Finite-state independence and normal words

Verónica Becher

Universidad de Buenos Aires & CONICET

Joint work with Olivier Carton and Nicolás Alvarez

Workshop INFINIS, Paris, November 4, 2016

Finite-state independence

The concept of independence appears in several areas:

Finite-state independence

The concept of independence appears in several areas:

Arithmetic: multiplicative independence

Finite-state independence

The concept of independence appears in several areas:

Arithmetic:	multiplicative independence
Linear Algebra:	linearly independent vectors

Finite-state independence

The concept of independence appears in several areas:

Arithmetic:	multiplicative independence
Linear Algebra:	linearly independent vectors
Probability Theory:	independent random variables

Finite-state independence

The concept of independence appears in several areas:

Arithmetic:	multiplicative independence
Linear Algebra:	linearly independent vectors
Probability Theory:	independent random variables
Shannon's Information Theory:	no mutual information for random variables

Finite-state independence

The concept of independence appears in several areas:

Arithmetic:	multiplicative independence
Linear Algebra:	linearly independent vectors
Probability Theory:	independent random variables
Shannon's Information Theory:	no mutual information for random variables
Algorithmic Information Theory:	independent random infinite words

Finite-state independence

The concept of independence appears in several areas:

Arithmetic:	multiplicative independence
Linear Algebra:	linearly independent vectors
Probability Theory:	independent random variables
Shannon's Information Theory:	no mutual information for random variables
Algorithmic Information Theory:	independent random infinite words
Automata Theory:	finite-state independent words

Intuitive idea

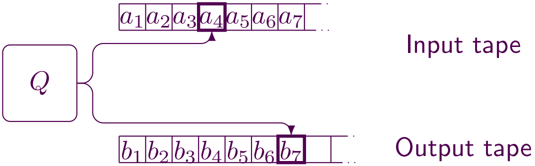
Two words are independent if one does not help to compress the other using any finite automata.

Intuitive idea

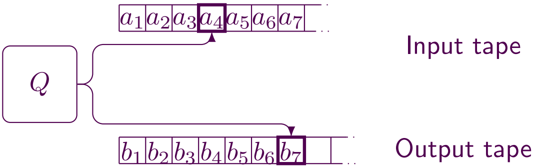
Two words are independent if one does not help to compress the other using any finite automata.

Formalized with compression ratio and conditional compression ratio.

Deterministic automata one input, one output



Deterministic automata one input, one output

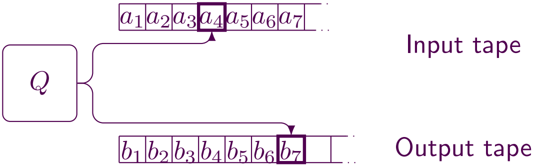


Let $\mathcal{A}$ be a deterministic finite automata with one input and one output, such that $x \mapsto \mathcal{A}(x)$ is one-to-one. The run of $\mathcal{A}$ with input x, starting at q_0 is

$$q_0 \xrightarrow{\alpha_1 | v_1} q_1 \xrightarrow{\alpha_2 | v_2} q_2 \xrightarrow{\alpha_3 | v_3} \cdots$$

$\alpha_i \in A \cup \{\varepsilon\}$, $\alpha_1 \alpha_2 \ldots = x$ and $v_i \in A^*$. The compression ratio of x

Deterministic automata one input, one output



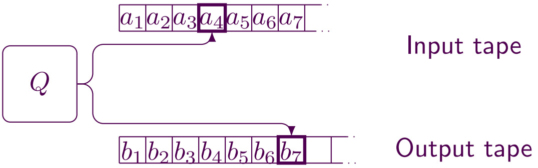
Let $\mathcal{A}$ be a deterministic finite automata with one input and one output, such that $x \mapsto \mathcal{A}(x)$ is one-to-one. The run of $\mathcal{A}$ with input x, starting at q_0 is

$$q_0 \xrightarrow{\alpha_1 | v_1} q_1 \xrightarrow{\alpha_2 | v_2} q_2 \xrightarrow{\alpha_3 | v_3} \cdots$$

$\alpha_i \in A \cup \{\varepsilon\}, \quad \alpha_1 \alpha_2 \ldots = x$ and $v_i \in A^*$. The compression ratio of x

$$\rho_{\mathcal{A}}(x) = \liminf_{n \to \infty} \frac{|v_1 v_2 \cdots v_n|}{|\alpha_1 \ldots \alpha_n|}$$

