An operational characterization of the notion of probability by algorithmic randomness and its applications

Kohtaro Tadaki

Department of Computer Science, College of Engineering
Chubu University
Nagoya, Japan

CCR 2015, June 24th, 2015, Institute of Computer Science, Heidelberg University

Abstract

The notion of probability plays an important role in almost all areas of science and technology. In modern mathematics, however, probability theory means nothing other than measure theory, and the operational characterization of the notion of probability does not seem to be established yet.

In this talk, based on the toolkit of algorithmic randomness we present an operational characterization of the notion of probability.

We use the notion of Martin-Löf randomness with respect to Bernoulli measure to present the operational characterization. As the first step of the research of this line, in this talk we consider the case of finite probability space, i.e., the case where the sample space of the underlying probability space is finite, for simplicity.

We give a natural operational characterization of the notion of conditional probability, and show how to represent the notion of the independence of random variables/events by the operational characterization.

Finally, we mention some of the applications of our formalism to the general areas of science and technology.

Historical Background

Historical Background

At the beginning of the past century, there was a comprehensive attempt to provide an operational characterization for the notion of probability. Namely, von Mises developed a mathematical theory of repetitive events which was aimed at reformulating the theory of probability and statistics based on an operational characterization of the notion of probability.

In the attempt, he introduced the notion of collective as a mathematical idealization of a long sequence of outcomes of experiments or observations repeated under a set of invariable conditions, such as the repeated tossing of a coin or of a pair of dice.

The collective plays a role as an operational characterization of the notion of probability, and is an infinite sequence of sample points of a probability space. In 1939, however, Ville revealed the defect of the notion of collective from the aspect of randomness. In addition, the collective has an intrinsic defect that it cannot exclude the possibility that an event with probability zero may occur.

Historical Background

In 1966, Martin-Löf introduced the definition of random sequences, which is called Martin-Löf randomness nowadays, and plays a central role in the recent development of algorithmic randomness.

At the same time, he introduced the notion of Martin-Löf randomness with respect to Bernoulli measure. He then pointed out that this notion overcomes the defect of collective, and this can be regarded precisely as the collective which von Mises wanted to define. However, Martin-Löf himself did not develop probability theory based on Martin-Löf random sequence with respect to Bernoulli measure.

The aim of this talk is to develop an operational characterization of the notion of probability based on Martin-Löf random sequence with respect to Bernoulli measure, according to von Mises's idea for reformulating probability theory based on the collective.

Probability Space

Finite Probability Space

We give an operational characterization of the notion of probability for a finite probability space.

Definition A *finite probability space* is a mapping $P\colon \Omega \to [0,1]$ which satisfies the following:

(i) The domain of definition Ω is a non-empty finite set.

(ii) $\sum_{a\in\Omega} P(a) = 1$.

Here, Ω is called the *sample space*, and elements in Ω are called *sample points* or *elementary events*. A subset of Ω is called an *event*. For each event A, $P(A)$ is defined by

$$P(A) := \sum_{a\in A} P(a),$$

and is called the *probability* of A. □

Note that most probability spaces appearing in engineering are finite.

Algorithmic Randomness

Bernoulli measure

Let Ω be a non-empty finite set. Then Ω^* denotes the set of all finite strings over Ω, and Ω^∞ denotes the set of all infinite sequences over Ω.

Let $P\colon \Omega \to [0,1]$ be a finite probability space. *Bernoulli measure* λ_P on Ω^∞ has the following property: For every $\sigma \in \Omega^*$,

$$\lambda_P\left([\sigma]^\prec\right) = \prod_{a\in\Omega} P(a)^{N_a(\sigma)},$$

where $[\sigma]^\prec$ denotes the set of all infinite sequences over Ω which have σ as a prefix, and $N_a(\sigma)$ denotes the number of the occurrences of the element a in a finite string σ over Ω.

Martin-Löf randomness with respect to Bernoulli measure

Definition [Martin-Löf 1966] Let $P\colon \Omega \to [0,1]$ be a finite probability space.

