Proceedings of Prague Stochastics'98, Vol. II, 383–389 August 9, 1998

BLOCK-FACTOR FIELDS OF BERNOULLI SHIFTS

František Matúš

Institute of Information Theory and Automation, Pod vodárenskou věží 4, 182 08 Prague, Czech Republic and
Laboratory of Intelligent Systems, University of Economics, nám. W. Churchila 4, 130 67 Prague, Czech Republic
e-mail: matus@utia.cas.cz

Abstract.* The distributions of the random arrays $(a_{\eta_i,\eta_j};\ i,j \geqslant 1)$ where $(a_{i,j};\ i,j \leqslant n)$ is a matrix and $\eta = (\eta_i;\ i \geqslant 1)$ is an i.i.d. sequence are completely characterized. They must be jointly exchangeable, dissociated and satisfy a new reducibility condition. Probabilities of configurations in these arrays are computed using combinatorial ideas motivated by category theory. The used methods are mainly algebraic and rely on the structure of ring homomorphisms.

AMS 1991 Subject Classification: Primary: 60G09, secondary: 62H05, 12E10, 13F20, 05A15.

Key words: Partial exchangeability, dissociatedness, invariant polynomials, ring homomorphisms.

1. INTRODUCTION

Let $\eta = (\eta_i;\ i \geqslant 1)$ be an i.i.d. sequence, a Bernoulli shift, each η_i taking values in $\widehat{n} = \{1, 2, \dots n\}$, $n \geqslant 1$, with probabilities $p_1, \dots, p_n$. Where $A = (a_{i,j};\ 1 \leqslant i,j \leqslant n)$ is a matrix with entries in a finite nonempty set S, the infinite random array $(a_{\eta_i,\eta_j};\ i,j \geqslant 1)$ will be denoted by $A_{\eta,\eta}$ and called *block-factor field* of the Bernoulli shift η.

A random array $\zeta = (\zeta_{i,j};\ i,j \geqslant 1)$ with the state space S is *jointly exchangeable* if its distribution remains unchanged under permutations $(\zeta_{\pi(i),\pi(j)};\ i,j \geqslant 1)$ where π permutes positive integers. The array is *(jointly) dissociated* if its subarrays $(\zeta_{i,j};\ i,j \leqslant n)$ and $(\zeta_{i,j};\ i,j > n)$ are stochastically independent. Block-factor fields are obviously jointly exchangeable and dissociated. Let us say that a matrix A is *jointly reducible* if there exists $1 \leqslant k < l \leqslant n$ such that the k-th and l-th rows of A coincide, $a_{k,j} = a_{l,j}$, $j \in \widehat{n}$, and the k-th and l-th columns of A coincide $a_{i,k} = a_{i,l}$, $i \in \widehat{n}$. In the block-factor field $A_{\eta,\eta}$ every finite subfield $(a_{\eta_i,\eta_j};\ i,j \leqslant m)$ is jointly reducible a.s. once $m > n$; this is because in the sequence $\eta_1, \dots, \eta_m$ one has $\eta_k = \eta_l$ for some $1 \leqslant k < l \leqslant m$, a.s.

*This research was partially supported by grants A 1075801 of GA AV, 201/98/0478 of GA ČR and by the grant No. VS 96008 of Ministry of Education of Czech Republic.

Theorem 1. *A random array ζ has the same distribution as a block-factor field of a Bernoulli shift if and only if ζ is jointly exchangeable, dissociated and the subarrays $(\zeta_{i,j}; i,j \leqslant m)$ are jointly reducible a.s. for all sufficiently large m.*

This paper is devoted mainly to a proof of the nontrivial implication in Theorem 1. In the next section, square matrices are taken as objects of a category. This algebraic languange enables a succint formulation of basic properties of morphisms, subobjects and congruences needed in the sequel. Since probabilities in $A_{\eta,\eta}$ are polynomials in $p_1, \dots, p_n$ we spend some time by identification of their coefficients in Section 3. Then, two auxiliary lemmas are worked out, on extensions of our objects and on the structure of ring homomorphisms for rings of invariant polynomials. Having proved the desired implication in Section 5, we discuss consequences and related results on separately exchangeable arrays in Section 6.

Partially exchangeable arrays have been studied in detail starting from the representation theorems of Aldous and Hoover, [1, 9]. The basic references seem to be [2, 3, 10, 12, 13, 14]. Two notes, [15, 11], are concerned with the conditional independences within these arrays. De Finetti-type theorems for jointly and separately (row-column) exchangeable arrays and their finite versions in the spirit of [7] are worked out in [18]. For applications to problems of human vision and nice examples we refer to [8]. The structure of these arrays becomes finer with additional rotatable symmetries, cf. [5, 6, 12, 13, 14].

Our methods differ substantially from all approaches the field has seen before. We have no idea how to prove Theorem 1 either by probabilistic methods of [1] or by nonstandart analysis evoked in [9] or by the tools of harmonic analysis as in [20]. We adopt the notion 'block-factor field' in accordance with the notion of 'block-factor sequence', this one being well established. The random sequences of this type were related to partially exchangeable arrays in [19].

2. A CATEGORY OF MATRICES

Let us consider finite nonempty index sets I, J and *objects* $A = (a_{i,j} \in S;\ i,j \in I) = (a_{i,j})_I$, $B = (b_{i,j})_J$. A mapping $\varphi\colon I \to J$ satisfying $A = (b_{\varphi(i),\varphi(j)})_I$ is said to be a *morphism* of A into B. We write $A \xrightarrow{\varphi} B$ or $\varphi \in \mathit{hom}(A,B)$ in this situation. If φ is onto we use the notation $A \xrightarrow{\varphi}\!\!\!\!\twoheadrightarrow B$. The group of automorphisms of A will be denoted by $\mathcal{S}_A = \{\tau;\ A \xrightarrow{\tau}\!\!\!\!\twoheadrightarrow A\}$.