Deterministic automata one input, one output



Let $\mathcal{A}$ be a deterministic finite automata with one input and one output, such that $x \mapsto \mathcal{A}(x)$ is one-to-one. The run of $\mathcal{A}$ with input x, starting at q_0 is

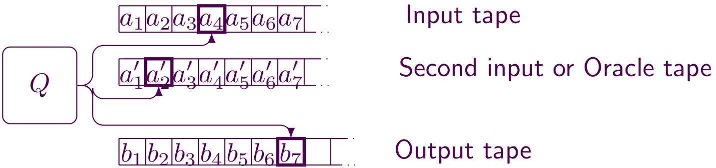
$$q_0 \xrightarrow{\alpha_1|v_1} q_1 \xrightarrow{\alpha_2|v_2} q_2 \xrightarrow{\alpha_3|v_3} \cdots$$

$\alpha_i \in A \cup \{\varepsilon\}, \quad \alpha_1\alpha_2 \ldots = x$ and $v_i \in A^*$. The compression ratio of x

$$\rho_{\mathcal{A}}(x) = \liminf_{n\to\infty} \frac{|v_1 v_2 \cdots v_n|}{|\alpha_1 \ldots \alpha_n|}$$

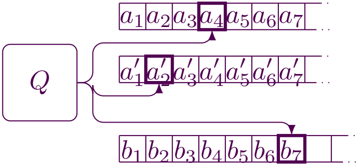
$$\rho(x) = \inf \{\rho_{\mathcal{A}}(x) : \mathcal{A} \text{ is deterministic and one-to-one}\}$$

Deterministic automata with two inputs, one output



Let $\mathcal{A}$ be a deterministic finite automata with two inputs and one output such that for each fixed y, $x \mapsto \mathcal{A}(x, y)$ is one-to-one.

Deterministic automata with two inputs, one output

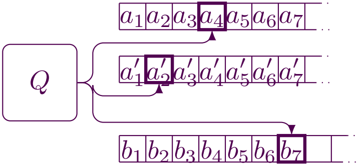


Let $\mathcal{A}$ be a deterministic finite automata with two inputs and one output such that for each fixed y, $x \mapsto \mathcal{A}(x, y)$ is one-to-one.
Consider the run of $\mathcal{A}$ for inputs x, y

$$p_0 \xrightarrow{\alpha_1,\gamma_1|v_1} p_1 \xrightarrow{\alpha_2,\gamma_2|v_2} p_2 \cdots$$

where α_i, γ_i in $A \cup \{\varepsilon\}$, $\alpha_1\alpha_2 \ldots = x$ and $\gamma_1\gamma_2 \ldots = y$, $v_i \in A^*$.

Deterministic automata with two inputs, one output



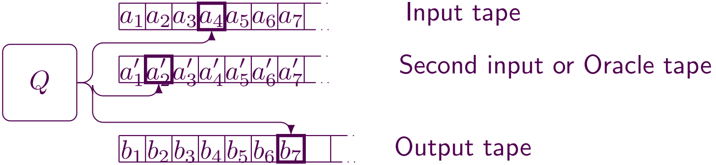
Let $\mathcal{A}$ be a deterministic finite automata with two inputs and one output such that for each fixed y, $x \mapsto \mathcal{A}(x, y)$ is one-to-one.
Consider the run of $\mathcal{A}$ for inputs x, y

$$p_0 \xrightarrow{\alpha_1,\gamma_1|v_1} p_1 \xrightarrow{\alpha_2,\gamma_2|v_2} p_2 \cdots$$

where α_i, γ_i in $A \cup \{\varepsilon\}$, $\alpha_1\alpha_2 \ldots = x$ and $\gamma_1\gamma_2 \ldots = y$, $v_i \in A^*$.
The conditional compression ratio of x given y

$$\rho_{\mathcal{A}}(x/y) = \liminf_{n\to\infty} \frac{|v_1 v_2 \cdots v_n|}{|\alpha_1 \ldots \alpha_n|}.$$

Deterministic automata with two inputs, one output



Let $\mathcal{A}$ be a deterministic finite automata with two inputs and one output such that for each fixed y, $x \mapsto \mathcal{A}(x, y)$ is one-to-one.
Consider the run of $\mathcal{A}$ for inputs x, y