(i) A Martin-Löf P-test over Ω is a uniformly recursively enumerable sequence $\{G_n\}_{n\in\mathbb{N}} \subset \Omega^*$ such that for every $n \in \mathbb{N}$,

$$\lambda_P\left([G_n]^{\prec}\right) \leq 2^{-n},$$

where $[G_n]^{\prec} := \{\alpha \in \Omega^\infty \mid \text{Some prefix of } \alpha \text{ is in } G_n\}$.

(ii) $\alpha \in \Omega^\infty$ is called *Martin-Löf P-random* if for every Martin-Löf P-test $\{G_n\}_{n\in\mathbb{N}}$ over Ω,

$$\alpha \notin \bigcap_{n=0}^{\infty} [G_n]^{\prec}.$$

□

Remark In this talk, a finite probability space P is not required to be computable at all (except for the results related to van Lambalgen's Theorem). Thus, Bernoulli measure λ_P is not necessarily computable.

An Operational Characterization of the Notion of Probability:

Ensemble

Ensemble

We propose that a Martin-Löf P-random sequence of elementary events gives an operational characterization of the notion of probability. Since this notion plays a central role in our formalism, we call it *ensemble*, in particular, instead of collective for distinction. The name "ensemble" comes from physics.

Definition [Ensemble]
Let $P\colon \Omega \to [0,1]$ be a finite probability space. A Martin-Löf P-random sequence is called an *ensemble* for the finite probability space P. □

Consider an infinite sequence $\alpha \in \Omega^\infty$ of outcomes which is being generated by infinitely repeated trials *described by* the finite probability space P. The operational characterization of the notion of probability for the finite probability space P is thought to be completed if the property which the infinite sequence α has to satisfy is determined. We thus propose the following thesis.

Thesis Let $P\colon \Omega \to [0,1]$ be a finite probability space. An infinite sequence of outcomes in Ω which is being generated by infinitely repeated trials *described by* the finite probability space P is an ensemble for P. □

We check the validity of the thesis

in what follows.

What is “probability” ?

"Necessary Conditions" for the Notion of Probability to Satisfy

Consider an infinite sequence $\alpha \in \Omega^{\infty}$ of outcomes which is being generated by infinitely repeated trials described by a finite probability space P. According to our intuitive understanding on the notion of probability, the necessary conditions which the notion of probability ought to satisfy seem as follows:

- The law of large numbers holds for α.
- An event with probability zero never occurs in α.
- α must be closed under a computable shuffling.
- α must be closed under the selection by a computable selection function.
- . . . . . .

The law of large numbers holds for ensembles

Theorem [The law of large numbers]

Let $P\colon \Omega \to [0,1]$ be a finite probability space.

(i) [Martin-Löf 1966] For every $\alpha \in \Omega^\infty$, if α is an ensemble for P, then the law of large numbers holds for α, that is, for every $a \in \Omega$,

$$\lim_{n\to\infty} \frac{\#\text{ of } a \text{ in } \alpha\restriction n}{n} = P(a).$$

(ii) Actually, there exists a single Martin-Löf P-test over Ω such that, for every $\alpha \in \Omega^\infty$, if α passes the test then the law of large numbers holds for α. □

This theorem holds even if the finite probability space P is not computable.

An event with probability zero never occurs in ensembles

Consider the finite probability space $P\colon \{a, b\} \to [0, 1]$ such that $P(a) = 0$ and $P(b) = 1$. Consider the infinite sequence

$$\alpha = b, a, b, b, b, b, b, b, b, b, b, b, \ldots\ldots .$$

Since

$$\lim_{n\to\infty} \frac{\#\text{ of } a \text{ in } \alpha\restriction n}{n} = 0 = P(a),$$

the law of large numbers certainly holds for α. However, the event a with probability zero has occurred in α once. This contradicts our intuition, in particular, contradicts the notion of probability in quantum mechanics. Thus, the law of large numbers is insufficient to characterizes the notion of probability, and the notion of probability is more than the law of large numbers.

