

A CLASS OF FINITARY CODES

BY

M. KEANE AND M. SMORODINSKY

ABSTRACT

It is shown that for any two Bernoulli schemes with a finite number of states and unequal entropies, there exists a finitary homomorphism from the scheme with larger entropy to the one with smaller entropy.

§1. Introduction

In recent work on the classification of dynamical systems in ergodic theory, the construction of codes has played an important role. The reason for this is that every ergodic dynamical system (on a Lebesgue space) has a representation as a shift transformation on a sequence space whose underlying alphabet is finite or countable, and hence it has become important to construct codes (i.e. shift invariant and measure preserving maps) from one sequence space to another.

In the important special case of Bernoulli schemes, the efforts culminated in a complete classification by Ornstein [5]. His methods are in fact more general and apply to a much wider class of sequence spaces, but they have the disadvantage of not having a continuity property which would seem to be necessary for applications. Moreover, Ornstein has shown in a yet unpublished result (see also [7]) that the desired continuity property cannot be true for the wider class of sequence spaces.

The continuity property in question can be briefly described as follows. Any sequence space over a finite or countable number of symbols is endowed with a natural product topology. A code from one sequence space to another is called *finitary* or *almost continuous* if after removing sets of measure zero from the spaces, the code is continuous on the remaining sets. This definition is of course valid for any spaces, but takes a special equivalent form in the case of sequence

spaces whose exact definition is given in §2. Loosely speaking, finitary codes between sequence spaces are those for which a finite number of image coordinates can be decided by looking at only a finite, but possibly larger, number of original coordinates. For further discussion of this concept see [2].

The special examples of codings between Bernoulli schemes given by Meshalkin [3] and Blum-Hanson [1] enjoyed the property of being finitary. More recently, Monroy-Russo [4] have constructed finitary isomorphisms between special Markov chains and Bernoulli shifts. In this paper we show how to construct finitary codes from any Bernoulli scheme to any other Bernoulli scheme of lower entropy. Our construction is based on an idea of Monroy and Russo. It differs from the Meshalkin and Blum-Hanson codes (see [9]) in that the average number of coordinates needed to decide one coordinate in the image point is *finite*, and this means that our process can be effectively carried out (e.g. by a computer).

A special case of this result is the following. Consider a three-sided coin with equal probabilities, and produce using this coin a sequence of independent trials at times $t \in \mathbf{Z}$. This yields, say, a sequence of symbols 0, 1, 2. Now unless we were very unlucky (with probability one) the procedure defined below can be applied to the 0, 1, 2 sequence to write down a sequence on two symbols a, b which is typical sequence for the flipping of a two-sided coin with equal probabilities (or with any preassigned probabilities, the procedure of course depending on the probabilities desired). The point is that we can determine individual elements of the a, b sequence by looking at a finite number of elements of the 0, 1, 2 sequence, so that the whole sequences need not be known in order to effect the mapping step by step, and also that on the average the number of elements we need to know in the first sequence to determine one element in the second one is finite.

Let us now try to describe briefly the procedure which will be used. The first step consists of reducing the problem to the case where there exist two blocks (finite sequences) of the same length and same frequency of appearance, one in each scheme. These blocks are called markers. The code will have the property that the appearances of markers in a point and in its image coincide. The rest of the construction is then concerned with what happens with blocks occurring between two marker blocks. Here it is necessary to define a procedure independent of the indices of the point, since the code must commute with the shift. If M denotes a marker, then we define a skeleton as a sequence of the form

$$M^{n_0} \text{ ——— } M^{n_1} \text{ ——— } \dots \text{ ——— } M^{n_{m-1}} \text{ ——— } M^{n_m}$$

where $M^n = M \cdots M$ (n times), --- denotes "holes" of fixed positive lengths (where the block M is not supposed to appear) and $n_t < \min(n_0, m_m)$ for $1 \leq t \leq m - 1$. It is shown that for almost all points of the first scheme there exists a sequence of increasing skeletons whose lengths tend to infinity which "appear" in the points and cover every coordinate eventually. Given a skeleton, there are many possibilities to fill in the holes to obtain blocks occurring in the schemes. Each of these possibilities is called a filler. Using a marriage lemma which we prove in §3, we construct in §4 by an inductive procedure, partial mappings from the set of fillers for a given skeleton in the larger entropy scheme to the set of fillers for the same skeleton in the smaller entropy scheme. These mappings are called partial assignments; the idea is that whenever we see a skeleton in a point of the first scheme filled with a filler which is assigned to some filler in the second scheme, then this defines the image of the point in the coordinates covered by the skeleton. A compatibility condition ensures us that the definition is not changed at some later stage of the construction. In the final paragraph, we then formally define the code and prove that it is a finitary code.

The use of the marriage lemma in §4 to construct assignments is not necessary. We could have defined an assignment as a matrix α satisfying the conditions 1), 3) and 4) of Corollary 8 and obtained the estimate of Lemma 14 in a more direct, although somewhat less obvious, manner. In fact, our first proof of the theorem was constructed along these lines. Here we have used the marriage lemma because it gives a somewhat better estimate with less difficulty in the case where all the elements of $\bar{\mathcal{F}}(s)$ are good, and also because we think it is new and may be of independent interest.

§2. Markers

We begin by defining the notations we shall use for Bernoulli schemes. Then we state the main theorem of this paper and effect a reduction of the problem. Finally we study markers and define the marker process, and make the relation between the marker process and the Bernoulli schemes explicit.

Let

$$A = \{1, 2, \dots, a\}$$

be a finite alphabet, $a \geq 2$, and let

$$p = (p_1, \dots, p_a)$$

be a probability vector with $p_t \geq 0$ for $1 \leq t \leq a$. The *Bernoulli scheme* $B(p) = (X, \mathcal{A}, \mu, T)$ is defined by

$$\begin{aligned}
 X &= A^{\mathbb{Z}} \\
 \mathcal{A} &= \text{product } \sigma\text{-algebra on } X \\
 \mu &= p^{\mathbb{Z}} \\
 T &= \text{left shift on } X.
 \end{aligned}$$

Its entropy is given by

$$h = - \sum_{i=1}^a p_i \log p_i ;$$

all logarithms will be taken to the base 2. If $x \in X$ and if $q \leq r$ are integers, then we set

$$x[q, r] = x_q x_{q+1} \cdots x_r \in A^{r-q+1}.$$

A second Bernoulli scheme with alphabet $\bar{A} = \{1, \dots, \bar{a}\}$, probability vector \bar{p} and entropy \bar{h} is denoted by $B(\bar{p}) = (\bar{X}, \bar{\mathcal{A}}, \bar{\mu}, \bar{T})$.