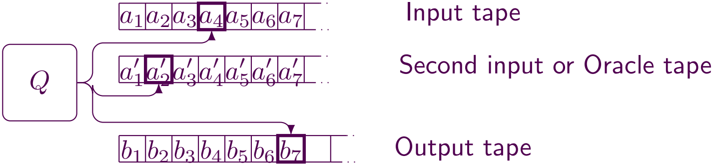
$$p_0 \xrightarrow{\alpha_1, \gamma_1 | v_1} p_1 \xrightarrow{\alpha_2, \gamma_2 | v_2} p_2 \cdots$$

where α_i, γ_i in $A \cup \{\varepsilon\}$, $\alpha_1 \alpha_2 \ldots = x$ and $\gamma_1 \gamma_2 \ldots = y$, $v_i \in A^*$.
The conditional compression ratio of x given y

$$\rho_{\mathcal{A}}(x/y) = \liminf_{n \to \infty} \frac{|v_1 v_2 \cdots v_n|}{|\alpha_1 \ldots \alpha_n|.}$$

$$\rho(x/y) = \inf \{\rho_{\mathcal{A}}(x/y) : \mathcal{A} \text{ is deterministic and one-to-one}\}$$

Deterministic automata with two inputs, one output



Let $\mathcal{A}$ be a deterministic finite automata with two inputs and one output such that for each fixed y, $x \mapsto \mathcal{A}(x, y)$ is one-to-one.
Consider the run of $\mathcal{A}$ for inputs x, y

$$p_0 \xrightarrow{\alpha_1,\gamma_1|v_1} p_1 \xrightarrow{\alpha_2,\gamma_2|v_2} p_2 \cdots$$

where α_i, γ_i in $A \cup \{\varepsilon\}$, $\alpha_1\alpha_2 \ldots = x$ and $\gamma_1\gamma_2 \ldots = y$, $v_i \in A^*$.
The conditional compression ratio of x given y

$$\rho_{\mathcal{A}}(x/y) = \liminf_{n\to\infty} \frac{|v_1 v_2 \cdots v_n|}{|\alpha_1 \ldots \alpha_n|.}$$

$$\rho(x/y) = \inf\{\rho_{\mathcal{A}}(x/y) : \mathcal{A} \text{ is deterministic and one-to-one}\}$$

Notice that it does not depend on the number of symbols read from y.

The definition of independence

Two words x and y are independent if

$$\rho(x) = \rho(x/y) > 0 \text{ and } \rho(y) = \rho(y/x) > 0.$$

Then, y does not help to compress x and x does not help to compress y.

The definition of independence

Two words x and y are independent if

$$\rho(x) = \rho(x/y) > 0 \text{ and } \rho(y) = \rho(y/x) > 0.$$

Then, y does not help to compress x and x does not help to compress y.

Theorem (Becher and Carton 2016)

The set $\{(x, y) : x$ *and* y *are independent*$\}$ *has Lebesgue measure* 1.

The definition of independence

. . . mais il n'est guère vraisemblable qu'un tel définition joue jamais un rôle en mathématiques, car il faudrait pour cela qu'on lui découvre une propriété particulière autre que sa définition.

Émile Borel, La définition en mathématiques,
Les grands courants de la pensée mathématique,
Cahiers du Sud, Paris 1948

Normal words

Normality is the most basic form of randomness, given by Borel in 1909.

Normal words

Normality is the most basic form of randomness, given by Borel in 1909.

Let A be an alphabet. An infinite word x is normal if all blocks of symbols of the same length occur in x with the same limiting frequency.

Normal words

Normality is the most basic form of randomness, given by Borel in 1909.

Let A be an alphabet. An infinite word x is normal if all blocks of symbols of the same length occur in x with the same limiting frequency.

Not normal: $01010101010101010101010101010101010101010101010\ldots$

Normal words

Normality is the most basic form of randomness, given by Borel in 1909.

Let A be an alphabet. An infinite word x is normal if all blocks of symbols of the same length occur in x with the same limiting frequency.

Not normal: $0101010101010101010101010101010101010101010\ldots$
Champernowne's example: $01234567891011121314151617181920 2\ldots$

Normal words

Normality is the most basic form of randomness, given by Borel in 1909.

Let A be an alphabet. An infinite word x is normal if all blocks of symbols of the same length occur in x with the same limiting frequency.