Where J is a nonempty subset of I, $A^J = (a_{i,j})_J$ is a *subobject* of the object $A = (a_{i,j})_I$. An equivalence $\sim$ on I such that $a_{i,j} = a_{k,l}$ once $i \sim k$ and $j \sim l$ is called *congruence* of A. If $I_\sim$ is the set of all blocks of the equivalence $\sim$ and $i_\sim$ is the block containing $i \in I$ the *factorobject* $A_\sim = (d_{i_\sim,j_\sim})_{I_\sim}$ of A is defined unambiguously by $d_{i_\sim,j_\sim} = a_{k,l}$ where $k \in i_\sim$ and $l \in j_\sim$. Obviously, $A \xrightarrow{\sim}\!\!\!\!\twoheadrightarrow A_\sim$ where the sign $\sim$ was (mis)used to denote the factormapping of the equivalence $\sim$.

The equivalence on I having one-element blocks exclusively is always a congruence of A. If this is the only congruence of A we call A *simple*. It is flat that $A = (a_{i,j})_{\widehat{n}}$ is simple if and only if A is not jointly reducible.

The following two lemmas exhibit basic properties of morphisms and congruences in our category. We do not supply proofs as they are almost straightforward.

Lemma 1.
(i) If $A \xrightarrow{\varphi} B$ then the equivalence $\sim_\varphi$ on I with the blocks $\varphi^{-1}(j)$, $j \in \varphi(I)$, is a congruence of A.
(ii) The equivalence $\approx_A$ on I given by $[i \approx j$ if and only if $a_{i,l} = a_{j,l}$ for $l \in I$ and $a_{k,i} = a_{k,j}$ for $k \in I]$ is the coarsest congruence of A.
(iii) Whenever $A \xrightarrow{\varphi}\!\!\!\!\twoheadrightarrow B$, B is simple if and only if $\sim_\varphi = \approx_A$.
(iv) If $A \xrightarrow{\varphi}\!\!\!\!\twoheadrightarrow B$, B is simple and $A \xrightarrow{\psi}\!\!\!\!\twoheadrightarrow C$ then $C \xrightarrow{\chi}\!\!\!\!\twoheadrightarrow B$ for unique $\chi \in \mathit{hom}(C,B)$ such that $\varphi = \chi\psi$.
(v) If $A \xrightarrow{\varphi}\!\!\!\!\twoheadrightarrow B$, $A \xrightarrow{\psi}\!\!\!\!\twoheadrightarrow C$ and both B,C are simple matrices then they are isomorphical.
(vi) If $A \xrightarrow{\varphi}\!\!\!\!\twoheadrightarrow B$ and B is a simple matrix then $\mathit{hom}(A,B)$ is equal to $\{\tau\varphi;\ \tau \in \mathcal{S}_B\}$. Especially, $\mathit{hom}(A,A) = \mathcal{S}_A$ for every simple matrix A.

The nonstandard notation $\#I$ for the cardinality of I will later make some formulas easier to read.

Lemma 2.
(i) If $A \xrightarrow{\chi\varphi} B$ and $C \xrightarrow{\chi} B$ then $A \xrightarrow{\varphi} C$.
(ii) If $B \xrightarrow{\varphi} A$ then there exists $K \subset I$ such that A^K is simple and $B \xrightarrow{\psi}\!\!\!\!\twoheadrightarrow A^K$ for some morphism ψ.
(iii) If $B \xrightarrow{\varphi}\!\!\!\!\twoheadrightarrow A$, $C \xrightarrow{\psi}\!\!\!\!\twoheadrightarrow A$ and $\#\varphi^{-1}(i) = \#\psi^{-1}(\tau^{-1}(i))$ for all $i \in I$ and for some permutation $\tau \in \mathcal{S}_A$ then B and C are isomorphical and $C \xrightarrow{\chi}\!\!\!\!\twoheadrightarrow B$ for some morphism χ satisfying $\varphi\chi = \tau\psi$.

$$\begin{tikzcd} B \arrow[r, two heads, "\varphi"] & A \\ C \arrow[u, two heads, "\chi"] \arrow[r, two heads, "\psi"'] & A \arrow[u, two heads, "\tau"'] \end{tikzcd}$$

(iv) If $B \xrightarrow{\varphi}\!\!\!\!\twoheadrightarrow A$, $C \xrightarrow{\psi}\!\!\!\!\twoheadrightarrow A$ and $\#\varphi^{-1}(i) = \sum_{k\in\psi^{-1}(i)} \gamma(k)$, $i \in I$, where $\gamma(k)$, $k \in K$, are positive integers then there exists $\chi \in \mathit{hom}(B,C)$ such that $\#\chi^{-1}(k) = \gamma(k)$, $k \in K$.

No deep knowledge in categories is necessary, we borrowed nothing but the parsimonious 'arrow-morphism' notation, cf. [16].

3. PROBABILITIES IN BLOCK-FACTOR FIELDS

Having the block-factor field $A_{\eta,\eta}$, $A = (a_{i,j})_{\widehat{n}}$, of a Bernoulli shift η, we can express the probability $\mathit{pr}_{A_{\eta,\eta}}(B)$ of seeing $B = (b_{i,j})_{\widehat{m}}$ in $A_{\eta,\eta}$, i.e. the probability of the event $[a_{\eta_i,\eta_j} = b_{i,j}$ for $i,j \leqslant m]$ by means of morphisms

$$\mathit{pr}_{A_{\eta,\eta}}(B) = \sum_{\varphi\in \mathit{hom}(B,A)} \prod_{i=1}^{n} p_i^{\#\varphi^{-1}(i)} \ .$$

The above product is exactly the probability of the event $[\eta_j = \varphi(j),\ j \leqslant m]$. Thus, in the block-factor fields constructed from A, the above probability is zero once $\mathit{hom}(B,A) = \emptyset$. Note that it is obtained by the substitution of $p_1,\ldots,p_n$ into a polynomial in n indeterminates. Though we do not need it in the proof of Theorem 1, we find it interesting to investigate coefficients of these polynomials below. Besides, it is a good occasion to fix further necessary notation and to build an intuition.

Given a set $I = \widehat{n}$, let $\mathcal{M}_I = \{0,1,\ldots\}^I$ denote the family of all multisets of I; for a multiset $\alpha \in \mathcal{M}_I$ we will work with $\mathit{supp}(\alpha) = \{i \in I;\ \alpha(i) > 0\}$. Typically, a multiset α will arise from a morphism $\varphi \in \mathit{hom}(B,A)$ by $\alpha(i) = \#\varphi^{-1}(i)$, $i \in I$; we write also $\alpha = \#\varphi^{-1}$.