A homomorphism ϕ from $B(p)$ to $B(\bar{p})$ is a measurable map ϕ from a subset of measure one of X to \bar{X} which takes μ to $\bar{\mu}$ and commutes with T and \bar{T} . The homomorphism ϕ is finitary if for almost every $x \in X$ there exist integers $q \leq r$ such that if $y \in X$ with $x[q, r] = y[q, r]$ and if $\phi(y)$ is defined, then $\phi(x)[0, 0] = \phi(y)[0, 0]$.

Our main result is the following theorem.

THEOREM 1. *If $\bar{h} < h$, then there exists a finitary homomorphism from $B(p)$ to $B(\bar{p})$.*

The following simple reduction of the problem permits us to introduce markers and starts the proof, which will continue throughout the paper.

LEMMA 2. *Let k_0 be any positive integer, and let $\bar{h} < h$. Suppose that Theorem 1 is true under the following additional hypothesis: there exists an integer $k \geq k_0$ such that*

$$p_1^{k-1} p_2 = \bar{p}_1^{k-1} \bar{p}_2.$$

Then Theorem 1 is true.

PROOF. Since $\bar{h} < h$, one of the elements of \bar{p} is larger than one of the elements of p , so that by rearranging we may assume $p_1 < \bar{p}_1$. Consider the Bernoulli scheme $B(p)$ based on the alphabet $\bar{A} = \{1, 2, \dots, \bar{a} + 1\}$ and the probability vector $\bar{p} = (\bar{p}_1, \dots, \bar{p}_{\bar{a}+1})$, where

$$\begin{aligned} \tilde{p}_1 &= \bar{p}_1 \\ \tilde{p}_2 &= \delta \\ \tilde{p}_3 &= \bar{p}_2 - \delta \\ \tilde{p}_t &= \bar{p}_{t-1} \text{ for } 4 \leq t \leq \bar{a} + 1, \end{aligned}$$

with $0 < \delta < \bar{p}_2$. There exists a finitary homomorphism from $B(\tilde{p})$ to $B(\bar{p})$, obtained by identifying the symbols 2 and 3 of \tilde{A} . If δ is small enough, we have

$$\bar{h} < \tilde{h} < h,$$

where \tilde{h} is the entropy of $B(\tilde{p})$. Moreover, for any $k \geq k_0$ there is a value of δ for which

$$p_1^{k-1} p_2 = \tilde{p}_1^{k-1} \tilde{p}_2,$$

namely

$$\delta = p_2 \cdot \left(\frac{p_1}{\bar{p}_1}\right)^{k-1}.$$

Because $p_1 < \bar{p}_1$, δ tends to zero as k tends to infinity. Now choose $k \geq k_0$ and $\delta = \delta(k)$ such that $\delta < \bar{p}_2$ and $\tilde{h} < h$. Then the additional hypothesis holds for $B(p)$ and $B(\tilde{p})$, and composing the finitary homomorphism from $B(p)$ to $B(\tilde{p})$ with the one from $B(\tilde{p})$ to $B(\bar{p})$, we obtain the desired result.

Now we fix the integer k for the rest of our argument, and we assume in the following that

$$p_1^{k-1} p_2 = \bar{p}_1^{k-1} \bar{p}_2.$$

A *marker* (for either scheme) is the block

$$M = 1^{k-1} 2 = \underbrace{1 \cdots 1}_{k-1 \text{ times}} 2.$$

In general, if $y = y_1 \cdots y_r \in A^r$, then we set

$$\mu(y) = \prod_{i=1}^r p_{y_i},$$

and similarly we extend $\bar{\mu}$ to finite sequences. The *marker measure* η is then given by

$$\eta = \mu(M) = \bar{\mu}(M) = p_1^{k-1} p_2 = \bar{p}_1^{k-1} \bar{p}_2.$$

Consider the sequence space X defined by

$$\hat{X} = \{\hat{1}, \hat{2}\}^{\mathbb{Z}}.$$

Define a map from X to \hat{X} by the following procedure. Take a point $x \in X$ and replace all markers M occurring in x by $\hat{1} \hat{1} \cdots \hat{1}$ (k times). Then replace all other symbols in x by $\hat{2}$. This map commutes with the shift and sends the measure μ to a measure $\hat{\mu}$ on \hat{X} . We call $(\hat{X}, \hat{\mu})$ the *marker process* of $B(p)$. Similarly we can define the marker process of $B(\bar{p})$.

LEMMA 3. *The marker processes of $B(p)$ and $B(\bar{p})$ coincide.*

PROOF. First consider the marker process of $B(p)$. For almost all $\hat{x} \in \hat{X}$ (w.r.t. $\hat{\mu}$), \hat{x} contains infinitely many $\hat{1}$, and the $\hat{1}$ in \hat{x} appear in groups whose length is a multiple of k . This is true since markers in a point $x \in X$ appear infinitely often (a.e.) and cannot overlap. Now consider a block of the form

$$\hat{y} = \hat{1}^{m_0 k} \hat{2}^{l_1} \hat{1}^{m_1 k} \hat{2}^{l_2} \cdots \hat{1}^{m_{r-1} k} \hat{2}^{l_r} \hat{1}^{m_r k},$$

where $t \geq 1$, $l_i \geq 1$, $m_i \geq 1$ ($0 \leq i \leq t$). Let $q < r$ be integers with $r - q + 1 = \Sigma(l_i + m_i k)$, and consider the cylinder set

$$\hat{Z} = \{\hat{x} \in \hat{X} : \hat{x}[q, r] = \hat{y}\}$$

and its inverse image

$$Z = \{x \in X : \hat{x} \in \hat{Z}\}$$

in X . We wish to calculate $\hat{\mu}$ for each such cylinder \hat{Z} . For $l \geq 1$ denote by A_0^l the set of blocks of length l over the alphabet A which contain no markers. Then

$$Z = \{x \in X : x[q, r] \in M^{m_0} \times A_0^{l_1} \times M^{m_1} \times \cdots \times A_0^{l_r} \times M^{m_r}\}$$

and

$$\hat{\mu}(\hat{Z}) = \mu(Z) = \eta^{m_0 + \cdots + m_r} \cdot \prod_{i=1}^r \mu(A_0^{l_i}).$$

The same calculation is valid for the marker process for $B(\bar{p})$, and $\hat{\mu}$ is certainly determined by $\hat{\mu}(\hat{Z})$ for all cylinders \hat{Z} of the above type. Thus it is sufficient for the proof of the lemma to show that for each $l \geq 1$, $\mu(A_0^l)$ depends only on l and η , and not otherwise on p_1, \dots, p_a .

