \ -b \ b \ -b \ b \ -b \ b] \\ 6[a \ b \ c \ b \ a \ d \ e \ d] &\rightarrow 35[a \ b \ c \ d \ e \ -d \ c \ -b] \\ 11[a \ b \ a \ c \ a \ d \ a \ e] &\rightarrow 31[a \ b \ c \ d \ e \ -b \ -c \ -d] \end{aligned}$$

$$\begin{aligned}
14[a b c d a b e d] &\rightarrow 21[a b c -b d b e -b] \\
17[a b a b c b a b] &\rightarrow 10[a b -b b c b -b b] \\
18[a b c b a d c d] &\rightarrow 5[a b c b d -b c -b] \\
20[a b c d a d c b] &\rightarrow 47[a b c -b d -b c b] \\
25[a a b a a a c a] &\rightarrow 37[a b c -b -c b c -b] \\
29[a b c d a e c f] &\rightarrow 13[a b c d e -b f -d] \\
34[a b c b a b d b] &\rightarrow 49[a b c -b d b c -b] \\
54[a b c d a d e b] &\rightarrow 44[a b c -b d e c -e]
\end{aligned}$$

Direct space \rightarrow Fourier space IP -stable signed-pattern $\rightarrow \bar{IP}$ -stable pattern

$$\begin{aligned}
5[a b c b d -b c -b] &\rightarrow 18[a b c b a d c d] \\
10[a b -b b c b -b b] &\rightarrow 17[a b a b c b a b] \\
13[a b c d e -b f -d] &\rightarrow 29[a b c d a e c f] \\
21[a b c -b d b e -b] &\rightarrow 14[a b c d a b e d] \\
31[a b c d e -b -c -d] &\rightarrow 11[a b a c a d a e] \\
35[a b c d e -d c -b] &\rightarrow 6[a b c b a d e d] \\
37[a b c -b -c b c -b] &\rightarrow 25[a a b a a a c a] \\
44[a b c -b d e c -e] &\rightarrow 54[a b c d a d e b] \\
47[a b c -b d -b c b] &\rightarrow 20[a b c d a d c b] \\
49[a b c -b d b c -b] &\rightarrow 34[a b c b a b d b] \\
55[a b -b b -b b -b b] &\rightarrow 4[a a a b a a a]
\end{aligned}$$

Direct space \rightarrow Fourier space \bar{IP} -stable signed-pattern $\rightarrow \bar{IP}$ -stable signed-pattern

$$\begin{aligned}
8[a b c -b a -b c b] &\rightarrow 8[a b c -b a -b c b] \\
16[a -a a -a b -a a -a] &\rightarrow 16[a -a a -a b -a a -a] \\
19[a b c d -a b -c d] &\rightarrow 19[a b c d -a b -c d] \\
23[a b c d a -d e -b] &\rightarrow 23[a b c d a -d e -b] \\
27[a b c b a -b c -b] &\rightarrow 27[a b c b a -b c -b] \\
32[a b c d -a e -c f] &\rightarrow 32[a b c d -a e -c f] \\
38[a b c d a -b c -d] &\rightarrow 38[a b c d a -b c -d] \\
42[a b c -b a d e -d] &\rightarrow 42[a b c -b a d e -d] \\
50[a b c -b a b d -b] &\rightarrow 50[a b c -b a b d -b] \\
1[a b c b a -b -c -b] &\leftrightarrow 52[a b a c a -c a -b] \\
2[a b c -b -a -b c b] &\leftrightarrow 45[a b -a c a c -a b] \\
7[a b c d a -d c -b] &\leftrightarrow 36[a b c b a -b d -b] \\
12[a b c -b a -b -c b] &\leftrightarrow 41[a b a -b a c a -c] \\
26[a b -a b a c -a c] &\leftrightarrow 57[a b c b -a -b c -b] \\
28[a b c -b a -b d b] &\leftrightarrow 33[a b c -b a d c -d] \\
30[a -a b -a a -a c -a] &\leftrightarrow 40[a b -a -b c b -a -b] \\
43[a b -a c a d -a e] &\leftrightarrow 46[a b c d -a -b e -d]
\end{aligned}$$