The group $\mathcal{S}_A$ acts naturally on the family $\mathcal{M}_I$. For $\alpha \in \mathcal{M}_I$, let $[\alpha] \subset \mathcal{M}_I$ be the *orbit* of α under the action, $[\alpha] = \{\alpha\tau;\ \tau \in \mathcal{S}_A\}$, and let $\mathcal{S}_{A,\alpha} \subset \mathcal{S}_A$ be the *stabilizer* of α, $\mathcal{S}_{A,\alpha} = \{\tau \in \mathcal{S}_A;\ \alpha = \alpha\tau\}$. As usually,

$$\#\mathcal{S}_A = \#[\alpha] \cdot \#\mathcal{S}_{A,\alpha}\ , \qquad \alpha \in \mathcal{M}_I\ .$$

If $\alpha,\beta \in \mathcal{M}_I$ and $J = \mathit{supp}(\alpha)$, $K = \mathit{supp}(\beta)$ are both nonempty sets we say that α and β are *A-related* when $A^J \xrightarrow{\chi}\!\!\!\!\twoheadrightarrow A^K$ for some χ such that $\beta(k) = \sum_{j\in\chi^{-1}(k)} \alpha(j)$, $k \in K$. The new combinatorial quantity $\binom{\beta}{\alpha}_A$ is defined to be zero if the multisets α and β are not A-related and to be $\prod_{k\in K} \beta(k)! \cdot \big(\prod_{j\in J} \alpha(j)!\big)^{-1}$, otherwise.

To examine $\mathit{pr}_{A_{\eta,\eta}}(B)$ when $\mathit{hom}(B,A) \neq \emptyset$, we know by Lemma 2 (ii) that there exists $K \subset \widehat{n}$ such that A^K is simple and $B \xrightarrow{\psi} A^K$ for a suitable ψ. This K need not be unique but due to Lemma 1 (iv) A^K is specified up to an isomorphism. Now, we can formulate

Proposition 1. *If $B = (b_{i,j})_{\widehat{m}} \xrightarrow{\psi} A^K$ and A^K is simple for some $K \subset \widehat{n}$ then*

$$\mathit{pr}_{A_{\eta,\eta}}(B) = \#\mathcal{S}_{A^K,\#\psi^{-1}} \cdot \sum_{\alpha \in \mathcal{M}_{\widehat{n}}} \binom{\beta}{\alpha}_A \prod_{i=1}^{n} p_i^{\alpha(i)}$$

where $\beta \in \mathcal{M}_{\widehat{n}}$ is given by $\beta(k) = \#\psi^{-1}(k)$, $k \in K$, and by $\beta(k) = 0$ otherwise.

Note that only a finite number of summands is nonzero because if $\sum_{i\in\widehat{n}} \alpha(i) \neq \sum_{k\in K} \#\psi^{-1}(k)$ $(= \sum_{i\in\widehat{n}} \beta(i))$ then α and β are not A-related.

Proof. We have to show that for $\alpha \in \mathcal{M}_{\widehat{n}}$ cardinality of the set

$$\{\varphi \in \mathit{hom}(B, A^{\mathit{supp}(\alpha)});\ \alpha(i) = \#\varphi^{-1}(i) \text{ for } i \in \mathit{supp}(\alpha)\}$$

is $\#\mathcal{S}_{A^K,\#\psi^{-1}} \cdot \binom{\beta}{\alpha}_A$. By Lemma 1 (iv), for every φ in this set there is a unique χ such that $A^{\mathit{supp}(\alpha)} \xrightarrow{\chi} A^K$ and $\psi = \chi\varphi$. In addition, $\#\psi^{-1}(k) = \sum_{j\in\chi^{-1}(k)} \alpha(j)$, $k \in K$. Thus, α and β are A-related if the displayed set is nonempty. The converse is true owing to Lemma 2 (iv).

Let us consider the set $\mathcal{X}$ of all χ's making α and β A-related; we can assume that $\mathcal{X}$ is nonempty. By Lemma 1 (vi) two $\chi, \phi \in \mathcal{X}$ are tied by $\chi = \tau\phi$ where $\tau \in \mathcal{S}_{A^K}$. This τ must leave $\beta|_K = \#\psi^{-1} \in \mathcal{M}_K$ invariant and hence $\#\mathcal{X} = \#\mathcal{S}_{A^K,\#\psi^{-1}}$. Now we partition the starting set into

$$\sum_{\chi\in\mathcal{X}} \{\varphi;\ B \xrightarrow{\varphi} A^{\mathit{supp}(\alpha)},\ \#\varphi^{-1} = \alpha|_{\mathit{supp}(\alpha)},\ \psi = \chi\varphi\}$$

and, having in mind Lemma 2 (i), drop out the morphism condition. It is an easy combinatorial task to find that the cardinalities of all above sets are

$$\prod_{k\in K} \frac{\beta(k)!}{\prod_{j\in\chi^{-1}(k)} \alpha(j)!} = \binom{\beta}{\alpha}_A$$

what closes the proof. ∎

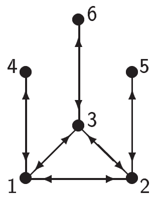
Consequence 1. *If $B \xrightarrow{\psi} A$, A is a simple matrix and $\beta = \#\psi^{-1}$ then*

$$\mathit{pr}_{A_{\eta,\eta}}(B) = \#\mathcal{S}_{A,\beta} \cdot \sum_{\alpha\in[\beta]} p^\alpha = \sum_{\tau\in\mathcal{S}_A} p^{\beta\tau}$$

where p^α abbreviates $\prod_{i=1}^n p_i^{\alpha(i)}$.

It is a crucial observation that the polynomials behind the probabilities in Consequence 1 are invariant to the permutations $\tau \in \mathcal{S}_A$ of variables. The key idea of the proof of Theorem 1 is to mimic properties of these polynomials.