Now consider the finite space A^l provided with the measure μ , and let E_t denote the event that a marker occurs at place t , $1 \leq t \leq l - k + 1$. Then

$$\mu(A_0^l) = 1 - \mu\left(\bigcup_{t=1}^{l-k+1} E_t\right) = 1 - \sum_t \mu(E_t) + \sum_{t,t'} \mu(E_t \cap E_{t'}) - \cdots.$$

If $E_t \cap E_{t'} \neq \emptyset$, then $|t - t'| \geq k$ since markers cannot overlap. Therefore

$$\mu(E_{t_1} \cdots E_{t_n}) = \begin{cases} 0 & \text{if there exist } v, w \text{ with } |t_v - t_w| < k \\ \prod_{v=1}^n \mu(E_{t_v}) & \text{otherwise,} \end{cases}$$

and the last product is just η^n . It follows that $\mu(A_0^l)$ can be written as a polynomial in η whose coefficients depend only on l and k , and the lemma is proved.

The notation $A_0^l(\bar{A}_0^l)$ will be used in the following for the set of sequences of length l over $A(\bar{A})$ which contain no markers. We also use repeatedly the formula

$$\mu(A_0^l) = \bar{\mu}(\bar{A}_0^l).$$

Consider now the projection $\pi : X \rightarrow \hat{X}$ from $B(p)$ to the marker process $(\hat{X}, \hat{\mu})$. For each $\hat{x} \in \hat{X}$ let

$$X(\hat{x}) = \pi^{-1}(\hat{x})$$

denote the fiber of X above \hat{x} . Almost all $\hat{x} \in \hat{X}$ have the following form:

$$\hat{x} = (\dots \hat{1}^{m_{-1}k} \hat{2}^b \hat{1}^{m_0k} \hat{2}^l \dots),$$

where $\{m_i\}$ and $\{l_i\}$ are sequences of positive integers. In this case, we identify the fiber above \hat{x} by setting

$$X(\hat{x}) = \prod_{i \in \mathbb{Z}} A_0^l.$$

Denote for any $l \geq 1$ the normalization of the measure μ on A_0^l by μ_0 . That is,

$$\mu_0(F) = \frac{\mu(F)}{\sum_{G \in A_0^l} \mu(G)} = \frac{\mu(F)}{\mu(A_0^l)} \quad (F \in A_0^l).$$

(Elements F of A_0^l will later be called *fillers*.) By taking the product measure of the μ_0 on the A_0^l , $t \in \mathbb{Z}$, we obtain a normalized measure μ_x on almost all fibers $X(\hat{x})$. The next lemma shows that the μ_x are actually the conditional probabilities of μ on the fibers $X(\hat{x})$.

LEMMA 4. For every non-negative measurable function ψ on X ,

$$\int_X \psi d\mu = \int_{\hat{X}} \left(\int_{X(\hat{x})} \psi d\mu_x \right) d\hat{\mu}(\hat{x}).$$

PROOF. Let $y \in A^n$ be of the form

$$y = M^{m_0} F_1 M^{m_1} F_2 \cdots M^{m_{t-1}} F_t M^{m_t},$$

where $F_i \in A_0^{l_i}$ for $1 \leq i \leq t$, and the m_i and l_i are positive integers. Let $q \leq r$ such that $r - q + 1 = \sum l_i + m_i k$, and set

$$Z = \{x \in X : x[q, r] = y\}.$$

It is sufficient to prove the lemma for $\psi = 1_Z$ for any such Z . Now if $Z \cap X(\hat{x}) \neq \emptyset$, then

$$\mu_{\hat{x}}(Z) = \mu_{\hat{x}}(Z \cap X(\hat{x})) = \prod_{i=1}^t \mu_0(F_i).$$

This is the same number for all such x . Moreover,

$$\hat{\mu}(\{\hat{x} \in \hat{X} : Z \cap X(\hat{x}) \neq \emptyset\}) = \eta^{m_0 + \dots + m_t} \prod_{i=1}^t \mu(A_0^{l_i})$$

and hence

$$\int_{\hat{X}} \left(\int_{X(\hat{x})} 1_Z d\mu_{\hat{x}} \right) d\hat{\mu}(\hat{x}) = \eta^{m_0 + \dots + m_t} \prod_{i=1}^t \mu(F_i) = \mu(Z)$$

as required.

For any $x \in X$ which belongs to a fiber

$$X(\hat{x}) = \prod_{i \in \mathbb{Z}} A_0^{l_i},$$

denote by $F_t(x) \in A_0^{l_t}$, $t \in \mathbb{Z}$, the sequence of elements of $A_0^{l_t}$ which determine x . To fix our notation, let us require that the 0-th coordinate of x belong either to an index of $A_0^{l_0}$ or to the marker string which immediately precedes $A_0^{l_0}$. We shall need the following version of the Shannon–McMillan–Breiman Theorem.

LEMMA 5. For almost all $x \in X$,

$$\lim_{t \rightarrow \infty} \frac{1}{\sum_{i=-t}^t l_i(x)} \log \prod_{i=-t}^t \mu_0(F_i(x)) = \frac{1}{1 - k\eta} (h - e),$$

where e denotes the entropy of the marker process.