In the following we show in detail that Eq. (13) is indeed verified on the example of the Fourier related pair of signed patterns labeled 7 and 36 above. We used the letters E for pattern 7 and F for pattern 36, and $\omega = \exp(2\pi/8)i$:

$$\chi(E_0^+) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \chi(E_1^+) = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \chi(E_1^-) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \quad \chi(E_2^+) = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix},$$

$$\chi(E_3^+) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \chi(E_3^-) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$\widehat{\chi}(E_0^+) = \begin{pmatrix} 2 \\ 0 \\ 2 \\ 0 \\ 2 \\ 0 \\ 2 \\ 0 \end{pmatrix}, \quad \widehat{\chi}(E_1^+) = \begin{pmatrix} 1 \\ \omega \\ i \\ -\bar{\omega} \\ -1 \\ -\omega \\ -i \\ \bar{\omega} \end{pmatrix}, \quad \widehat{\chi}(E_1^-) = \begin{pmatrix} 1 \\ \bar{\omega} \\ -i \\ -\omega \\ -1 \\ -\bar{\omega} \\ i \\ \omega \end{pmatrix}, \quad \widehat{\chi}(E_2^+) = \begin{pmatrix} 2 \\ 0 \\ -2 \\ 0 \\ 2 \\ 0 \\ -2 \\ 0 \end{pmatrix}, \quad (\text{A1})$$

$$\widehat{\chi}(E_3^+) = \begin{pmatrix} 1 \\ -\bar{\omega} \\ -i \\ \omega \\ -1 \\ \bar{\omega} \\ i \\ -\omega \end{pmatrix}, \quad \widehat{\chi}(E_3^-) = \begin{pmatrix} 1 \\ -\omega \\ i \\ \bar{\omega} \\ -1 \\ \omega \\ -i \\ -\bar{\omega} \end{pmatrix},$$

$$\widehat{\chi}(E_0^+) = \begin{pmatrix} 2 \\ 0 \\ 2 \\ 0 \\ 2 \\ 0 \\ 2 \\ 0 \end{pmatrix}, \quad \widehat{\chi}(E_1^+) - \widehat{\chi}(E_1^-) = \begin{pmatrix} 0 \\ \sqrt{2}i \\ 2i \\ \sqrt{2}i \\ 0 \\ -\sqrt{2}i \\ -2i \\ -\sqrt{2}i \end{pmatrix}, \quad \widehat{\chi}(E_2^+) = \begin{pmatrix} 2 \\ 0 \\ -2 \\ 0 \\ 2 \\ 0 \\ -2 \\ 0 \end{pmatrix}, \quad \widehat{\chi}(E_3^+) - \widehat{\chi}(E_3^-) = \begin{pmatrix} 0 \\ \sqrt{2}i \\ -2i \\ \sqrt{2}i \\ 0 \\ -\sqrt{2}i \\ 2i \\ -\sqrt{2}i \end{pmatrix},$$

on another hand

$$5 \ [a \ c \ d \ e \ e \ b \ f \ c \ f \ g \ b \ d \ g \ g \ d \ b \ g \ f \ c \ f \ b \ e \ e \ d \ c],$$

$$6 \ [a \ d \ e \ f \ g \ b \ h \ i \ j \ k \ c \ l \ m \ m \ l \ c \ k \ j \ i \ h \ b \ g \ f \ e \ d],$$

$$7 \ [a \ g \ h \ i \ j \ c \ k \ l \ n \ b \ d \ p \ m \ o \ q \ e \ r \ s \ t \ u \ f \ v \ w \ x \ y].$$

Finally the remaining patterns are computed from $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$,

$$K_1 = \{1, 2, 3, 4\},$$

$$K_2 = \{1, 4\},$$

$$K_3 = \{1\},$$

$$P^{-1}(K_1) = \mathbb{Z}_{25}^*,$$

$$P^{-1}(K_2) = \{1, 4, 6, 9, 11, 14, 16, 19, 21, 24\},$$

$$P^{-1}(K_3) = \{1, 6, 11, 16, 21\},$$

yielding the six last patterns:

$$8 \ [a \ b \ b \ b \ b \ c \ b \ b \ b \ b \ d \ b \ b \ b \ b \ d \ b \ b \ b \ b \ c \ b \ b \ b \ b],$$

$$9 \ [a \ b \ b \ b \ b \ c \ b \ b \ b \ b \ d \ b \ b \ b \ b \ e \ b \ b \ b \ b \ f \ b \ b \ b \ b],$$

$$10 \ [a \ c \ d \ d \ c \ b \ c \ d \ d \ c \ b \ c \ d \ d \ c \ b \ c \ d \ d \ c \ b \ c \ d \ d \ c],$$

$$11 \ [a \ b \ c \ c \ b \ d \ b \ c \ c \ b \ e \ b \ c \ c \ b \ f \ b \ c \ c \ b \ g \ b \ c \ c \ b],$$

$$12 \ [a \ c \ d \ e \ f \ b \ c \ d \ e \ f \ b \ c \ d \ e \ f \ b \ c \ d \ e \ f \ b \ c \ d \ e \ f],$$

$$13 \ [a \ d \ e \ f \ g \ b \ d \ e \ f \ g \ c \ d \ e \ f \ g \ c \ d \ e \ f \ g \ b \ d \ e \ f \ g].$$

¹J.-Ch. Anglès d'Auriac, J.-M. Maillard, and C. M. Viallet, *J. Phys. A* **39**, 3641 (2006).

