Independence of normal numbers

Olivier Carton

IRIF
Université Paris Diderot & CNRS

Join work with Verónica Becher and Pablo Heiber
(Universidad de Buenos Aires & CONICET)

Work supported by LIA Infinis

ANR Fractals and Numeration

Outline

Expansion of real numbers

Fix an integer base $b \geqslant 2$. The alphabet is $A = \{0, 1, \ldots, b-1\}$.

- if $b = 2$, $A = \{0, 1\}$,
- if $b = 10$, $A = \{0, 1, 2, \ldots, 9\}$.

Each real number $\xi \in [0, 1)$ has an expansion in base b:
$x = a_1 a_2 a_3 \cdots$ where $a_i \in A$ and

$$\xi = \sum_{k \geq 1} \frac{a_k}{b^k}.$$

In the rest of this talk:

real number $\xi \in [0, 1)$	$\longleftrightarrow$	infinite word $x \in A^\omega$
$1/3$	$\longleftrightarrow$	$010101 \cdots = (01)^\omega$
$\pi/4$	$\longleftrightarrow$	$110010010000111 \cdots$

Normality (Borel 1909)

The number of occurrences of a word u in a word w is

$$\mathrm{occ}(w,u) = |\{i : w[i..i+|u|-1] = u\}|$$

An infinite word $x \in A^\omega$ (resp. a real number ξ) is simply normal (in base b) if for any $a \in A$,

$$\lim_{n\to\infty} \frac{\mathrm{occ}(x[1..n],a)}{n} = \frac{1}{b}.$$

An infinite word $x \in A^\omega$ (resp. a real number ξ) is normal (in base b) if for any $u \in A^*$,

$$\lim_{n\to\infty} \frac{\mathrm{occ}(x[1..n],u)}{n} = \frac{1}{b^{|u|}}.$$

In base $b = 2$, this means

- the frequencies in x of the 2 digits 0 and 1 are $1/2$,
- the frequencies in x of the 4 words $00, 01, 10, 11$ are $1/4$,
- the frequencies in x of the 8 words $000, 001, \ldots, 111$ are $1/8$,
- ...

Examples

Theorem (Borel 1909)

Almost all real numbers are normal, that is, the measure of the set of normal numbers in $[0,1)$ *is* 1.

Examples

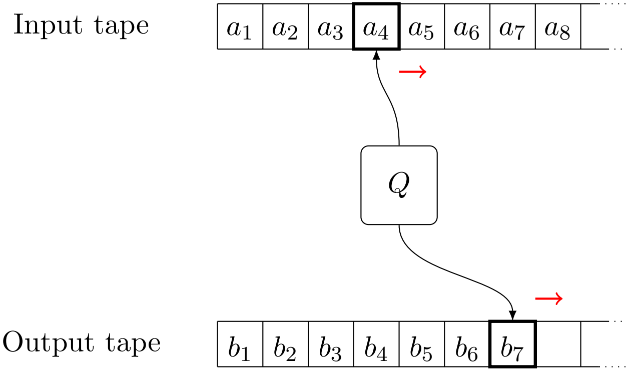
- the infinite word $(001)^\omega = 0010010\cdots$ is not simply normal in base 2,
- the infinite word $(01)^\omega = 01010\cdots$ is simply normal in base 2 but it is not normal,
- the Champernowne word $012345678910111213\cdots$ is normal in base 10.
- the Champernowne word $01\,000110111\,000001010\cdots$ is normal in base 2.

Independence: naive definition

- If $x = a_1 a_2 a_3 \cdots$, then $\text{odd}(x) = a_1 a_3 a_5 \cdots$ and $\text{even}(x) = a_2 a_4 a_6 \cdots$.
- If $x = a_1 a_2 a_3 \cdots$ and $y = b_1 b_2 b_3 \cdots$, then their join $x \vee y$ is $a_1 b_1 a_2 b_2 \cdots$.
- Thus $x = \text{odd}(x) \vee \text{even}(x)$.