PROOF. Let $x \in X$ be such that the Shannon–McMillan–Breiman Theorem [6] holds for x and for $\hat{x} = \pi(x) \in \hat{X}$. This is true for almost all $x \in X$. Then as $q \rightarrow -\infty$ and $r \rightarrow +\infty$,

$$\frac{1}{r - q} \log \mu (x[q, r]) \rightarrow -h,$$

$$\frac{1}{r - q} \log \hat{\mu} (\{\hat{y} \in \hat{X} : \hat{y}[q, r] = \hat{x}[q, r]\}) \rightarrow -e,$$

$$\frac{\sum_{i=-l}^l l_i}{r - q} \rightarrow 1 - k\eta,$$

where in the last limit we have supposed the sequence (q, r) “compatible” with the marker structure. The last limit is valid by applying the ergodic theorem to the characteristic function of the marker block in X . Since for (q, r) “compatible”,

$$\frac{\mu(x[q, r])}{\hat{\mu}(\{\hat{y} : \hat{y}[q, r] = \hat{x}[q, r]\})} = \prod_{i=-l}^l \mu_o(F_i(x)),$$

the lemma is proved.

The above results are all valid also for $B(\bar{p})$, and we shall use them as well as the notation freely in the sequel. We set

$$g = \frac{1}{1 - k\eta} (h - e)$$

and

$$\bar{g} = \frac{1}{1 - k\eta} (\bar{h} - e).$$

The quantities g and \bar{g} are called the *filler entropies* of the schemes $B(p)$ and $B(\bar{p})$.

§3. A marriage lemma

We digress for a moment to prove a lemma which will be useful for our construction in §4. Some parts of the following proof are known (e.g. [8]), but we insert everything for completeness.

Let (U, ρ) and (V, σ) be two finite measure spaces. We also assume that $U = \{1, 2, \dots, u\}$ is a finite set, the set of *boys*, V is called the set of *girls* and is not necessarily finite.

A *society* S is a map which assigns to each $b \in U$ a measurable set $S(b) \subset V$ such that for all subsets B of U ,

$$\rho(B) \leq \sigma(S(B)),$$

where we have set $S(B) = \bigcup_{b \in B} S(b)$.

We say that the society R is *less promiscuous* than the society S iff $R(b) \subset S(b)$ for all $b \in U$.

LEMMA 6. *Let S be a society. Suppose that there exist measurable disjoint subsets G_1 and G_2 of V and distinct elements $b_1, b_2 \in U$ with the following properties:*

$$G_1 \cup G_2 \subset S(b_1) \cap S(b_2).$$

For $i = 1$ or $i = 2$, denote by S_i the map obtained by setting

$$S_i(b) = S(b) \quad (b \neq b_i),$$

$$S_i(b_i) = S(b_i) \setminus G_i.$$

Then either S_1 or S_2 is a society.

PROOF. Assume that S_1 is not a society. Then there exists $B_1 \subset U$ such that

$$\rho(B_1) > \sigma(S_1(B_1)).$$

Obviously $b_1 \in B_1$ and $b_2 \notin B_1$, since otherwise we would have $S_1(B_1) = S(B_1)$. Let B be any subset of U . We show that

$$\rho(B) \leq \sigma(S_2(B)).$$

If $b_2 \notin B$ or if $b_1 \in B$ this relation follows because then $S_2(B) = S(B)$. Suppose $b_1 \notin B \ni b_2$. Then

$$S(B \cup B_1) = S_1(B_1) \cup S_2(B) = S_1(B_1) \cup [S_2(B \setminus B_1) \setminus S_1(B \cap B_1)]$$

and

$$B_1 \cup B = B_1 \cup (B \setminus B_1).$$

Since S is a society, we have that

$$\rho(B_1) + \rho(B \setminus B_1) \leq \sigma(S_1(B_1)) + \sigma(S_2(B \setminus B_1) \setminus S_1(B \cap B_1)),$$

and since B_1 violates S_1 it follows that

$$\rho(B \setminus B_1) < \sigma(S_2(B \setminus B_1) \setminus S_1(B \cap B_1)).$$

Moreover $B \cap B_1$ contains neither b_1 nor b_2 . Therefore

$$S(B \cap B_1) = S_1(B \cap B_1) = S_2(B \cap B_1)$$

and

$$\rho(B \cap B_1) \leq \sigma(S_1(B \cap B_1)).$$

Adding the last two inequalities yields

$$\begin{aligned} \rho(B) &= \rho(B \setminus B_1) + \rho(B \cap B_1) \leq \sigma(S_2(B \setminus B_1) \setminus S_1(B \setminus B_1)) + \sigma(S_1(B \cap B_1)) \\ &= \sigma(S_2(B \setminus B_1) \cup S_1(B \cap B_1)) \\ &= \sigma(S_2(B)) \end{aligned}$$

and the lemma is proved.

COROLLARY 7. *If (V, σ) is a continuous measure space, and if S is a society, then there exists a society R less promiscuous than S such that $R(b_1) \cap R(b_2) = \emptyset$ if $b_1 \neq b_2$.*

PROOF. It is obviously sufficient to attain $\sigma(R(b_1) \cap R(b_2)) = 0$ for $b_1 \neq b_2$, since removing a set of measure 0 does not change the society property. By Lemma 6, if $\sigma(R(b_1) \cap R(b_2)) = \delta > 0$, then we can reduce the measure of the intersection to $\delta/2$, since (V, σ) is continuous. Iterating this procedure yields the desired result.

COROLLARY 8. *Suppose now that $V = \{1, \dots, v\}$ is finite. Given a society S , there exists a matrix $\alpha(b, g)$ ($b \in U$ and $g \in V$) such that:*

- 1) $\alpha(b, g) \geq 0$ for all $b \in U$ and $g \in V$,
- 2) $\alpha(b, g) = 0$ if $g \notin S(b)$,
- 3) $\sum_{g \in V} \alpha(b, g) = \rho(b)$ for all $b \in U$,
- 4) $\sum_{b \in U} \alpha(b, g) \leq \sigma(g)$ for all $g \in V$.

PROOF. Let \tilde{V} be a continuous measure space with disjoint subsets $\{V_1, \dots, V_v\}$ and measure $\tilde{\sigma}$ such that $V = \bigcup_{i=1}^v V_i$ and such that $\tilde{\sigma}(V_i) = \tilde{\sigma}(i)$, $i \in V$. Define the continuous analog \tilde{S} of S on \tilde{V} by setting

$$\tilde{S}(b) = \bigcup_{g \in S(b)} V_g \quad (b \in U).$$

By Corollary 7 there exist disjoint subsets $R(b) \subset \tilde{S}(b)$, $b \in U$ which form a society. We may assume that $e(b) = \tilde{\sigma}(R(b))$ for each $b \in U$, simply by making $R(b)$ smaller if necessary. Now set

$$\alpha(b, g) = \tilde{\sigma}(R(b) \cap V_g).$$

The four conditions above are easily seen to be true for this α , and we leave the details to the reader.