Example. Let $S = \{0,1\}$ and A be the adjacency matrix of the following digraph



$$A = \begin{pmatrix} 0&1&1&1&0&0\\ 1&0&1&0&1&0\\ 1&1&0&0&0&1\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0 \end{pmatrix}.$$

Since $\#\mathcal{S}_A = 6$ we have $\mathit{pr}_{A_{\eta,\eta}}(A) = 6 \cdot p_1 p_2 \cdots p_6$. Further, let us take

$$B = \begin{pmatrix} 0&0&0&1&1&1\\ 0&0&0&1&1&1\\ 0&0&0&1&1&1\\ 1&1&1&0&0&0\\ 1&1&1&0&0&0\\ 1&1&1&0&0&0 \end{pmatrix} \xrightarrow{\psi} \begin{pmatrix} 0&1\\ 1&0 \end{pmatrix} = A^K$$

where $K = \{1,2\}$ and $\#\psi^{-1}(1) = \#\psi^{-1}(2) = 3$. Obviously $\#\mathcal{S}_{A^K,\#\psi^{-1}} = 2$ and

$$\begin{aligned}\mathit{pr}_{A_{\eta,\eta}}(B) = 2(&p_1^3p_2^3 + p_1^3p_3^3 + p_2^3p_3^3 + p_1^3p_4^3 + p_2^3p_5^3 + p_3^3p_6^3)\\ &+ 6(p_1^3p_3p_4^2 + p_1^3p_3^2p_4 + p_1^3p_2p_4^2 + p_1^3p_2^2p_4 + \dots)\end{aligned}$$

(8 missing terms).

4. TWO AUXILIARY LEMMAS

This section has a preparatory character. First, let $A = (A_{i,j})_I$, $B = (B_{i,j})_J$ and $C = (C_{i,j})_K$ be three matrices such that $J \cap K = \emptyset$. We are going to investigate extensions of B and C, i.e. the set $\mathcal{E}_A(B,C)$ given by

$$\{D = (d_{i,j})_{J\cup K}\ ;\ D^J = B,\ D^K = C \text{ and } \mathit{hom}(D,A) \neq \emptyset\}.$$

This set is obviously nonempty if and only if $\mathit{hom}(B,A)$ and $\mathit{hom}(C,A)$ are nonempty.

Lemma 3. *Let $L \subset I$, both matrices A and A^L be simple, and $B \xrightarrow{\varphi} A$, $C \xrightarrow{\psi} A^L$.*
(i) *Let $L = I$. Where $\tau \in \mathcal{S}_A$, we define the mapping $\chi_\tau\colon J \cup K \to I$ by $\chi_\tau|_J = \varphi$ and $\chi_\tau|_K = \tau\psi$. There is a unique D_τ such that $D_\tau \xrightarrow{\chi_\tau} A$. The mapping $\tau \mapsto D_\tau$ is a bijection between $\mathcal{S}_A$ and $\mathcal{E}_A(B,C)$.*
(ii) *Let $A = B$. Where $\phi \in \mathit{hom}(C,A)$ we define the mapping $\chi_\phi\colon I \cup K \to I$ by $\chi_\phi|_I = \mathit{id}$ and $\chi_\phi|_K = \phi$. There is*

a unique D_ϕ such that $D_\phi \xrightarrow{\chi_\phi} A$. The mapping $\phi \mapsto D_\phi$ is a bijection between $hom(C,A)$ and $\mathcal{E}_A(A,C)$.

Proof. (i) It is straightforward that $D_\tau \in \mathcal{E}_A(B,C)$ for all $\tau \in \mathcal{S}_A$. If $D \in \mathcal{E}_A(B,C)$, $D \xrightarrow{\chi} A$ then by Lemma 1 (vi) $hom(D,A) = \{\varrho\chi;\ \varrho \in \mathcal{S}_A\}$. Thus $D^J = B \xrightarrow{\varrho\chi|_J} A$ and $D^K = C \xrightarrow{\varrho\chi|_K} A$. Using Lemma 1 (iv), $\varrho\chi|_J = \pi_\varrho\varphi$ and $\varrho\chi|_K = \tau_\varrho\psi$ for unique $\pi_\varrho, \tau_\varrho \in \mathcal{S}_A$. Since $\pi_\sigma = \sigma\varrho^{-1}\pi_\varrho$ and $\tau_\sigma = \sigma\varrho^{-1}\tau_\varrho$, $\sigma, \varrho \in \mathcal{S}_A$, the permutation $\pi_\varrho^{-1}\tau_\varrho$ does not depend on ϱ. It does not depend on χ as well. Thus, we have constructed a mapping $D \mapsto \pi_\varrho^{-1}\tau_\varrho$ which is easily seen to be inverse to $\tau \mapsto D_\tau$.

(ii) We proceed as in (i). Obviously, $D_\phi \in \mathcal{E}_A(A,C)$. If $D \in \mathcal{E}_A(A,C)$ and $D \xrightarrow{\chi} A$ then owing to Lemma 1 (vi) $hom(D,A) = \{\varrho\chi;\ \varrho \in \mathcal{S}_A\}$. But $D^I = A \xrightarrow{\varrho\chi|_I} A$ whence we have $\tau_\varrho = \varrho\chi|_I \in \mathcal{S}_A$. Also, $D^K = C \xrightarrow{\varrho\chi|_K} A$ and thus $\tau_\varrho^{-1}(\varrho\chi|_K) = (\chi|_I)^{-1}\chi|_K$ is a morphism from $hom(C,A)$. It does not depend on ϱ and χ. We have again a mapping $D \mapsto (\chi|_I)^{-1}\chi|_K$ which is inverse to $\phi \mapsto D_\phi$. ∎

In the second part of this section we want to formulate a fact on ring homomorphisms. It may be known or regarded as 'easy' by a specialist in commutative algebra, but we have not found an explicit reference.