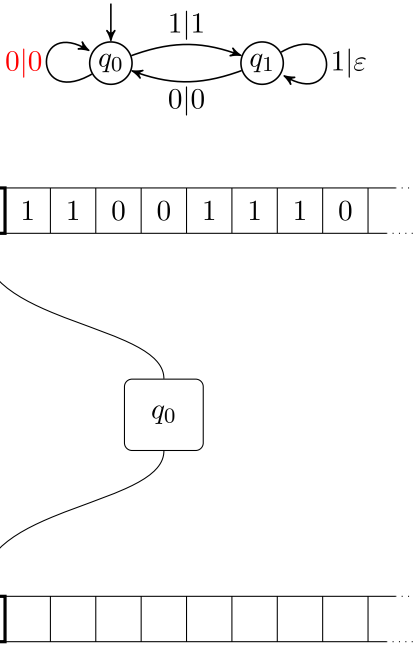
Two words $x = a_1 a_2 a_3 \cdots$ and $y = b_1 b_2 b_3 \cdots$ are independent if their join $x \vee y$ is also normal.
If x is normal, then $\text{odd}(x)$ and $\text{even}(x)$ are independent.
What about $a_1 a_2 b_1 a_3 a_4 b_2 a_5 a_6 b_3 \cdots$?

Transducers

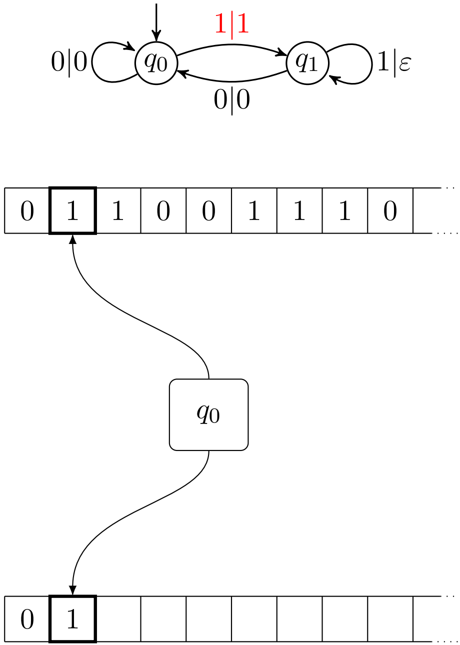


Transitions $p \xrightarrow{a|v} q$ for $a \in A$, $v \in B^*$.