LEMMA 9. *Let V be finite. Suppose that $\alpha(b, g)$ ($b \in U$ and $g \in V$) is a matrix satisfying conditions 1), 3) and 4) above. Define for each $b \in U$*

$$S(b) = \{g \in V : \alpha(b, g) > 0\}.$$

Then S is a society.

PROOF. Let B be any subset of U . Then

$$\begin{aligned} \rho(B) &= \sum_{b \in B} \rho(b) = \sum_{b \in B} \sum_{g \in V} \alpha(b, g) = \sum_{b \in B} \sum_{g \in S(b)} \alpha(b, g) \\ &\leq \sum_{g \in S(B)} \sum_{b \in U} \alpha(b, g) \leq \sum_{g \in S(B)} \sigma(g) = \sigma(S(B)). \end{aligned}$$

COROLLARY 10. *If S is as in Corollary 8 and if there exists a pair (b, g) with $g \in S(b)$ and $\alpha(b, g) = 0$, then the map obtained by deleting g from $S(b)$ is still a society.*

Now we come to the main result of this paragraph. If S is a society and if V is finite, we set

$$\pi(S) = \text{card}\{g \in V : b_1 \neq b_2 \text{ with } g \in S(b_1) \cap S(b_2)\}.$$

The number $\pi(S)$ is called the *promiscuity number* of the society S .

THEOREM 11. *Let V be a finite set. To every society R there exists a less promiscuous society S such that $\pi(S) \leq u - 1$, where $u = \text{card}(U)$.*

PROOF. Since there are only finitely many societies, we may choose a society S less promiscuous than R which is minimal w.r.t. this property. That is, no other society is less promiscuous than S . Let S be any such society.

A *cycle* is a sequence b_1, \dots, b_t of different boys in U ($t \geq 2$) together with girls g_1, \dots, g_t , who are all different, such that for each $1 \leq i \leq t$,

$$g_i \in S(b_i) \cap S(b_{i+1})$$

(where we have set $b_{t+1} = b_1$). We show that S has no cycles. Note that Lemma 6 says for finite V that S has no cycles of length $t = 2$.

Suppose there is a cycle as above. Let α be a matrix for S as in Corollary 8. Define a matrix α' by setting

$$\alpha'(b_i, g_i) = \alpha(b_i, g_i) - \epsilon \quad (1 \leq i \leq t)$$

$$\alpha'(b_{i+1}, g_i) = \alpha(b_{i+1}, g_i) + \epsilon$$

and

$$\alpha'(b, g) = \alpha(b, g) \text{ for all other } (b, g).$$

Now set $\varepsilon = \min_{1 \leq i \leq r} \alpha(b_i, g_i)$. It is easy to check that α' satisfies conditions 1)–4) of Corollary 8. Moreover $\alpha'(b_i, g_i) = 0$ for at least one value of i . This is a contradiction to the minimality of S by Corollary 10.

Next we may consider a graph whose vertices are the elements of U and whose edges are the pairs (b, b') for which $S(b) \cap S(b') \neq \emptyset$. By the above, this graph has no cycles and is therefore a tree, with at most $u - 1$ edges. But the number of edges is equal to the promiscuity number $\pi(S)$.

Finally, we note that if S_i is a society on (U_i, e_i) and (V_i, σ_i) , $i = 1, 2$, then the product $S_1 \times S_2$ is a society on $(U_1 \times U_2, e_1 \times e_2)$ and $(V_1 \times V_2, \sigma_1 \times \sigma_2)$, where

$$S_1 \times S_2(b_1 \times b_2) = S_1(b_1) \times S_2(b_2).$$

This follows from Corollary 8 and Lemma 9, by setting

$$\alpha(b_1 \times b_2, g_1 \times g_2) = \alpha_1(b_1, g_1) \cdot \alpha_2(b_2, g_2)$$

and by noting that the society S of Lemma 9 is less promiscuous than $S_1 \times S_2$, so that $S_1 \times S_2$ must be a society.

§4. Skeletons, fillers and assignments

In the construction of the homomorphism of Theorem 1 which we produce in the next paragraph, fibers $X(\hat{x})$ will be mapped to fibers $\bar{X}(\hat{x})$ in the barred scheme for almost all $\hat{x} \in \hat{X}$. The purpose of this paragraph is to prepare the definition of the map on each fiber in a way which is shift invariant.

By a skeleton we mean a non-indexed finite sequence of M 's and blanks (of different positive lengths) of the following form:

$$M^{n_0} \text{---}_{l_1} M^{n_1} \text{---}_{l_2} \dots M^{n_{m-1}} \text{---}_{l_m} M^{n_m}$$

where $m \geq 1$, $n_t \geq 1$ ($0 \leq t \leq m$), $l_t \geq 1$ ($1 \leq t \leq m$), and where

$$n_t < \min(n_0, n_m) \quad (1 \leq t \leq m - 1).$$

The numbers l_1, \dots, l_m are called the filler lengths of the skeleton. We set

$$l = l_1 + \dots + l_m.$$

Skeletons will be denoted by the symbol s , and the set of skeletons by \mathcal{S} .

If $s, s' \in \mathcal{S}$, then s' is a *subskeleton* of s if (in the above notation for s) there exist integers t and t' such that

$$s' = M^{n_1} \text{---}_{l_1} M^{n_2} \text{---}_{l_2} \dots \text{---}_{l_r} M^{n_r}.$$

Two subskeletons are said to be disjoint (in s) if the indices of the l 's corresponding to them are disjoint. Since the requirement for skeletons specifies that the marker sequences M^{n_0} and M^{n_m} at the ends are longer than those in the middle, it follows that if s' and s'' are subskeletons of s , either s' and s'' are disjoint or one of them contains the other as a subskeleton.

A *maximal* subskeleton s' of s is a skeleton $s' \neq s$ such that it is contained in no other subskeleton $s'' \neq s$. From the above it follows that either s contains no maximal subskeletons or that the maximal subskeletons s_1, \dots, s_j of s are disjoint and cover s .

