INDEPENDENT EVENTS AND INDEPENDENT EXPERIMENTS

YULIY M. BARYSHNIKOV AND BENNETT EISENBERG

(Communicated by George C. Papanicolaou)

Abstract. It is shown that independent events in a probability space with equally likely outcomes are isomorphic to events coming from independent experiments each with equally likely outcomes.

INTRODUCTION

Let $\Omega$ be a finite set with uniform probability distribution $P$. Denote the cardinality of $\Omega$ by $|\Omega| = \prod_{j=1}^{n} p_j$, where the $p_j$'s are prime numbers greater than one, which are not necessarily distinct. Eisenberg and Ghosh [1] show that there does not exist a collection of more than $n$ nontrivial mutually independent events in $\Omega$, where $n$ is the number of prime factors of $|\Omega|$. An event is called trivial if it has probability 0 or 1. The proof is complicated by the fact that it uses the number of times that each distinct prime number occurs in the factorization of $|\Omega|$. In this article we give a more unified proof of the result of Eisenberg and Ghosh.

Next consider the product space $\Omega_1 \times \cdots \times \Omega_n$ with the uniform probability distribution where $|\Omega_j| = p_j$. The $\Omega_j$'s can be interpreted as spaces of outcomes of independent experiments, each with equally likely outcomes. If $A_j$ is a nontrivial cylinder set based on $\Omega_j$ for $j = 1, \ldots, n$, then $A_1, \ldots, A_n$ form a collection of $n$ nontrivial mutually independent events in $\Omega_1 \times \cdots \times \Omega_n$. These are the most fundamental types of independent events since they are events related to independent experiments. There is a 1-1 map from this product space to $\Omega$, and under this isomorphism the images of the $A_j$'s are nontrivial mutually independent events in $\Omega$. In this article we show that any set of nontrivial mutually independent events in $\Omega$ must be of this form; that is, mutually independent events in $\Omega$ must be isomorphic to events from independent experiments with equally likely outcomes.
1. INDEPENDENT EVENTS IN A SPACE OF $N$ EQUALLY LIKELY OUTCOMES

The main results are corollaries to the following lemma. The notation of the lemma is used throughout this section.

**Lemma.** Let $\Omega$ be a probability space with $N$ equally likely outcomes. Assume that $A_1, \ldots, A_m$ are nontrivial mutually independent events in $\Omega$. Let $\mathcal{F}_0 = \{\emptyset, \Omega\}$ and let $\mathcal{F}_j$ be the field generated by $\{A_1, \ldots, A_j\}$ for $j = 1, \ldots, m$. Let $N_j$ be the greatest common divisor of the cardinalities of the sets in $\mathcal{F}_j$.

Then

1. $N_0 = N$ and $N_j$ is a proper divisor of $N_{j-1}$ for $j = 1, \ldots, m$ and
2. $P(A_j) = \frac{h_j N_j}{N_{j-1}}$ for an integer $h_j$ with $1 \leq h_j < \frac{N_{j-1}}{N_j}$.

**Proof.** Since $\mathcal{F}_{j-1} \subset \mathcal{F}_j$, it follows that $N_j$ divides the cardinality of every set in $\mathcal{F}_{j-1}$, and hence $N_j$ divides $N_{j-1}$. We must show that it is a proper divisor, i.e., $N_j < N_{j-1}$.

From the definition of $N_{j-1}$, it follows that there exists a representation $N_{j-1} = \sum k_a |B_a|$, where the $k_a$'s are integers and the $B_a$'s are sets in $\mathcal{F}_{j-1}$. Form the sum $S = \sum k_a |B_a A_j|$. Since $A_j$ is independent of $\mathcal{F}_{j-1}$, it follows that $|B_a A_j| = P(B_a A_j)N = P(B_a)P(A_j)N = |B_a|P(A_j)$. Thus $S = \sum k_a |B_a|P(A_j) = N_{j-1}P(A_j)$. Since $S$ is a sum of integral multiples of the cardinalities of sets in $\mathcal{F}_j$, it must be divisible by $N_j$. Thus $N_{j-1}P(A_j) = h_j N_j$ for some integer $h_j$. Since $0 < P(A_j) < 1$, it follows that $1 \leq h_j < \frac{N_{j-1}}{N_j}$.

Hence $N_j = P(A_j)N_{j-1}/h_j < N_{j-1}$. This proves (1).

Furthermore, $P(A_j) = \frac{h_j N_j}{N_{j-1}}$, which gives (2). \qed

**Theorem 1.** If $A_1, \ldots, A_m$ are nontrivial mutually independent events in $\Omega$ then $m \leq n$, where $n$ is the number of prime factors of $N$.