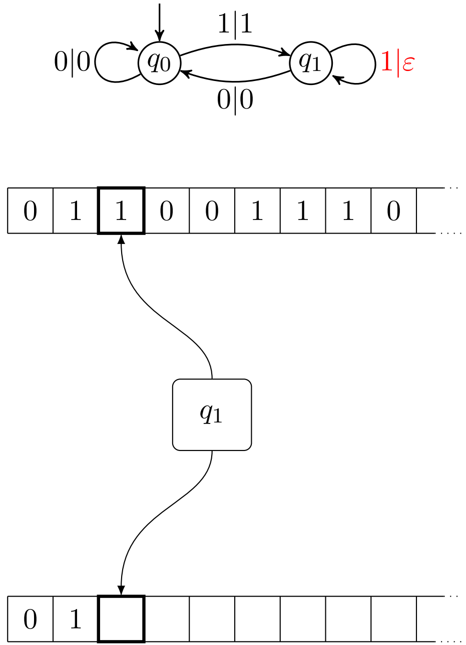
Example



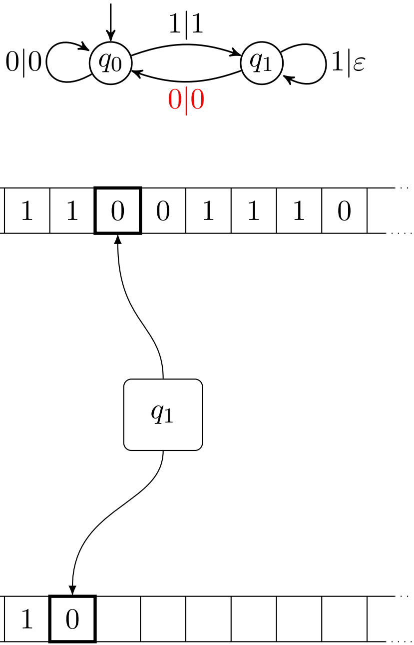
Example



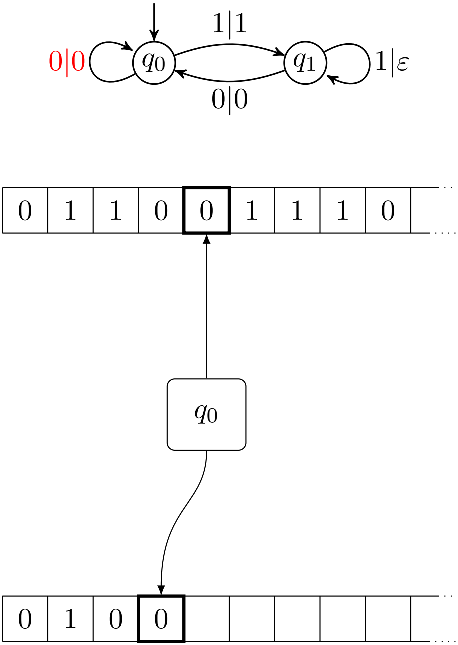
Example



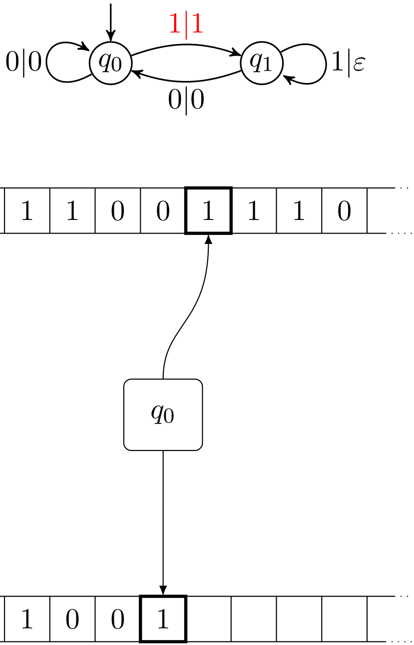
Example



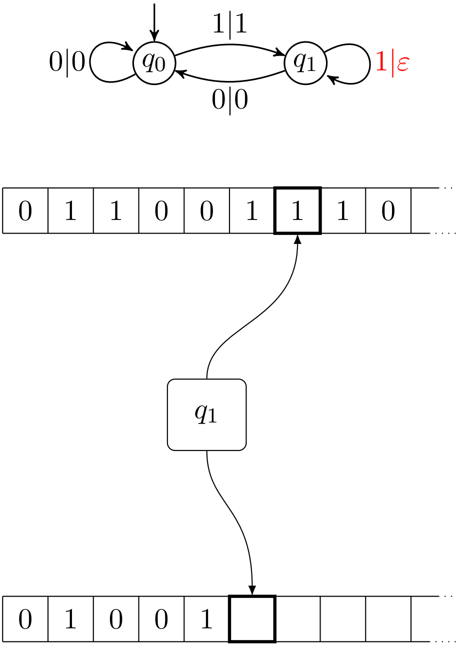
Example



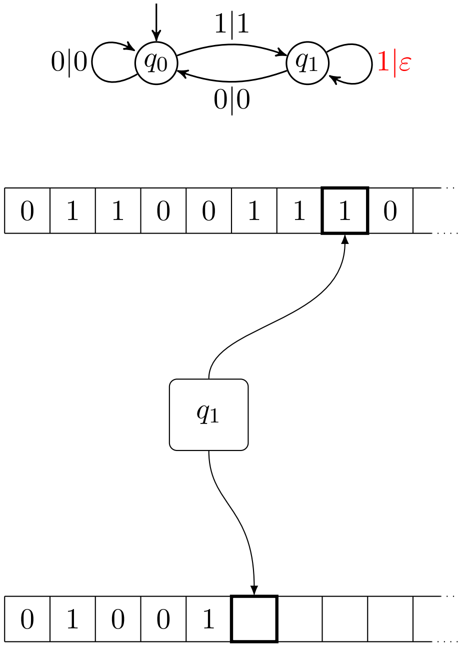
Example



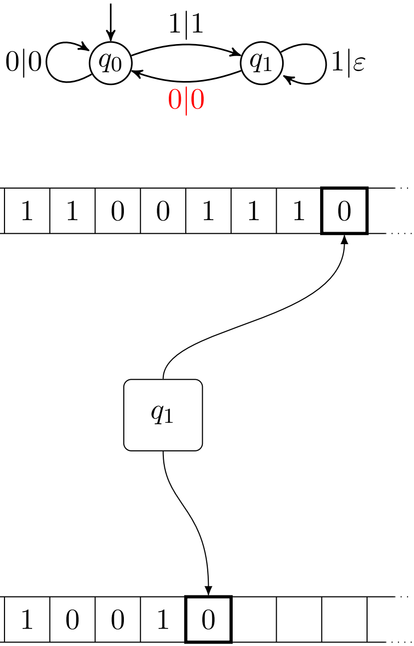
Example



Example



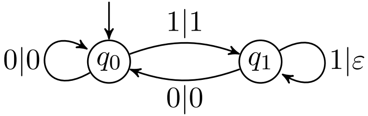
Example



Examples

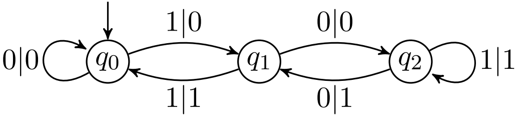
A transducer is an automaton $\mathcal{T} = \langle Q, A, B, \Delta, I, F \rangle$ where Δ is a finite set of transitions $p \xrightarrow{a|v} q$ where $a \in A$ and $v \in A^*$.

Example (Compression of blocks of consecutive 1)



If the input is $010011000111\cdots$, the output is $01001000100\cdots$.

Example (Division by 3 in base 2)



If the input is $(01)^\omega$, the output is $(000111)^\omega$.

Dimension

The compression ratio of the run $q_0 \xrightarrow{a_1|v_1} q_1 \xrightarrow{a_2|v_2} q_2 \xrightarrow{a_3|v_3} \cdots$ in $\mathcal{T}$ with input x

$$\rho_{\mathcal{T}}(x) = \liminf_{n\to\infty} \frac{|v_1 v_2 \cdots v_n| \log|B|}{n \log|A|}.$$

The dimension of an infinite word $x = a_1 a_2 a_3 \cdots$ is

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

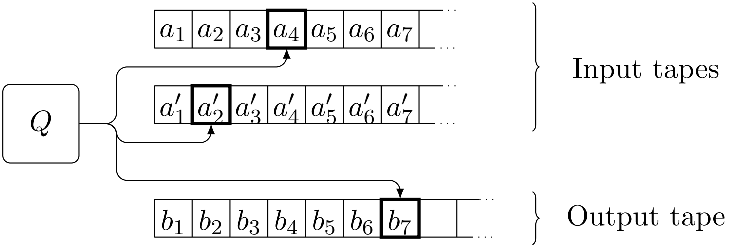
Characterization of normal words

Theorem (Many people)