Theorem [Martin-Löf 1966] Let $P\colon \Omega \to [0, 1]$ be a finite probability space, and let $a \in \Omega$. Suppose that $P(a) = 0$. Then, for every $\alpha \in \Omega^\infty$, if α is an ensemble for P, then α does not contain a at all. □

Other Necessary Conditions for the Notion of Probability I

Assume that an observer A performs an infinite reputation of trials described by a finite probability space $P\colon \Omega \to [0,1]$, and thus is generating an infinite sequence $\alpha \in \Omega^{\infty}$ of outcomes of trials:

$$\alpha = a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ a_6,\ a_7,\ a_8,\ a_9,\ a_{10},\ a_{11},\ a_{12},\ \ldots\ldots\ldots .$$

According to our thesis, α is an ensemble for P.

Consider another observer B who wants to adopt the following subsequence β of α as the outcomes of the trials:

$$\beta = a_2,\ a_3,\ a_5,\ a_7,\ a_{11},\ a_{13},\ a_{17},\ \ldots\ldots\ldots ,$$

where the observer B only takes into account the nth elements in the original sequence α such that n is a prime number. According to our thesis, β has to be an ensemble for P, as well. However, is this true?

Consider this problem in a general setting.

Other Necessary Conditions for the Notion of Probability I

Assume that an observer A performs an infinite reputation of trials described by a finite probability space $P\colon \Omega \to [0,1]$, and thus is generating an infinite sequence $\alpha \in \Omega^{\infty}$ of outcomes of trials:

$$\alpha = a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ a_6,\ a_7,\ a_8,\ a_9,\ a_{10},\ a_{11},\ a_{12},\ \ldots\ldots\ldots .$$

According to our thesis, α is an ensemble for P.

Let $f\colon \mathbb{N}^+ \to \mathbb{N}^+$ be an injection. Consider another observer B who wants to adopt the following sequence β as the outcomes of the trials:

$$\beta = a_{f(1)},\ a_{f(2)},\ a_{f(3)},\ a_{f(4)},\ a_{f(5)},\ a_{f(6)},\ a_{f(7)},\ \ldots\ldots\ldots,$$

instead of α.

According to our thesis, β has to be an ensemble for P, as well. However, is this true?

We can confirm this by restricting the ability of B, that is, by assuming that every observer can select elements from the original sequence α only in an effective manner. This means that the function $f\colon \mathbb{N}^+ \to \mathbb{N}^+$ has to be a computable function.

Other Necessary Conditions for the Notion of Probability I

Ensembles for P are closed under a computable shuffling.

Theorem [Closure property under a computable shuffling]

Let $P\colon \Omega \to [0,1]$ be a finite probability space, and let $\alpha = a_1 a_2 a_3 a_4 a_5 \cdots\cdots \in \Omega^\infty$ be an ensemble for P. Then, for every injective function $f\colon \mathbb{N}^+ \to \mathbb{N}^+$, if f is computable then the infinite sequence

$$a_{f(1)} a_{f(2)} a_{f(3)} a_{f(4)} a_{f(5)} a_{f(6)} \cdots\cdots\cdots$$

is an ensemble for P. □

Note that this theorem holds even if the finite probability space P is not computable.

Other Necessary Conditions for the Notion of Probability II

Consider an infinite sequence $\alpha \in \Omega^\infty$ of outcomes which is obtained by an infinite reputation of trials described by a finite probability space $P\colon \Omega \to [0,1]$:

$$\alpha = a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ a_6,\ a_7,\ a_8,\ a_9,\ a_{10},\ a_{11},\ a_{12},\ \cdots\cdots\cdots .$$

Ensembles for P are closed under "the selection by" a selection function in the definition of von Mises-Wald-Church stochasticity.