We are going to work with the ring $\mathbb{C}[x_1,\dots,x_n]$ of polynomials in n variables $x = (x_1,\dots,x_n)$, coefficients ranging in the field of complex numbers $\mathbb{C}$. A polynomial

$$f(x) = f(x_1,\dots,x_n) = \sum_{\alpha\in\mathcal{M}_{\widehat{n}}} c_\alpha x^\alpha \ ,$$

where $x^\alpha = \prod_{i=1}^n x_i^{\alpha(i)}$ and only finite number of the coefficients $c_\alpha \in \mathbb{C}$ is nonzero, is invariant to a permutation $\tau\colon \widehat{n} \mapsto \widehat{n}$ if

$$f(x) = f(x_{\tau(1)},\dots,x_{\tau(n)}) = \sum_{\alpha\in\mathcal{M}_{\widehat{n}}} c_\alpha x^{\alpha\tau^{-1}} \ .$$

Let G be a group of permutations of $\widehat{n}$. The set of all polynomials that are invariant to every $\tau \in G$ is a subring $\mathbb{C}[x_1,\dots,x_n]^G$ of $\mathbb{C}[x_1,\dots,x_n]$. We need to understand all homomorphisms of $\mathbb{C}[x_1,\dots,x_n]^G$ onto $\mathbb{C}$, i.e. all mappings conserving addition, multiplication and moving the constant polynomial 1 onto $1 \in \mathbb{C}$.

If $a = (a_1,\dots,a_n)$ is an n-tuple of complex numbers the substitution of a into a polynomial $f(x)$ gives a complex number $f(a)$. The mapping $\Phi_a\colon \mathbb{C}[x_1,\dots,x_n] \to \mathbb{C}$ given by $\Phi_a(f(x)) = f(a)$ is obviously a homomorphism. Also $\Phi_a \neq \Phi_b$ if $a, b \in \mathbb{C}^n$ are different. It is a consequence of the Nullstellensatz that every homomorphism of $\mathbb{C}[x_1,\dots,x_n]$ onto $\mathbb{C}$ equals Φ_a for some $a \in \mathbb{C}^n$.

The group G acts naturally on $\mathbb{C}^n$ moving a point a to the n-tuple $(a_{\tau(1)},\dots,a_{\tau(n)})$ for $\tau \in G$. Let Ga be the orbit of a. If $b \in Ga$ then it is not difficult to see that the restrictions of Φ_a and Φ_b on $\mathbb{C}[x_1,\dots,x_n]^G$ coincide. Let us denote them by Φ_{Ga}. Also, $\Phi_{Ga} \neq \Phi_{Gb}$ if $Ga \neq Gb$ (if this is not clear, a look in [4] p. 347, Exercise 12 will help). We are going to demonstrate that Φ_{Ga}, $a \in \mathbb{C}^n$, exhaust all the desired homomorphisms.

Lemma 4. *For every ring homomorphism Ψ of the ring of G-invariant polynomials $\mathbb{C}[x_1,\dots,x_n]^G$ onto $\mathbb{C}$ there exists $a \in \mathbb{C}^n$ such that $\Psi = \Phi_{Ga}$.*

Proof. The ring $\mathbb{C}[x_1,\dots,x_n]^G$ is finitely generated, i.e. there exist polynomials $f_1(x),\dots,f_m(x)$ in the ring such that every $f(x) \in \mathbb{C}[x_1,\dots,x_n]^G$ can be writen as

$$f(x) = g(f_1(x),\dots,f_m(x))$$

for at least one $g(y) \in \mathbb{C}[y_1,\dots,y_m]$. This is a consequence of the Hilbert's basis theorem, see also the Noether's theorem in [4] (Theorem 5, p. 331). It is easy to see that the mapping Φ given by

$$\Phi(g(y)) = g(f_1(x),\dots,f_m(x))$$

is a homomorphism of $\mathbb{C}[y_1,\dots,y_m]$ onto $\mathbb{C}[x_1,\dots,x_n]^G$.

Given a homomorphism $\Psi\colon \mathbb{C}[x_1,\dots,x_n]^G \to \mathbb{C}$, the composition $\Psi\Phi$ is equal to a homomorphism Φ_c for some $c \in \mathbb{C}^m$. Let $\mathbb{I}$ be the ideal in $\mathbb{C}[x_1,\dots,x_n]$ generated by $f_j(x) - c_j$, $j \in \widehat{m}$. We claim that $\mathbb{I} \neq \mathbb{C}[x_1,\dots,x_n]$. In fact, if not, the polynomial 1 could be written as the sum $\sum_{j=1}^m (f_j(x) - c_j)h_j^*(x)$ for some $h_j^*(x)$ in $\mathbb{C}[x_1,\dots,x_n]$. Let us permute variables in this expression by $\tau \in G$ and average over $\tau \in G$. We get

$$1 = \sum_{j=1}^m \big(f_j(x) - c_j\big)h_j(x)$$

where, however, every $h_j(x) \in \mathbb{C}[x_1,\dots,x_n]^G$, $j \in \widehat{m}$, admits the form $h_j(x) = g_j(f_1(x),\dots,f_m(x))$. Applying Ψ to the left-hand side we obtain $1 \in \mathbb{C}$ and to the right-hand side

$$\Psi\Phi\Big(\sum_{j=1}^m \ (y_j - c_j)\ g_j(y_1,\dots,y_m)\Big) = 0 \ ,$$

a contradiction.

Since $\mathbb{I}$ is a proper ideal of $\mathbb{C}[x_1,\dots,x_n]$ the Nullstellensatz implies existence of $a \in \mathbb{C}^n$ such that $f_j(a) = c_j$, $j \in \widehat{m}$. If a polynomial $f(x) \in \mathbb{C}[x_1,\dots,x_n]^G$ is expressed as $f(x) = g(f_1(x),\dots,f_m(x))$ then

$$\begin{aligned}\Psi(f(x)) = \Psi\Phi(g(y)) &= g(c_1,\dots,c_m)\\ &= g(f_1(a),\dots,f_m(a)) = f(a)\end{aligned}$$

what entails $\Psi = \Phi_{Ga}$. ∎

5. PROOF OF THEOREM 1

Only one implication is nontrivial. Let ζ be an array satisfying the three assumptions. We will construct a matrix A and a Bernoulli shift η leading to the block-factor field $A_{\eta,\eta}$ having the same distribution as ζ.