An infinite word x is normal if and only $\dim(x) = 1$.

- Schnorr and Stimm (1971)
  non-normality $\Leftrightarrow$ finite-state martingale success
- Dai, Lathrop, Lutz and Mayordomo (2004)
  compressibility $\Leftrightarrow$ finite-state martingale success
  normality $\Rightarrow$ no martingale success
- Bourke, Hitchcock and Vinodchandran (2005)
  non-normality $\Rightarrow$ martingale success
- Becher and Heiber (2013)
  non-normality $\Leftrightarrow$ compressibility (direct)
- Becher, Carton and Heiber
  generalized to non-deterministic or two-way transducers

Two input transducers



- The content of the first input tape is the real input.
- The content of the second input tape is used as an oracle.

Transitions

The transition function δ:

$$\begin{aligned}\delta : Q \times A \times A &\to Q \times \{0,1\} \times \{0,1\} \times B^* \\ (p, a, a') &\mapsto (q, d, d', v)\end{aligned}$$

where

- p is the current state and q is the new state,
- a and a' are the two symbols read on the input tapes,
- d and d' are the two moves of the heads on the input tapes,
- v is the word written on the output tape.

Let $x = a_1 a_2 a_3 \cdots$ and $x' = a'_1 a'_2 a'_3 \cdots$ be two infinite words. We write

$$\langle p, m, m' \rangle \xrightarrow{a_m, a'_{m'} | v} \langle q, n, n' \rangle$$

if $\delta(p, a_m, a'_{m'}) = (q, d, d', v)$ and $n = m + d$ and $n' = m' + d'$.