Theorem [Closure property under the selection by a selection function]
Let $P\colon \Omega \to [0,1]$ be a finite probability space, and let $\alpha = a_1a_2a_3a_4a_5\cdots\cdots \in \Omega^\infty$ be an ensemble for P. Let g be a selection function, i.e., a partial computable function $g\colon \Omega^* \to \{\mathrm{Yes}, \mathrm{No}\}$. Suppose that $g(\alpha\restriction_k)$ is defined for all $k \in \mathbb{N}$ and $\{k \in \mathbb{N} \mid g(\alpha\restriction_k) = \mathrm{Yes}\}$ is an infinite set. Then, the infinite sequence

$$a_{f(1)}a_{f(2)}a_{f(3)}a_{f(4)}a_{f(5)}a_{f(6)}\cdots\cdots\cdots$$

is an ensemble for P, where the function $f\colon \mathbb{N}^+ \to \mathbb{N}^+$ is defined by $f(n) := \min\{m \in \mathbb{N} \mid \#\{k \in \mathbb{N} \mid k \le m \ \&\ g(\alpha\restriction_k) = \mathrm{Yes}\} = n\} + 1$. □

Note that this theorem holds even if the finite probability space P is not computable.

Conditional Probability

Conditional Probability

Definition [Conditional probability] Let $P\colon \Omega \to [0,1]$ be a finite probability space, and let $B \subset \Omega$. Suppose that $P(B) > 0$. Then, for each event $A \subset \Omega$, the *conditional probability of A given B*, denoted by $P(A|B)$, is defined as $P(A \cap B)/P(B)$. This notion defines a finite probability space $P_B\colon B \to [0,1]$ such that $P_B(a) = P(\{a\}|B)$ for every $a \in B$. □

Definition When an infinite sequence $\alpha \in \Omega^\infty$ contains infinitely many elements from B, $\mathrm{Filtered}_B(\alpha)$ is defined as the infinite sequence over B obtained from α by eliminating all elements in $\Omega - B$ occurring in α. □

Example Let $P\colon \{0,1,2\} \to [0,1]$ be a finite probability space, and let B be $\{0,2\}$. Consider an ensemble α for P:

$$\alpha = 1,0,1,2,2,0,1,0,2,1,1,0,0,1,2,\ldots\ldots.$$

Then

$$\mathrm{Filtered}_B(\alpha) = 0,2,2,0,0,2,0,0,2,\ldots\ldots.$$

Note that the notion of $\mathrm{Filtered}_B(\alpha)$ in our theory corresponds to the notion of *partition* in the theory of collectives by von Mises.

Conditional Probability

Theorem [Ensembles are closed under conditioning]

Let $P\colon \Omega \to [0,1]$ be a finite probability space, and let $B \subset \Omega$ with $P(B) > 0$. For every ensemble α for P, $\text{Filtered}_B(\alpha)$ is an ensemble for the finite probability space $P_B\colon B \to [0,1]$. □

Application [Von Neumann extractor]

> "Consider a Bernoulli sequence. Von Neumann extractor takes successive pairs of consecutive bits from the Bernoulli sequence. If the two bits matches, no output is generated. If the bits differs, the value of the first bit is output. The Von Neumann extractor can be shown to produce a uniform binary output."

In our framework, the Von Neumann extractor operates as follows: Let $P\colon \{0,1\} \to [0,1]$ be a finite probability space, and let α be an ensemble for P. Then α can be regarded as an ensemble for a finite probability space $Q\colon \{00,01,10,11\} \to [0,1]$ where $Q(ab) = P(a)P(b)$ for every $a,b \in \{0,1\}$. Consider the event $B = \{01,10\}$. It follows from the above theorem that $\text{Filtered}_B(\alpha)$ is an ensemble for $Q_B\colon \{01,10\} \to [0,1]$ with $Q_B(01) = Q_B(10) = 1/2$. Namely, α is a Martin-Löf random sequence over the alphabet $\{01,10\}$. Hence, a random sequence is certainly extracted. □

In general, an ensemble has strong closure properties.

Independence

Independence

Probability Theory

- Independence between events
- Independence between random variables

Operational Characterization: Ensembles

- Independence between ensembles
- Independence in the sense of van Lambalgen's Theorem

Independence between Two Events

Independence between Two Events

Definition [Independence between two events]

Let $P\colon \Omega \to [0,1]$ be a finite probability space. For any events $A, B \subset \Omega$, we say that A and B are *independent* if $P(A \cap B) = P(A)P(B)$. □

In the case of $P(B) > 0$, A and B are independent if and only if $P(A|B) = P(A)$.