We define the *order* of skeletons inductively in the following manner. A *one-skeleton* (skeleton of order 1) is a skeleton with no maximal subskeletons. These are just all skeletons of the form

$$M^{n_0} \text{---} M^{n_1}$$

with $n_0, n_1 \geq 1$. If $n \geq 2$, an *n-skeleton* (skeleton of order m) is a skeleton which is not of order less than n , but all of whose subskeletons $s' \neq s$ have order less than n . If s is a skeleton, then by breaking up s into maximal disjoint subskeletons, breaking these each up again, etc., it is easy to see that the order of s is well-defined. We omit these details.

If $s \in \mathcal{S}$ and $x \in X$, we say that s occurs in x at (q, r) if (denoting by \hat{x} the image of x in the marker process) $\hat{x}[q, r]$ can be obtained from s by replacing each M by $\hat{1}^k$ and each blank of length l by $\hat{2}^l$, and if $x[q, r]$ is neither immediately preceded nor immediately followed by the symbol $\hat{1}$ in \hat{x} . We use a similar definition for the occurrence of a skeleton in a point of \bar{X} . The following lemma is obvious.

LEMMA 12. *For almost every $x \in X$ there exists a sequence of skeletons s_t , $t \geq 1$, and sequences of integers q_t and r_t such that*

- 1) $q_t \leq 0 \leq r_t$,
- 2) s_t occurs in x at (q_t, r_t) ,
- 3) $q_t \rightarrow -\infty$ and $r_t \rightarrow +\infty$.

PROOF. Let $x \in X$ be such that for each integer $u > 0$, the marker sequence M^u occurs at least once to the left of zero and to the right of zero and is neither preceded nor followed by M . This is obviously a set of measure one (by the ergodic theorem, for instance). Now we may take for s_1 the skeleton

M^{n_0} ——— M^{n_1} which occurs in x and contains the zero coordinate. To obtain s_2 , look to the left and to the right for the first occurrence of an M^n with $n > n_0$, $n > n_1$, etc.

If $x \in X$ satisfies Lemma 12, we may define the *sequence of skeletons* $s_t(x)$ of x as the maximal sequence such that $s_t(x)$ occurs in x at (q_t, r_t) and such that $s_t(x)$ is a (maximal) subskeleton of $s_{t+1}(x)$. To remove ambiguity at the beginning, we should not only assume that $q_t \leq 0 \leq r_t$, but also that the zero coordinate of x appears in the “interior” of the skeleton s_1 , i.e. it does not correspond to an element of one of the end marker sequences of s_1 . Then $s_t(x)$ is uniquely defined for almost all x . Moreover, the sequences $s_t(x)$ and $s_t(Tx)$ coincide for large t (after shifting indices if necessary), since $q_t \rightarrow -\infty$ and $r_t \rightarrow +\infty$.

The above results are also valid for the scheme $B(\bar{p})$. The sequence $s_t(x)$ obviously depends only on \hat{x} , and not on $x \in X(\hat{x})$.

Next we define fillers. Let s be a skeleton as above. A filler F for s is an element of the set

$$\mathcal{F}(s) = A_0^{l_1} \times \cdots \times A_0^{l_m}.$$

If $F = F_1 \times \cdots \times F_m$, then we set

$$\mu_0(F) = \prod_{i=1}^m \mu_0(F_i),$$

where μ_0 is the normalized measure on A_0^l ($l \geq 1$) defined in §2. We call this μ_0 the *filler measure* on $\mathcal{F}(s)$. $\bar{\mathcal{F}}(s)$ and $\bar{\mu}_0$ are defined similarly.

We shall need to distinguish between good (typical) fillers and bad fillers. The definition most convenient for our purpose is not the same for $B(p)$ and $B(\bar{p})$. If g and \bar{g} are the filler entropies for $B(p)$ and $B(\bar{p})$, then $\bar{h} < h$ implies $\bar{g} < g$. We fix an ε with $0 < \varepsilon < \frac{1}{3}(g - \bar{g})$.

An element

$$F = F_1 \times \cdots \times F_m \quad A_0^{l_1} \times \cdots \times A_0^{l_m}$$

is *good* if

$$\mu_0(F) \leq 2^{-(g-\varepsilon)l},$$

where $l = l_1 + \cdots + l_m$. An element

$$\bar{F} = \bar{F}_1 \times \cdots \times \bar{F}_m \quad \bar{A}_0^{l_1} \times \cdots \times \bar{A}_0^{l_m}$$

is *good* if

$$\bar{\mu}_0(\bar{F}) \geq 2^{-(\bar{g}+\varepsilon)l}.$$

Elements which are not good are said to be *bad*. We shall need to subdivide the bad elements of $\bar{\mathcal{F}}(s)$ a bit more. This is done by the following definition. If $\bar{F} \in \bar{\mathcal{F}}(s)$ and if s' is a subskeleton of s , then by restricting \bar{F} to s' we obtain an element of $\bar{\mathcal{F}}(s')$ which we shall denote by $\bar{F}(s')$. Now set

$$\mathcal{G}(\bar{F}, s) = \{s' : s' \text{ subskeleton of } s, \bar{F}(s') \text{ good, and } s' \text{ maximal w.r.t these properties}\}.$$

For instance, if \bar{F} was good to begin with, then $\mathcal{G}(\bar{F}, s) = \{s\}$. If $s', s'' \in \mathcal{G}(\bar{F}, s)$, then s' and s'' are disjoint, since if one were contained in the other then it wouldn't be maximal. We say that $\bar{F} \in \bar{\mathcal{F}}(s)$ and $\bar{G} \in \bar{\mathcal{F}}(s)$ are *equivalent* ($\bar{F} \sim \bar{G}$) iff

$$\mathcal{G}(\bar{F}, s) = \mathcal{G}(\bar{G}, s)$$

and

$$\bar{F}(s') = \bar{G}(s')$$

for all $s' \in \mathcal{G}(\bar{F}, s)$. If \bar{F} is good, then no other element is equivalent to it.

LEMMA 13. *Let s be a skeleton with filler lengths l_1, \dots, l_m . The number of equivalence classes in $\bar{\mathcal{F}}(s)$ is at most*

$$2^{m + (\bar{g} + \epsilon)l},$$

where $l = l_1 + \dots + l_m$.