Conditional dimension

A run over x and x' is an infinite sequence of consecutive transitions

$$\langle p_0, m_0, m'_0 \rangle \xrightarrow{a_{m_0}, a'_{m'_0} | v_1} \langle p_1, m_1, m'_1 \rangle \xrightarrow{a_{m_1}, a'_{m'_1} | v_2} \langle p_2, m_2, m'_2 \rangle \cdots$$

where $m_0 = m'_0 = 1$.
Its compression ratio is $\rho_{\mathcal{T}}(x/x')$ is

$$\rho_{\mathcal{T}}(x/x') = \liminf_{n\to\infty} \frac{|v_1 v_2 \cdots v_n|}{m_n}.$$

Note that it does not depend on m'_n.
The conditional dimension of x on y is

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

one-to-one means here that for each y fixed, the function $x \mapsto \mathcal{T}(x, y)$ is one-to-one.

Independence

The two words x and y are independent if they satisfy $\dim(x) = \dim(x/y) > 0$ and $\dim(y) = \dim(y/x) > 0$.

This means that x cannot be compressed better with the help of y and that y cannot be compressed better with the help of x.

Theorem

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

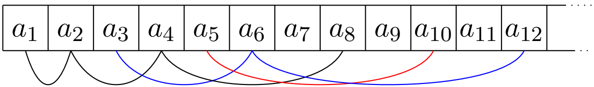
Lemma

For each normal word y, the set $\{x : dim(x/y) < 1\}$ has Lebesgue measure 0.

Stronger than the naive independence

Theorem

There exists a normal word x over a binary alphabet such that $x = \mathrm{even}(x)$, that is $a_{2n} = a_n$ for each $n \geqslant 1$ if $x = a_1 a_2 a_3 \cdots$.



Corollary

There exists a normal word x such that $\mathrm{odd}(x)$ and $\mathrm{even}(x)$ are not independent.

Toeplitz transformation: $x \mapsto T(x)$

$x =$	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}						
	a_1		a_2		a_3		a_4		a_5		a_6		a_7		a_8		a_9	
	a_1	a_1	a_2		a_3	a_2	a_4		a_5	a_3	a_6		a_7	a_4	a_8		a_9	a_5
	a_1	a_1	a_2	a_1	a_3	a_2	a_4		a_5	a_3	a_6	a_2	a_7	a_4	a_8		a_9	a_5
	a_1	a_1	a_2	a_1	a_3	a_2	a_4	a_1	a_5	a_3	a_6	a_2	a_7	a_4	a_8		a_9	a_5

Let $x = a_1 a_2 a_3 \cdots$, then $T(x) = b_1 b_2 b_3 \cdots$ where

$$b_n = a_m \quad \text{if } n = 2^k(2m-1) \text{ for some } k \geqslant 0.$$

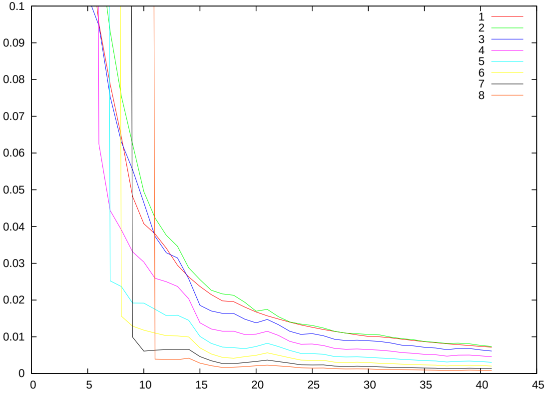
Facts:

- $x = \text{even}(x)$ if and only if $x = T(\text{odd}(x))$.
- There is a normal word x such that $T(x)$ is still normal.
- If $x = \text{even}(x)$, then $T(x)$ is not normal.

Experiments and proofs

Let x be the Champernowne's word $01\,00011011\,000001\cdots$.

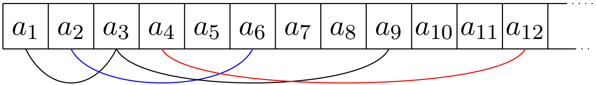
- It seems experimentally that $T(x)$ is normal.



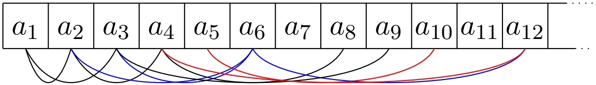
- We have no proof.
- We construct another word such that $x = \text{even}(x)$.

Many questions

- Is there a normal word on a binary alphabet satisfying $x_{3n} = x_n$ for each $n \geqslant 1$.
  We guess yes because experiments are positive but we have no proof.