Independence between Two Events

Definition Let $P\colon \Omega \to [0,1]$ be a finite probability space, and let $A \subset \Omega$ be an event. For each ensemble α for P, $\mathsf{C}_A(\alpha)$ is defined as the infinite binary sequence such that, for every i, its ith element $\mathsf{C}_A(\alpha)(i)$ is 1 if $\alpha(i) \in A$ and 0 otherwise. The pair (P, A) induces a finite probability space $\mathcal{C}(P, A) : \{0,1\} \to [0,1]$ such that $\mathcal{C}(P, A)(1) = P(A)$ and $\mathcal{C}(P, A)(0) = 1 - P(A)$. □

Example Let $P\colon \{a, b, c\} \to [0,1]$ be a finite probability space, and let A be $\{a, c\}$. Consider an ensemble α for P:

$$\alpha = b, a, b, c, c, a, b, a, c, b, b, a, a, b, c, \ldots\ldots .$$

Then

$$\mathsf{C}_A(\alpha) = 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, \ldots\ldots .$$

Note that the notions of $\mathsf{C}_A(\alpha)$ and $\mathcal{C}(P, A)$ in our theory together correspond to the notion of *mixing* in the theory of collectives by von Mises.

Theorem [Closure property under membership] Let $P\colon \Omega \to [0,1]$ be a finite probability space, and let $A \subset \Omega$. Suppose that α is an ensemble for P. Then $\mathsf{C}_A(\alpha)$ is an ensemble for the finite probability space $\mathcal{C}(P, A)$. □

Independence between Two Events

Definition Let $\alpha, \beta \in \Omega^\infty$. We say that α and β are *equivalent* if there exists a finite probability space $P \in \Omega \to [0,1]$ such that α and β are both an ensemble for P. □

The following theorem gives an operational characterization of the notion of the independence between two events by the notion of ensemble.

Theorem Let $P \colon \Omega \to [0,1]$ be a finite probability space, and let $A, B \subset \Omega$. Suppose that $P(B) > 0$. Then the following conditions are equivalent.

(i) The events A and B are independent.

(ii) For every ensemble α for the finite probability space P it holds that $\mathsf{C}_A(\alpha)$ is equivalent to $\mathsf{C}_A(\mathsf{Filtered}_B(\alpha))$.

(iii) There exists an ensemble α for the finite probability space P such that $\mathsf{C}_A(\alpha)$ is equivalent to $\mathsf{C}_A(\mathsf{Filtered}_B(\alpha))$. □

Independence of Random Variables and Independence of Ensembles

Independence of Random Variables

A *random variable* on a non-empty finite set Ω is a function $X : \Omega \to \Omega'$ where Ω' is a non-empty finite set.

Definition [Independence of random variables]

Let $P : \Omega \to [0, 1]$ be a finite probability space. Let $X_1 : \Omega \to \Omega_1, \ldots, X_n : \Omega \to \Omega_n$ be random variables on Ω. We say that the random variables $X_1, \ldots, X_n$ are *independent* if for every $x_1 \in \Omega_1, \ldots, x_n \in \Omega_n$ it holds that

$$P(X_1 = x_1 \;\&\; \ldots \;\&\; X_n = x_n) = P(X_1 = x_n) \cdots P(X_n = x_n),$$

where $X_i = x_i$ denotes the set $\{a \in \Omega \mid X_i(a) = x_i\}$ for each $i = 1, \ldots, n$. □

Independence of Ensembles

Let $\Omega_1, \ldots, \Omega_n$ be non-empty finite sets. For any $\alpha_1 \in \Omega_1^\infty, \ldots, \alpha_n \in \Omega_n^\infty$, we use

$$\alpha_1 \times \cdots \times \alpha_n$$

to denote an infinite sequence α over $\Omega_1 \times \cdots \times \Omega_n$ such that

$$\alpha(i) := (\alpha_1(i), \ldots, \alpha_n(i))$$

for every $i \in \mathbb{N}^+$.