PROOF. The number of possibilities for (\bar{F}, s) is at most 2^m , the number of subsets of $\{1, \dots, m\}$. If s' is any subskeleton of length l' , the number of good elements of $\bar{\mathcal{F}}(s')$ is at most

$$2^{(\bar{g} + \epsilon)l'},$$

since each one has measure at least $2^{-(\bar{g} + \epsilon)l'}$. Since the skeletons of (\bar{F}, s) are disjoint, the number of possibilities for $\bar{F}(s'), s' \in \mathcal{G}(\bar{F}, s), \bar{F}(s')$ good, is at most

$$\prod_{s' \in \mathcal{G}} 2^{(\bar{g} + \epsilon)l'} \leq 2^{(\bar{g} + \epsilon)l}.$$

Next we define partial assignments. Let s be any skeleton. A *partial assignment* P_s for s is a society (see §3) on the sets

$$U = \bar{\mathcal{F}}(s) \quad (\text{boys}), \quad \rho = \bar{\mu}_0$$

and

$$V = \mathcal{F}(s) \quad (\text{girls}), \quad \sigma = \mu_0.$$

The partial assignment P_s is good iff

$$\bar{F} \sim \bar{G} \Rightarrow P_s(\bar{F}) = P_s(\bar{G}).$$

Note that a good partial assignment is the same thing as a society with V as above and U the set of equivalence classes of $\bar{\mathcal{F}}(s)$, e being the measure $\bar{\mu}_0$ of each equivalence class.

LEMMA 14. *If Q_s is a good partial assignment for s , then there exists a good partial assignment P_s less promiscuous than Q_s , and such that*

$$\begin{aligned} &\mu_0(\{F \in \mathcal{F}(s): F \text{ belongs to more than one } P_s(\bar{F})\}) \leq \\ &2^{m - ((g - \bar{g})/3)l} + \mu_0(\{F \in \mathcal{F}(s): F \text{ bad}\}) + \bar{\mu}_0(\{\bar{F} \in \bar{\mathcal{F}}(s): \bar{F} \text{ bad}\}). \end{aligned}$$

PROOF. Applying Theorem 11 to Q_s with U equal to the set of equivalence classes of boys, we obtain a good partial assignment P_s such that the number of elements in the set on the left hand side of the inequality is at most

$$2^{m + (\bar{g} + \varepsilon)l},$$

if we discount the F belonging to only one equivalence class with more than one element. Since our measures are normalized, this latter set cannot have measure greater than

$$\bar{\mu}_0(\{\bar{F} \in \bar{\mathcal{F}}(s): \bar{F} \text{ bad}\});$$

otherwise this would violate the societal condition. Each of the $2^{m + (\bar{g} + \varepsilon)l}$ elements mentioned above is either good or bad (in (s)). Therefore their total measure is at most

$$2^{m + (\bar{g} + \varepsilon)l} \cdot 2^{-(g - \varepsilon)l} + \mu_0(\{F \in \mathcal{F}(s): F \text{ bad}\}).$$

Finally,

$$m + (\bar{g} + \varepsilon)l - (g - \varepsilon)l = m - (g - \bar{g} - 2\varepsilon)l \leq m - \left(\frac{g - \bar{g}}{3}\right)l$$

and the lemma is proved.

The last task of this paragraph is to define and construct global assignments. Let s be a skeleton, and suppose that the order of s is greater than one. Let s_1, \dots, s_j denote the maximal subskeletons of s . They are disjoint and cover s . Let P_1, \dots, P_j be partial assignments for s_1, \dots, s_j . We define the *product assignment* $P_s = P \times \dots \times P_j$ on s in the following manner. If $\bar{F} \in \bar{\mathcal{F}}(s)$, then $P(\bar{F})$ consists of all $F \in \mathcal{F}(s)$ such that for each $1 \leq i \leq j$, $F(s_i) \in P_i(\bar{F}(s_i))$. (Remember that $F(s_i)$ denotes the restriction of F to s_i .)

LEMMA 15. $P = P_1 \times \cdots \times P_j$ is a partial assignment on s . If P_1, \dots, P_j are good, then P is good.

PROOF. The first statement follows from the fact that the product of two societies is a society (see the remark at the end of §3). The second statement follows from the fact that if $\bar{F} = \bar{F}_1 \times \cdots \times \bar{F}_j$ and $\bar{G} = \bar{G}_1 \times \cdots \times \bar{G}_j$, then

$$\bar{F} \sim \bar{G}$$

implies

$$\bar{F}_t \sim \bar{G}_t \quad (1 \leq t \leq j).$$

A global assignment P is a collection $(P_s)_{s \in \mathcal{S}}$ of good partial assignments, one for each skeleton s , such that for any $s \in \mathcal{S}$ with maximal subskeletons s_1, \dots, s_j , P_s is less promiscuous than $P_{s_1} \times \cdots \times P_{s_j}$. The global assignment P is minimal if for each $s \in \mathcal{S}$, there is no other good assignment less promiscuous than P_s .

LEMMA 16. *Minimal global assignments exist.*

PROOF. For one-skeletons s , set $Q_s(\bar{F}) = \mathcal{F}(s)$ for all $\bar{F} \in \bar{\mathcal{F}}(s)$. Choose any P_s less promiscuous than Q_s which has the above minimality property.

If $P_{s'}$ has been defined for all skeletons s' of order less than n , and if s is an n -skeleton with maximal subskeletons s_1, \dots, s_j (of order less than n), then set

$$Q_s = P_1 \times \cdots \times P_j$$

and proceed as for one-skeletons. This defines P by induction and the lemma is proved.

Note that any minimal global assignment satisfies the inequality of Lemma 14.