**Proof.** Suppose $m > n$. From the lemma, $N_1$ is a proper divisor of $N$. Hence $N_1$ has at most $n - 1$ prime factors. Continuing in this way, $N_m$ has at most $n - m$ prime factors. Thus $N_n = 1$, which has no proper divisors. But the lemma implies that $N_{n+1}$ must be a proper divisor of $N_n$. This is a contradiction. \qed

**Theorem 2.** If $A_1, \ldots, A_m$ are nontrivial mutually independent events in $\Omega$, then there exists an isomorphism from $\Omega$ to $\Omega' = \Omega_1 \times \cdots \times \Omega_m \times \Omega_{m+1}$, where $|\Omega_j| = \frac{N_{j-1}}{N_j}$ for $j = 1, \ldots, m$ and $|\Omega_{m+1}| = N_m$, such that $A_j$ gets mapped to a cylinder set based in $\Omega_j$ for $j = 1, \ldots, m$.

**Proof.** According to the lemma, $P(A_j) = \frac{h_j N_j}{N_{j-1}}$ with $1 \leq h_j < \frac{N_{j-1}}{N_j}$. Choose a set of $h_j$ points in $\Omega_j$ and let $A'_j$ be the cylinder set based on this set. Then if all points in $\Omega'$ are equally likely, we have that $P(A_j) = P(A'_j)$. Due to the independence of $A_1, \ldots, A_m$ in $\Omega$ and $A'_1, \ldots, A'_m$ in $\Omega'$, we have that each atom in the field generated by $A_1, \ldots, A_m$ has the same probability as the corresponding atom in the field generated by $A'_1, \ldots, A'_m$. Since $|\Omega| = |\Omega'|$, these atoms must have the same number of points as well. By choosing arbitrary 1-1 maps between points in the corresponding atoms, we get the desired isomorphism. \qed

**Corollary.** If $A_1, \ldots, A_n$ are nontrivial mutually independent events in $\Omega$, where $n$ is the number of prime factors $|\Omega|$, then one can choose $\Omega' = \Omega_1 \times \cdots \times \Omega_n$ in Theorem 2.
Proof. As in the proof of Theorem 1 we have that \( N_n = 1 \) so that the factor \( \Omega_{n+1} \) is not needed in order that \(|\Omega| = |\Omega'|\). The proof of Theorem 2 then applies to complete the proof. □

Example. Let \( \Omega = \{1, 2, 3, 4, 5, 6\} \), \( A_1 = \{2, 4, 6\} \), and \( A_2 = \{1, 2, 3, 4\} \). Then \( A_1 \) and \( A_2 \) are independent events. \( N = N_0 = 6 \), \( N_1 = 3 \), and \( N_2 = 1 \). \( N_0/N_1 = 2 \) and \( N_1/N_2 = 3 \). Let \( \Omega_1 = \{1, 2\} \) and \( \Omega_2 = \{1, 2, 3\} \). We may then choose \( A'_1 = \{(1, 1), (1, 2), (1, 3)\} \) and \( A'_2 = \{(1, 1), (2, 1), (1, 2), (2, 2)\} \) so that \( A'_1 \) represents the event "1 on experiment 1" and \( A'_2 \) represents the event "1 or 2 on experiment 2." The isomorphism is then any 1-1 map that takes \( A_1A_2 = \{2, 4\} \) to \( A'_1A'_2 = \{(1, 1), (1, 2)\} \), that takes \( A_1A'_2 = \{1, 3\} \) to \( A'_1A'_2 = \{(1, 3)\} \), that takes \( A'_1A_2 = \{1, 3\} \) to \( A'_1A'_2 = \{(1, 3)\} \), and takes \( A'_1A'_2 = \{5\} \) to \( A'_1A'_2 = \{(2, 3)\} \). One way to achieve this is 1 \( \rightarrow (2, 1) \), 2 \( \rightarrow (1, 1) \), 3 \( \rightarrow (2, 2) \), 4 \( \rightarrow (1, 2) \), 5 \( \rightarrow (2, 3) \), and 6 \( \rightarrow (1, 3) \).

In general these conclusions do not apply to pairwise independent events. For example, Eisenberg and Ghosh show that if \(|\Omega| = k^2\) for any \( k \geq 2 \), then there exists a collection of \( k + 1 \) nontrivial pairwise independent events in \( \Omega \). For example, if \(|\Omega| = 25\) then there is a collection of six nontrivial pairwise independent events. On the other hand, there can be no more than two nontrivial mutually independent events in this case. Theorem 1 does extend to pairwise independent events, however, if the prime factors of \(|\Omega|\) are all distinct. This result is also proved in the Eisenberg and Ghosh article.

References


Department of Mathematics, University of Osnabruck, Osnabruck, Germany  
E-mail address: yuliy@chryseis.mathematik.uni-osnabrueck.de

Department of Mathematics, Lehigh University, Bethlehem, Pennsylvania 18015  
E-mail address: BE01@Lehigh.EDU