Definition [Independence of ensembles]

Let $P_1 \colon \Omega_1 \to [0,1], \ldots, P_n \colon \Omega_n \to [0,1]$ be finite probability spaces. Let $\alpha_1, \ldots, \alpha_n$ be ensembles for $P_1, \ldots, P_n$, respectively. We say that $\alpha_1, \ldots, \alpha_n$ are *independent* if $\alpha_1 \times \cdots \times \alpha_n$ is an ensemble for a finite probability space $P \colon \Omega_1 \times \cdots \times \Omega_n \to [0,1]$ where

$$P(a_1, \ldots, a_n) := P_1(a_1) \cdots P_n(a_n)$$

for every $a_1 \in \Omega_1, \ldots, a_n \in \Omega_n$. □

Note that the notion of the independence of ensembles in our theory corresponds to the notion of *independence* in the theory of collectives by von Mises.

Independence of Random Variables and Independence of Ensembles

Let $\alpha \in \Omega^{\infty}$, and $X : \Omega \to \Omega'$ be a random variable. We define $X(\alpha)$ as an infinite sequence β over Ω' such that $\beta(i) := X(\alpha(i))$ for every $i \in \mathbb{N}^{+}$.

Theorem [Closure property under mapping by random variable]
Let $P : \Omega \to [0, 1]$ be a finite probability space, and let $X : \Omega \to \Omega'$ be a random variable on Ω. If α is an ensemble for P then $X(\alpha)$ is an ensemble for a finite probability space $P' : \Omega' \to [0, 1]$ where $P'(x) := P(X = x)$ for every $x \in \Omega'$. □

Theorem [Equivalence of two independence notions] Let $P : \Omega \to [0, 1]$ be a finite probability space, and let $X_1 : \Omega \to \Omega_1, \ldots, X_n : \Omega \to \Omega_n$ be random variables on Ω. Then the following conditions are equivalent.

(i) The random variables $X_1, \ldots, X_n$ are independent.

(ii) For every ensemble α for P, the ensembles $X_1(\alpha), \ldots, X_n(\alpha)$ are independent.

(iii) There exists an ensemble α for P such that the ensembles $X_1(\alpha), \ldots, X_n(\alpha)$ are independent. □

The independence of random variables/events is equivalent to the independence in the sense of van Lambalgen's Theorem *in the case where the underlying finite probability space is computable.*

van Lambalgen's Theorem

Theorem [van Lambalgen's Theorem, van Lambalgen 1987]

For every $\alpha, \beta \in \{0,1\}^\infty$, the following conditions are equivalent.

(i) $\alpha \oplus \beta$ is Martin-Löf random.

(ii) α is Martin-Löf random relative to β and β is Martin-Löf random. □

Equivalence of Two Independence Notions

Definition [Computable finite probability space]

Let $P\colon \Omega \to [0,1]$ be a finite probability space. We say that P is *computable* if $P(a)$ is a computable real for every $a \in \Omega$. □

Theorem [A generalization of van Lambalgen's Theorem]

Let $P_1\colon \Omega_1 \to [0,1], \ldots, P_n\colon \Omega_n \to [0,1]$ be finite probability spaces. Let $\alpha_1, \ldots, \alpha_n$ be ensembles for $P_1, \ldots, P_n$, respectively. Suppose that $P_1, \ldots, P_n$ are computable. Then the following conditions are equivalent.

(i) The ensembles $\alpha_1, \ldots, \alpha_n$ are independent.

(ii) For every $k = 1, \ldots, n-1$ it holds that α_k is Martin-Löf P_k-random relative to $\alpha_{k+1}, \ldots, \alpha_n$. □

In summary, the three independence notions are equivalent in the case where the underlying finite probability space is computable.