²M. P. Bellon, J.-M. Maillard, and C. M. Viallet, *Phys. Lett. A* **159**, 221 (1991).

³R. J. Baxter, *Exactly Solved Model in Lattice Statistical Mechanics* (Academic, New York, 1982).

⁴H. Meyer, J.-C. Anglès d'Auriac, and J.-M. Maillard, *Physica A* **209**, 223 (1994).

⁵S. Boukraa, J.-M. Maillard, and G. Rollet, *Int. J. Mod. Phys. B* **8**, 137 (1994).

⁶S. Boukraa, J.-M. Maillard, and G. Rollet, *Physica A* **209**, 162 (1994).

⁷S. Boukraa, J.-M. Maillard, and G. Rollet, *Int. J. Mod. Phys. B* **8**, 2157 (1994).

⁸R. C. Bose and D. M. Mesner, *Ann. Math. Stat.* **30**, 21 (1959).

⁹F. Jaeger, *J. Math. Soc. Jpn.* **24**, 197 (1996).

¹⁰A conjecture probably due to R. Paley, see http://en.wikipedia.org/wiki/hadamard_matrix#the_hadamard_conjecture.

¹¹B. Schmidt, *J. Am. Math. Soc.* **12**, 929 (1999).

¹²F. Y. Wu, *Rev. Mod. Phys.* **54**, 235 (1982).

¹³Yu. G. Stroganov, *Phys. Lett.* **74A**, 116 (1979).

¹⁴M. T. Jaekel and J.-M. Maillard, *J. Phys. A* **15**, 1309 (1982); M. T. Jaekel and J.-M. Maillard, *ibid.* **15**, 2241 (1982); M. T. Jaekel and J.-M. Maillard, *ibid.* **16**, 1975 (1983).

¹⁵H. Au-Yang, B. M. McCoy, J. H. H. Perk, S. Tang, and Y. M. Lin, *Phys. Lett. A* **123**, 219 (1987).

¹⁶R. Baxter, H. Au-Yang, and J. H. H. Perk, *Phys. Lett. A* **128**, 138 (1988).

¹⁷M. Marcu and V. Rittenberg, *J. Math. Phys.* **22**, 2740 (1981); *J. Math. Phys.* **22**, 2753 (1981).

¹⁸J.-Ch. Anglès d'Auriac, J.-M. Maillard, and C. M. Viallet, *J. Phys. A* **35**, 9251 (2002).

¹⁹S. Boukraa and J.-M. Maillard, *Physica A* **220**, 403 (1995).

- ²⁰E. Bedford and K. Kim, *J. Geom. Anal.* **14**, 567 (2004).
- ²¹N. Abarenkova, J. C. Anglès d'Auriac, and J. M. Maillard, *Physica A* **237**, 123 (1997).
- ²²M. P. Bellon and C.-M. Viallet, *Commun. Math. Phys.* **204**, 425 (1999).
- ²³J.-C. Anglès d'Auriac, S. Boukraa, and J.-M. Maillard, *Ann. Comb.* **3**, 131 (1999).
- ²⁴<http://www.research.att.com/~njas/hadamard>.
- ²⁵T. M. Apostol, *Introduction to Analytic Number Theory* (Springer-Verlag, Berlin, 1998).
- ²⁶K. Ireland and M. Rosen, *A. Classical Introduction to Modern Number Theory*, 2nd ed. (Springer-Verlag, 1990).
- ²⁷M. P. Bellon, J.-M. Maillard, G. Rollet, and C.-M. Viallet, *Int. J. Mod. Phys. B* **6**, 3575 (1992).
- ²⁸N. Abarenkova J.-C. Anglès d'Auriac, S. Boukraa, and J.-M. Maillard, *Physica D* **130**, 27 (1999).
- ²⁹<http://perso.neel.cnrs.fr/jean-christian.angles-dauriac/>.