Let $n \geqslant 1$ be maximal such that $(\zeta_{i,j};\ i,j \leqslant n)$ is not jointly reducible a.s. Then there exists a simple matrix $A = (a_{i,j})_{\widehat{n}}$ with a positive probability, $pr_\zeta(A) > 0$. We show that $hom(B,A) \neq \emptyset$ for every B of positive probability. In fact, by the joint exchangeability of ζ we can suppose that $B = (b_{i,j})_J$ where $J \cap \widehat{n} = \emptyset$. The dissociatedness implies that $pr_\zeta(A) \cdot pr_\zeta(B)$ is equal to

$$\sum \{ pr_\zeta(D);\ D = (d_{i,j})_{\widehat{n}\cup J},\ D^{\widehat{n}} = A \text{ and } D^J = B \} \ .$$

If $pr_\zeta(B) > 0$ then $pr_\zeta(D) > 0$ for at least one matrix D on the right. By Lemma 2 (ii) $D \xrightarrow{\psi} D^K$ where D^K is a simple submatrix of D and $K \subset \widehat{n} \cup J$. Since $pr_\zeta(D^K)$ is positive the maximality of n entails $\#K \leqslant n$. But $D^{\widehat{n}} = A \xrightarrow{\psi|_{\widehat{n}}} D^K$ and by Lemma 1 (i) the restriction $\psi|_{\widehat{n}}$ must be injective. Therefore $\#K = n$ and A and D^K are isomorphic. Consequently, $D \xrightarrow{\varphi} A$ for some φ whence $\varphi|_J \in hom(B,A)$.

We shall say that A is the *characteristic configuration* of ζ. It is unique up to isomorphisms (note that if a matrix $B = (b_{i,j})_{\widehat{n}}$ is simple and $pr_\zeta(B) > 0$, then $hom(B,A)$ is nonempty and A, B are isomorphic).

Let $\beta \in \mathcal{M}^+_{\widehat{n}} = \{\alpha \in \mathcal{M}_{\widehat{n}};\ \alpha(i) > 0, i \in \widehat{n}\}$ and $[\beta]$ be the orbit of β under the action of $\mathcal{S}_A$. Every two matrices in the nonempty set

$$\{B\,;\ \exists\varphi \in hom(B,A)\ \#\varphi^{-1} \in [\beta]\}$$

are isomorphical by Lemma 2 (iii). Using the joint exchangeability, pr_ζ is constant on this set and we can denote this probability by $\mathfrak{r}[\beta]$. In this way we specified a nonnegative function $\mathfrak{r}$ on orbits of $\mathcal{M}^+_{\widehat{n}}$. Since ζ is dissociated we have for any $B \xrightarrow{\varphi} A$ and $C \xrightarrow{\psi} A$, $J \cap K = \emptyset$,

$$pr_\zeta(B) \cdot pr_\zeta(C) = \sum_{D \in \mathcal{E}_A(B,C)} pr_\zeta(D) = \sum_{\tau \in \mathcal{S}_A} pr_\zeta(D_\tau)$$

applying Lemma 3 (i). If $\beta = \#\varphi^{-1}$ and $\gamma = \#\psi^{-1}$ then $\#\chi_\tau^{-1} = \beta + \gamma\tau^{-1}$ and we can recast this equality into

$$\mathfrak{r}[\beta] \cdot \mathfrak{r}[\gamma] = \sum_{\tau \in \mathcal{S}_A} \mathfrak{r}[\beta + \gamma\tau] \,, \qquad \beta, \gamma \in \mathcal{M}^+_{\widehat{n}} \ .$$

Where $\iota \in \mathcal{M}^+_{\widehat{n}}$ is the characteristic function of $\widehat{n}$, $\iota(i) = 1$, $i \in \widehat{n}$, we have $\mathfrak{r}[\iota + \alpha] \cdot \mathfrak{r}[\iota] = \#\mathcal{S}_A \cdot \mathfrak{r}[2\iota + \alpha]$ and then

$$\mathfrak{r}[\iota + \alpha] \cdot \mathfrak{r}[\iota + \beta] \cdot \#\mathcal{S}_A = \sum_{\tau \in \mathcal{S}_A} \mathfrak{r}[\iota + \alpha + \beta\tau] \cdot \mathfrak{r}[\iota]$$

for any $\alpha, \beta \in \mathcal{M}_{\widehat{n}}$.

If $\mathfrak{q}[\alpha] = \#[\alpha] \cdot \mathfrak{r}[\iota + \alpha]/\mathfrak{r}[\iota]$ for $\alpha \in \mathcal{M}_{\widehat{n}}$ this equality leads to

$$\begin{aligned} \mathfrak{q}[\alpha] \cdot \mathfrak{q}[\beta] &= \frac{\#[\alpha] \cdot \#[\beta]}{\#\mathcal{S}_A} \sum_{\tau \in \mathcal{S}_A} \frac{\mathfrak{q}[\alpha + \beta\tau]}{\#[\alpha + \beta\tau]} \\ &= \#[\alpha] \sum_{\delta \in [\beta]} \frac{\mathfrak{q}[\alpha + \delta]}{\#[\alpha + \delta]} \end{aligned}$$

and then to

$$\mathfrak{q}[\alpha] \cdot \mathfrak{q}[\beta] = \sum_{\gamma \in [\alpha]} \sum_{\delta \in [\beta]} \frac{\mathfrak{q}[\gamma + \delta]}{\#[\gamma + \delta]} \,, \qquad \alpha, \beta \in \mathcal{M}_{\widehat{n}} \ .$$

For $\varepsilon \in \mathcal{M}_{\widehat{n}}$ the integer-valued function

$$\varepsilon \longmapsto \#\{(\gamma, \delta) \in [\alpha] \times [\beta]\,;\ \gamma + \delta = \varepsilon\}$$

is obviously constant on orbits; let $\mathfrak{O}_{[\alpha][\beta]}[\varepsilon]$ be this cardinality. With this notation

$$\mathfrak{q}[\alpha] \cdot \mathfrak{q}[\beta] = \sum_{[\varepsilon]} \mathfrak{O}_{[\alpha][\beta]}[\varepsilon] \cdot \mathfrak{q}[\varepsilon] \,, \qquad \alpha, \beta \in \mathcal{M}_{\widehat{n}} \,, \qquad (*)$$

where the summation is over orbits $[\varepsilon]$. Only finite number of summands is nonzero.