Equivalence of the Three Independence Notions

Theorem [Operational characterizations of the notion of independence of random variables]

Let $P\colon \Omega \to [0,1]$ be a finite probability space, and let $X_1\colon \Omega \to \Omega_1, \ldots, X_n\colon \Omega \to \Omega_n$ be random variables on Ω. Suppose that P is computable. Then the following conditions are equivalent.

(i) The random variables $X_1, \ldots, X_n$ are independent.

(ii) For every ensemble α for P, the ensembles $X_1(\alpha), \ldots, X_n(\alpha)$ are independent.

(iii) There exists an ensemble α for P such that the ensembles $X_1(\alpha), \ldots, X_n(\alpha)$ are independent.

(iv) For every ensemble α for P and every $k = 1, \ldots, n-1$ it holds that $X_k(\alpha)$ is Martin-Löf P_k-random relative to $X_{k+1}(\alpha), \ldots, X_n(\alpha)$.

(v) There exists an ensemble α for P such that for every $k = 1, \ldots, n-1$ it holds that $X_k(\alpha)$ is Martin-Löf P_k-random relative to $X_{k+1}(\alpha), \ldots, X_n(\alpha)$.

Here, $P_k\colon \Omega_k \to [0,1]$ is a finite probability space such that $P_k(x) := P(X_k = x)$ for every $x \in \Omega_k$. □

Independence of an Arbitrary Number of Events

Independence of an Arbitrary Number of Events

Definition [Independence of events]

Let $P\colon \Omega \to [0,1]$ be a finite probability space, and let $A_1, \ldots, A_n \subset \Omega$. We say that the events $A_1, \ldots, A_n$ are *independent* if for every $i_1, \ldots, i_k$ with $1 \leq i_1 < \cdots < i_k \leq n$ it holds that

$$P(A_{i_1} \cap \cdots \cap A_{i_k}) = P(A_{i_1}) \cdots P(A_{i_k}).$$

□

Proposition

Let $P\colon \Omega \to [0,1]$ be a finite probability space, and let $A_1, \ldots, A_n \subset \Omega$. Then the events $A_1, \ldots, A_n$ are independent if and only if random variables $\chi_{A_1}, \ldots, \chi_{A_n}$ are independent, where the random variable $\chi_{A_k}\colon \Omega \to \{0,1\}$ is defined by the condition that $\chi_{A_k}(a) := 1$ if $a \in A_k$ and $\chi_{A_k}(a) := 0$ otherwise. □

Equivalence of the Independence Notions

Theorem [Operational characterizations of the notion of independence of events]

Let $P\colon \Omega \to [0,1]$ be a finite probability space, and let $A_1, \ldots, A_n \subset \Omega$. Suppose that P is computable. Then the following conditions are equivalent.

(i) The events $A_1, \ldots, A_n$ are independent.

(ii) For every ensemble α for P and every $k = 1, \ldots, n-1$ it holds that $\mathsf{C}_{A_k}(\alpha)$ is Martin-Löf $\mathcal{C}(P, A_k)$-random relative to $\mathsf{C}_{A_{k+1}}(\alpha), \ldots, \mathsf{C}_{A_n}(\alpha)$.

(iii) There exists an ensemble α for P such that for every $k = 1, \ldots, n-1$ it holds that $\mathsf{C}_{A_k}(\alpha)$ is Martin-Löf $\mathcal{C}(P, A_k)$-random relative to $\mathsf{C}_{A_{k+1}}(\alpha), \ldots, \mathsf{C}_{A_n}(\alpha)$. □

Applications to the general areas of science and technology

Some of the Applications

A Refinement of Quantum Mechanics by Algorithmic Randomness

The notion of probability plays a crucial role in quantum mechanics. In modern mathematics which describes quantum mechanics, however, probability theory means nothing other than measure theory, and therefore any operational characterization of the notion of probability is still missing in quantum mechanics. In this sense, the current form of quantum mechanics is considered to be imperfect as a physical theory which must stand on operational means. We reformulate quantum mechanics in terms of our formalism to make it perfect (as partly reported at CCR 2014).