- Is there a normal word on a binary alphabet satisfying $x_{2n} = x_n$ and $x_{3n} = x_n$ for each $n \geqslant 1$.
  We guess yes because experiments are positive but we have no proof.

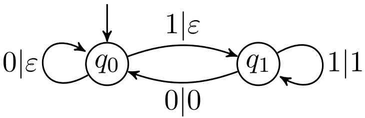


Selecting with finite state control

Let L be a set of finite words.
If $x = a_1 a_2 a_3 \cdots$, then $x \upharpoonright L$ is the word $a_{i_1} a_{i_2} a_{i_3} \cdots$ where $i_1 < i_2 < i_3 \cdots$ and $\{i_1, i_2, i_3, \ldots\}$ is the set $\{i : a_1 \cdots a_{i-1} \in L\}$.

Theorem (Agafonof)

If x is normal and L is rational (accepted by a finite automaton), then $x \upharpoonright L$ is still normal.



Oblivious selector picking each digit after a 1

Input	$x = 00110100011100 \cdots$
Output	$z = 100110 \cdots$

Theorem

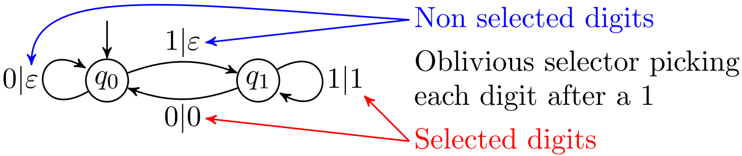
If the selector uses an independent word as an oracle, the output is still normal.

Selecting with finite state control

Let L be a set of finite words.
If $x = a_1 a_2 a_3 \cdots$, then $x \upharpoonright L$ is the word $a_{i_1} a_{i_2} a_{i_3} \cdots$ where $i_1 < i_2 < i_3 \cdots$ and $\{i_1, i_2, i_3, \ldots\}$ is the set $\{i : a_1 \cdots a_{i-1} \in L\}$.

Theorem (Agafonof)

If x is normal and L is rational (accepted by a finite automaton), then $x \upharpoonright L$ is still normal.



Input $x = 00110100011100\cdots$

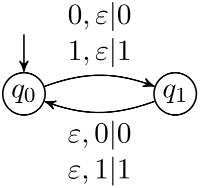
Output $z = 100110\cdots$

Theorem

If the selector uses an independent word as an oracle, the output is still normal.

Shuffling with finite state control

An oblivious shuffler is a deterministic two input transducer which shuffles two input words into a new word. Whether the next digit is taken from either the first or the second input word only depends the current state.



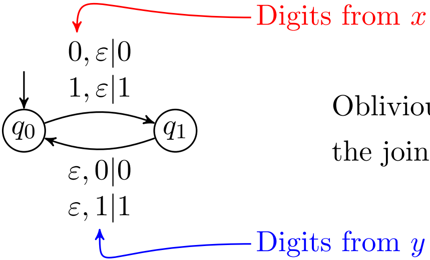
Oblivious shuffler computing the join $x \vee y$

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

Output word $\quad x \vee y = 00011010001101000010\cdots$

Shuffling with finite state control

An oblivious shuffler is a deterministic two input transducer which shuffles two input words into a new word. Whether the next digit is taken from either the first or the second input word only depends the current state.



Oblivious shuffler computing the join $x \vee y$

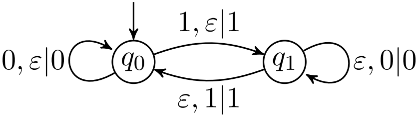
Input words $\begin{cases} x = 0011010001 \cdots \\ y = 0100011000 \cdots \end{cases}$

Output word $x \vee y = 00011010001101000010 \cdots$

Shuffling independent words

Theorem

Shuffing two independent words with finite state control yields a normal word.



Oblivious shuffler

Input words $\begin{cases} x = 001\,1\,01\,0001\ \cdots \\ y = 01\,0001\,1\,0001\ \cdots \end{cases}$

Output word $z = 00101100010110001 0001\cdots$

Open problems

- Give explicitly two independent normal words and even more, provide a Champernowne-like construction for independent normal words.
- Find $x = a_1 a_2 a_3 \cdots$ on a binary alphabet such that $x_{3n} = x_n$.

Thanks