§5. Proof of the main theorem

We can now prove Theorem 1. By Lemma 2 we may assume that $p_1^{k-1} p_2 = \bar{p}_1^{k-1} \bar{p}_2$ and we may choose k as large as we wish. Now as k tends to infinity, the average number of places in a point \hat{x} of \hat{X} occupied by the symbol $\hat{1}$ is $k\eta = kp_1^{k-1} p_2$ and this tends to zero. Thus the entropy e of the marker process also tends to zero, and the filler entropies g and \bar{g} approach the original entropies h and \bar{h} of the Bernoulli schemes. Moreover, if $\hat{x} \in \hat{X}$ corresponds to a fiber $X(\hat{x})$ of the form $\prod_{t \in \mathbb{Z}} A_0^t$, then for almost all \hat{x} the average length of the l_t , which is constant by the ergodic theorem for a fixed k , tends to infinity as k tends to infinity. For $x \in X$ let $s_t(x)$ be the sequence of skeletons defined after Lemma 12 corresponding to x , $t \geq 1$, and let $m_t(x)$ be the number of filler blocks

of $s_i(x)$, and $l_i(x)$ the total filler length of $s_i(x)$. By the above, we may choose k large enough such that for almost all $x \in X$,

$$\lim_{i \rightarrow \infty} m_i(x) - \left(\frac{g - \bar{g}}{3}\right) l_i(x) = -\infty.$$

(This is one of the uses of our hypothesis $h > \bar{h}$ with a strict inequality.) Choose and fix k such that this relation holds. This fixes also g and \bar{g} .

By Lemma 4, the formula of Lemma 5 holds a.e. on fibers $X(\hat{x})$ with respect to the fiber measure μ_x , at least for almost all fibers $X(\hat{x})$. It follows that for almost all $x \in X$,

$$\lim_{i \rightarrow \infty} \mu_0(\{F \in \mathcal{F}(s_i(x)): F \text{ bad}\}) = 0.$$

Likewise for $\bar{\mu}_0$ we have for almost all $x \in X$,

$$\lim_{i \rightarrow \infty} \bar{\mu}_0(\{\bar{F} \in \bar{\mathcal{F}}(S_i(x)): \bar{F} \text{ bad}\}) = 0.$$

Now let P be any minimal global assignment (Lemma 16). It follows from Lemma 14 and the above remarks that for almost all $x \in X$,

$$(1) \quad \lim_{i \rightarrow \infty} \mu_0(\{F \in \mathcal{F}(s_i(x)): F \text{ belongs to more than one } P_i(\bar{F})\}) = 0.$$

This statement depends only on $\hat{x} = \pi(x)$, and is thus true for almost all fibers $X(\hat{x})$. If x belongs to such a fiber, we define $\phi(x) \in \bar{X}(\hat{x}) \subset \bar{X}$ in the following manner. Let $s_i(x)$ be the skeleton sequence corresponding to x (which depends only on \hat{x}), and let $F_i(x)$ denote the filler for $s_i(x)$ determined by x . Suppose that $S_i(x)$ occurs at (q_i, r_i) in x . Then for any t such that $F_t(x)$ belongs to only one $P_{s(x)}(\bar{F})$, say $P_{s(x)}(\bar{F}_t(x))$, we set

$$\phi(x)[q_t, r_t] = s_t(x) \text{ filled with } \bar{F}_t(x).$$

By the definition of global assignments, if $t < t'$ and if the above is true for both t and t' , then $\bar{F}_t(x)$ is the restriction of $\bar{F}_{t'}(x)$ to the subskeleton $s_t(x)$, so that the definition is consistent. Moreover, by (1), $\phi(x)[q_t, r_t]$ is defined for an infinity of t for almost all elements $x \in X(\hat{x})$ with respect to the fiber measure. By Lemma 4, this defines $\phi(x)$ for almost all $x \in X$.

To complete the proof, we must show that ϕ is a finitary homomorphism. It is obvious from the definition that ϕ is (measurable and) finitary and that ϕ commutes with T and \bar{T} . To check that $\phi\mu = \bar{\mu}$ it suffices to prove that for almost all $\hat{x} \in \bar{X}$, the map

$$\phi|_{X(\hat{x})}: X(\hat{x}) \rightarrow \bar{X}(\hat{x})$$

carries $\mu_{\hat{x}}$ to $\bar{\mu}_{\hat{x}}$. Now if s is a skeleton occurring around zero in \hat{x} , then the elements of $\mathcal{F}(s)$ and $\bar{\mathcal{F}}(s)$ correspond to cylinder sets in $X(\hat{x})$ and $\bar{X}(\hat{x})$ whose $\mu_{\hat{x}}$ and $\bar{\mu}_{\hat{x}}$ measures are given by μ_0 and $\bar{\mu}_0$ respectively. It follows easily from the construction above and from the definition of a society that

$$\phi|_{X(\hat{x})}(\mu_{\hat{x}}) \leq \bar{\mu},$$

and hence

$$\phi\mu \leq \bar{\mu}.$$

Therefore $\phi\mu = \bar{\mu}$ and our proof is complete.

We close this paragraph by stating the following result without proof.

THEOREM 17. *The construction of ϕ is effective; that is, it can be carried out by a machine if the probability vectors p and \bar{p} are given, and the average time needed to determine the zero coordinate of $\phi(x)$ (or any finite number of coordinates) is finite.*

This is in contrast to the Meshalkin and Blum–Hanson codes, which are simpler but have infinite expectation.

BIBLIOGRAPHY

1. J. R. Blum and D. Hanson, *On the isomorphism problem for Bernoulli schemes*, Bull. Amer. Math. Soc. **69** (1963), 221–223.
2. M. Keane, *Coding problems in ergodic theory*, Proceedings of the International Conference on Mathematical Physics, Camerino, Italy, 1974.
3. L. Meshalkin, *A case of isomorphism of Bernoulli schemes*, Dokl. Akad. Nauk SSSR **128** (1959), 41–44.
4. G. Monroy and B. Russo, *A family of codes between some Markov and Bernoulli schemes*, to appear.
5. D. Ornstein, *Ergodic Theory, Randomness, and Dynamical Systems*, Yale Univ. Press, 1974.
6. M. Smorodinsky, *Ergodic Theory, Entropy*, SLN 214, 1971.
7. B. Weiss, *The structure of Bernoulli systems*, Proceedings of the ICM, Vancouver, 1974.
8. B. Bollobás and N. Th. Varopoulos, *Representation of systems of measurable sets*, Math. Proc. Camb. Phil. Soc. **78** (1974), 323–325.
9. R. Dehnad, Ph.D. Thesis, U.C., Berkeley, 1975.

LABORATOIRE DE PROBABILITÉS

E.R.A. 250 DU CNRS UNIVERSITÉ DE RENNES

B.P. 25A, 35031 RENNES CÉDEX, FRANCE

AND

DEPARTMENT OF STATISTICS

TEL AVIV UNIVERSITY

TEL AVIV, ISRAEL