Not normal: $010101010101010101010101010101010101010101010\ldots$
Champernowne's example: $0123456789101112131415161718192021\ldots$

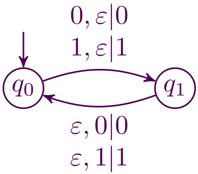
Theorem (Schnor, Stimm 1972; Dai,Lothrup,Lutz,Mayordomo 2004; Heiber,Becher 2012)

An infinite word x is normal if and only if it is incompressible by one-to-one finite automata.

Shuffling

A shuffler is a deterministic finite automaton with two inputs and one output, whose transitions are of the form $p \xrightarrow{a,\varepsilon|a} q$ or $p \xrightarrow{\varepsilon,a|a} q$ (for each state p, all outgoing transitions are of the same type).

The simplest shuffler computes the join:



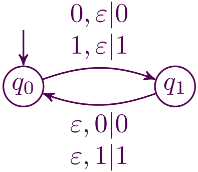
$$x = 0011010001...$$

$$y = 0100011000...$$

Shuffling

A shuffler is a deterministic finite automaton with two inputs and one output, whose transitions are of the form $p \xrightarrow{a,\varepsilon|a} q$ or $p \xrightarrow{\varepsilon,a|a} q$ (for each state p, all outgoing transitions are of the same type).

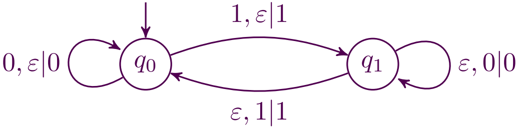
The simplest shuffler computes the join:



Input words $\begin{cases} x = 0011010001... \\ y = 0100011000... \end{cases}$

Output word $00011010001101000010...$

A shuffler



Input $\quad \overline{0011010001}\cdots$

Oracle $\quad \underline{01000110001}\cdots,$

Output $\quad \overline{001}\underline{01}\overline{1}\underline{0001}\overline{01}\underline{1}\overline{0001}\underline{0001}\cdots$

It alternates blocks of 0s followed by a 1, from each word.

Shuffling

Theorem (Alvarez, Becher, Carton 2016)

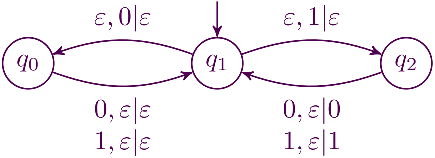
Two normal words x and y are independent if and only if, for every shuffler $\mathcal{S}$, the result $\mathcal{S}(x, y)$ is also normal.

Selecting

A selector is a deterministic finite automaton with two inputs and one output, whose transitions are of the form, for any two symbols $a, b \in A$,

$$p \xrightarrow{a,\varepsilon|a} q \text{ or } p \xrightarrow{a,\varepsilon|\varepsilon} q \text{ or } p \xrightarrow{\varepsilon,b|\varepsilon} q.$$

(all outgoing transitions from a given state are of the same type).



It selects symbols from x at positions where there is a 1 in y.

Selecting

Theorem (Alvarez, Becher, Carton 2016)

Two normal words x and y are independent if and only if for any selector $\mathcal{S}$, the result $\mathcal{S}(x, y)$ is also normal.

Selecting

Theorem (Alvarez, Becher, Carton 2016)

Two normal words x and y are independent if and only if for any selector $\mathcal{S}$, the result $\mathcal{S}(x, y)$ is also normal.

Agafonov, 1968, proved that selection by any finite automaton preserves normality.

Construction of independent normal words

Theorem (Alvarez, Becher, Carton 2016)

For every alphabet A, there is an algorithm that computes a pair of independent normal words.

Open problems

Construct independent normal words in polynomial time.

Open problems

Construct independent normal words in polynomial time.

Given a normal word y, construct x independent of y.

Open problems

Consider the combinatorial definition of normality: A real x is normal if and only if every block of digits of the same size appears with the same frequency. Characterize independence in terms of combinatorics.

Open problems

Consider the combinatorial definition of normality: A real x is normal if and only if every block of digits of the same size appears with the same frequency. Characterize independence in terms of combinatorics.

Consider the characterization of normaliy in terms of u.d: A real x is normal to base b if and only if the sequence $(b^n x)_{n\geq 0}$ is u.d. modulo 1. Characterize independence as uniform distribution modulo 1.

Future Work

Develop the notion of independence for finite sets.

Future Work

Develop the notion of independence for finite sets.

Develop the notion of independence of normality for shift spaces.

Future Work

Develop the notion of independence for finite sets.

Develop the notion of independence of normality for shift spaces.

The End