Every polynomial $f(x) \in \mathbb{C}[x_1, \dots, x_n]^{\mathcal{S}_A}$ can be written uniquely in the form $f(x) = \sum_{[\alpha]} c_{[\alpha]} x^{[\alpha]}$ where $c_{[\alpha]}$ are complex numbers, only finite number of them being nonzero, and $x^{[\alpha]} = \sum_{\beta \in [\alpha]} x^\beta$. Let

$$\Psi(f(x)) = \sum_{[\alpha]} c_{[\alpha]}\, \mathfrak{q}[\alpha] \ .$$

We claim that Ψ is a ring homomorphism mapping the ring $\mathbb{C}[x_1, \dots, x_n]^{\mathcal{S}_A}$ to $\mathbb{C}$. We are going to show only that Ψ conserves products. If $g(x) = \sum_{[\beta]} d_{[\beta]} x^{[\beta]}$ then

$$\begin{aligned} \Psi(f(x) \cdot g(x)) &= \Psi\Bigl(\sum_{[\alpha]} \sum_{[\beta]} c_{[\alpha]} d_{[\beta]} \sum_{[\varepsilon]} \mathfrak{O}_{[\alpha][\beta]}[\varepsilon] \cdot x^{[\varepsilon]} \Bigr) \\ &= \Psi(f(x)) \cdot \Psi(g(x)) \end{aligned}$$

because the mapping $[\alpha] \mapsto x^{[\alpha]}$ satisfies $(*)$. By Lemma 4 there exist complex numbers $(p_1, \dots, p_n) = p \in \mathbb{C}^n$ such that $\mathfrak{q}[\alpha] = \Psi(x^{[\alpha]}) = p^{[\alpha]}$. If a polynomial $f(x)$ from $\mathbb{C}[x_1, \dots, x_n]^{\mathcal{S}_A}$ has all coefficients nonnegative then obviously $\Psi(f(x)) \geqslant 0$. Especially, if $f[x]$ is symmetric, i.e. invariant to all permutations of $\widehat{n}$, then $\Psi(f(x)) = f(p) \geqslant 0$. By [17] the numbers $p_1, \dots, p_n$ must be nonnegative.

As $\mathfrak{r}[\iota]^2 = \#\mathcal{S}_A \cdot \mathfrak{r}[2\iota]$ and $\mathfrak{q}[\iota] \cdot \mathfrak{r}[\iota] = \mathfrak{r}[2\iota]$ we arrive at $\mathfrak{r}[\iota] = \#\mathcal{S}_A \cdot p^\iota$ and

$$\mathfrak{r}[\iota + \alpha] = \mathfrak{r}[\iota] \cdot p^{[\alpha]}/\#[\alpha] = \#\mathcal{S}_{A,\alpha} \cdot p^{[\iota + \alpha]} \,, \qquad \alpha \in \mathcal{M}_{\widehat{n}} \ .$$

Note that $\mathfrak{r}[\iota] = pr_\zeta(A)$ is positive and all p_i must be therefore positive. That means $pr_\zeta(B) = \#\mathcal{S}_{A,\#\varphi^{-1}} \cdot p^{[\#\varphi^{-1}]}$ for $B \xrightarrow{\varphi} A$, cf. Consequence 1. Further, if $C = (c_{i,j})_K$, $K \cap \widehat{n} = \emptyset$ and $hom(C, A) \neq \emptyset$ then by Lemma 2 (ii) there exists $L \subset \widehat{n}$ such that A^L is simple and $C \xrightarrow{\psi} A^L$ for a morphism ψ. Using Lemma 3 (ii) one gets

$$pr_\zeta(A) \cdot pr_\zeta(C) = \sum_{D \in \mathcal{E}_A(A,C)} pr_\zeta(D) = \sum_{\phi \in hom(C,A)} pr_\zeta(D_\phi) .$$

It is easy to see that $pr_\zeta(D_\phi) = \#\mathcal{S}_{A,\iota+\#\phi^{-1}} \cdot p^{[\iota+\#\phi^{-1}]}$ and thus

$$pr_\zeta(C) = \sum_{\phi \in hom(C,A)} \frac{p^{[\#\phi^{-1}]}}{\#[\#\phi^{-1}]} = \sum_{\phi \in hom(C,A)} p^{\#\phi^{-1}}.$$

This formula is valid even for all matrices C. As a consequence

$$1 = \sum_{s \in S} pr_\zeta(C_s) = \sum_{s \in S} \sum_{i \in I_s} p_i = \sum_{i=1}^{n} p_i$$

where C_s is the matrix with one entry equal to s and $I_s = \{i \in \widehat{n};\ a_{i,i} = s\}$. If η is the Bernoulli shift ruled by $p_1, \dots, p_n$ then the arrays $A_{\eta,\eta}$ and ζ have the same distribution. ∎

6. REMARKS

Let $A = (a_{i,j})_{\widehat{n}}$ be a matrix and η a Bernoulli shift with the probabilities $p_1, \dots, p_n$. If $J = \{j \in \widehat{n};\ p_j > 0\}$ we can reduce the submatrix A^J to a simple submatrix A^K, $K \subset J$, by $A^J \xrightarrow{\phi} A^K$, and set $q_k = \sum_{j \in \phi^{-1}(k)} p_j$ for $k \in K$. The random field $A_{\eta,\eta}$ has obviously the same disribution as the block-factor field constructed from A^K and the Bernoulli shift ruled by q_k, $k \in K$. Therefore, comparing the fields $A_{\eta,\eta}$ we can assume that A is simple and all p_i are positive.