Application to Information Theory

Instantaneous codes play a basic role in the source coding problem in information theory. We present a natural and intuitive equivalent characterization of the notion of *absolute optimality* of an instantaneous code in terms of our formalism.

Application to Cryptography

Information-theoretic security plays a basic role in modern cryptography. We present natural and intuitive equivalent characterizations of the notion of information-theoretic security in terms of our formalism.

Applications to Cryptography

Security Notions in Modern Cryptography

Information-Theoretic Security

- Perfect secrecy, Shannon 1949

Computational Security

- Private-key encryption schemes:

  DES, AES

- Public-key encryption schemes:

  RSA, El Gamal encryption scheme,

  Elliptic curve cryptography

Security Notions in Modern Cryptography

Information-Theoretic Security

- Perfect secrecy, Shannon 1949

Computational Security

- Private-key encryption schemes:

  DES, AES

- Public-key encryption schemes:

  RSA, El Gamal encryption scheme,

  Elliptic curve cryptography

Information-Theoretic Security

Definition [Encryption scheme]

Let $\mathcal{M}$, $\mathcal{K}$, and $\mathcal{C}$ be non-empty finite sets. An *encryption scheme* over a message space $\mathcal{M}$, a key space $\mathcal{K}$, and a ciphertext space $\mathcal{C}$ is a tuple $\Pi = (P_{\mathsf{K}}, \mathsf{Enc}, \mathsf{Dec})$ such that (i) $P_{\mathsf{K}} \colon \mathcal{K} \to [0,1]$ is a finite probability space, (ii) $\mathsf{Enc} \colon \mathcal{M} \times \mathcal{K} \to \mathcal{C}$, (iii) $\mathsf{Dec} \colon \mathcal{C} \times \mathcal{K} \to \mathcal{M}$, and (iv) $\mathsf{Dec}(\mathsf{Enc}(m,k),k) = m$ for every $m \in \mathcal{M}$ and $k \in \mathcal{K}$. □

Let $Q \colon \mathcal{M} \to [0,1]$ be a finite probability space, which serves as a probability distribution over message space $\mathcal{M}$. Define a finite probability space $P_{\Pi,Q} \colon \mathcal{M} \times \mathcal{K} \to [0,1]$ by the condition that $P_{\Pi,Q}(m,k) = Q(m)P_{\mathsf{K}}(k)$ for every $m \in \mathcal{M}$ and $k \in \mathcal{K}$. Define random variables $M_{\Pi,Q}$ and $C_{\Pi,Q}$ on $\mathcal{M} \times \mathcal{K}$ by $M_{\Pi,Q}(m,k) = m$ and $C_{\Pi,Q}(m,k) = \mathsf{Enc}(m,k)$, respectively.

Definition [Perfect secrecy, Shannon 1949]

The encryption scheme Π is *perfectly secret* if for every finite probability space $Q \colon \mathcal{M} \to [0,1]$ it holds that the random variables $M_{\Pi,Q}$ and $C_{\Pi,Q}$ are independent. □

Information-Theoretic Security

Theorem [Equivalent characterizations of perfect secrecy by algorithmic randomness]

Suppose that the finite probability space P_{K} is computable. Then the following conditions are equivalent.

(i) The encryption scheme Π is perfectly secret.

(ii) For every computable finite probability space $Q\colon \mathcal{M} \to [0,1]$ and every ensemble α for $P_{\Pi,Q}$ it holds that $M_{\Pi,Q}(\alpha)$ is Martin-Löf Q-random relative to $C_{\Pi,Q}(\alpha)$.

(iii) For every computable finite probability space $Q\colon \mathcal{M} \to [0,1]$ there exists an ensemble α for $P_{\Pi,Q}$ such that $M_{\Pi,Q}(\alpha)$ is Martin-Löf Q-random relative to $C_{\Pi,Q}(\alpha)$. □

Note that the finite probability space P_{K}, which serves as a probability distribution over key space $\mathcal{K}$, is normally *computable* in modern cryptography.

Information-Theoretic Security

=

Algorithmic Information-Theoretic Security