Consequence 2. *Let $A = (a_{i,j})_{\widehat{n}}$ and $B = (b_{i,j})_{\widehat{m}}$ be two simple matrices and η and ξ two Bernoulli shifts ruled by positive probabilities $p_1, \dots, p_n$ and $q_1, \dots, q_m$, respectively. The fields $A_{\eta,\eta}$ and $B_{\xi,\xi}$ are equidistributed if and only if there exists an isomorphism φ of A onto B such that $p_i = q_{\varphi(i)}$, $i \leqslant n$.*

Proof. One implication is trivial. If $A_{\eta,\eta} \stackrel{d}{=} B_{\xi,\xi} = \zeta$ then both A and B must be the characteristic configurations of ζ and thus $n = m$ and $A \xrightarrow{\chi} B$ for an isomorphism χ. Since, $pr_{A_{\eta,\eta}}(C) = pr_{B_{\xi,\xi}}(C)$ we have

$$\sum_{\varphi \in hom(C,A)} p^{\#\varphi^{-1}} = \sum_{\varphi \in hom(C,A)} q^{\#(\chi\varphi)^{-1}} = \sum_{\varphi \in hom(C,A)} r^{\#\varphi^{-1}}$$

where $r = (q_{\chi(1)}, \dots, q_{\chi(n)})$. Thus, $\Phi_{Gp} = \Phi_{Gr}$ denoting $G = \mathcal{S}_A = \mathcal{S}_B$. Then $p_i = q_{\tau\chi(i)}$, $i \leqslant n$, for some permutation $\tau \in G$ (see our reference before Lemma 4). The mapping $\tau\chi$ is the desired isomorphism. ∎

For related results on more general partially exchangeable arrays see [13].

A random array $\zeta = (\zeta_{i,j};\ i,j \geqslant 1)$ is *separately exchangeable* (some authors prefer row-column exchangeable, RCE) if $\zeta \stackrel{d}{=} (\zeta_{\pi(i),\tau(j)};\ i,j \geqslant 1)$ for any permutations π and τ of positive integers. In similar situations one usually assumes that the permutations move only finite number of points but it is unnecessary, see [21, 14]. An array is *(separately) dissociated* if $(\zeta_{i,j};\ i \leqslant n, j \leqslant m)$ is independent of $(\zeta_{i,j};\ i > n, j > m)$ for all positive n and m. In the separately exchangeable arrays this is the same as the joint dissociatedness. A rectangular matrix $A = (a_{i,j}; i \leqslant n, j \leqslant m)$ is said to be *separately reducible* if it has two identical rows or two identical columns. Whenever ξ and η are two independent Bernoulli shifts ruled by probabilities $p_1, \dots, p_n$ and $q_1, \dots, q_m$, respectively, the random field $A_{\xi,\eta} = (a_{\xi_i,\eta_j};\ i,j \geqslant 1)$ is evidently RCE, dissociated and its subfields $(a_{\xi_i,\eta_j};\ i \leqslant k, j \leqslant l)$ are separately reducible a.s. for $k > n$ or $l > m$. By our methods one can work out also the version of Theorem 1 for separately exchangeable arrays.

Theorem 2. *A random array ζ is equidistributed with the field $A_{\xi,\eta}$ originating from a rectangular matrix A and two independent Bernoulli shifts ξ and η if and only if ζ is separately exchangeable, dissociated and the subarrays $(\zeta_{i,j};\ i \leqslant k,\ j \leqslant l)$ are separately reducible a.s. for all sufficiently large k or l.*

7. BIBLIOGRAPHY

[1] Aldous D.J. (1981) Representations for partially exchangeable arrays of random variables. *J. Multivariate Anal.* **11**, 581–598.

[2] Aldous D.J. (1982) On exchangeability and conditional independence. In: Koch G. and Spizzichino F. (eds.), *Exchangeability in Probability and Statistics,* North-Holland, Amsterdam, 165–170.

[3] Aldous D.J. (1985) Exchangeability and related topics. In: Hennequin P.L. (ed.), *École d'Été de Probabilité de Saint-Flour XIII-1983, Lecture Notes in Math.*, Springer-Verlag, Berlin, **1117**, 1–198.

[4] Cox D., Little J. and O'Shea D. (1997) *Ideals, Varieties, and Algorithms.* Springer-Verlag, New York, Berlin, Heidelberg.

[5] Dawid A.P. (1977) Spherical matrix distributions and a multivariate model. *J. R. Statist. Soc. Series B* **39**, 254–261.

[6] Dawid A.P. (1978) Extendibility of spherical matrix distributions. *J. Multivariate Anal.* **8**, 559–566.

[7] Diaconis P.W. and Freedman D.A. (1980) Finite exchangeable sequences *Ann. Probab.* **8**, 745–764.

[8] Diaconis P.W. and Freedman D.A. (1981) On the statistics of vision: the Julesz conjecture *J. Math. Psychology* **24**, 112–138.

[9] Hoover D.N. (1979) Relations on probability spaces and arrays of random variables. Institute of Advanced Study, Princeton (preprint).

[10] Hoover D.N. (1982) Row-column exchangeability and a generalized model for probability. In: Koch G. and Spizzichino F. (eds.), *Exchangeability in Probability and Statistics,* North-Holland, Amsterdam, 281–291.

[11] Hoover D.N. (1989) Tail fields of partially exchangeable arrays. *J. Multivariate Anal.* **31**, 160–163.

[12] Kallenberg O. (1988) Some new representations in bivariate exchangeability. *Probab. Th. Rel. Fields* **77**, 415–455.

[13] Kallenberg O. (1989) On the representation theorem for exchangeable arrays. *J. Multivariate Anal.* **30**, 137–154.

[14] Kallenberg O. (1993) Symmetries on random arrays and set-indexed processes. *J. Theor. Probab.* **6**, 727–765.

[15] Lynch J. (1984) Canonical row-column-exchangeable arrays. *J. Multivariate Anal.* **15**, 135–140.

[16] Mac Lane S. (1971) *Categories for the Working Mathematician.* Springer-Verlag, New York, Heidelberg, Berlin.

[17] Matúš F. (1994) On nonnegativity of symmetric polynomials. *The American Math. Monthly* **101**, 661–664.

[18] Matúš F. (1995) Finite partially exchangeable arrays. Institute of Information Theory and Automation, Prague (Research Report 1856).

[19] Matúš F. (1996) On two-block-factor sequences and one-dependence. *Proceedings of AMS* **14**, 1237–1242.

[20] Ressel P. (1985) De Finetti-type theorems: an analytical approach. *Ann. Probab.* **13**, 898–922.

[21] Ryll-Nardzewski C. (1957) On stationary sequences of random variables and the de Finetti's equivalence. *Colloq. Math.* **4**, 149–156.