Finite Automata and Randomness

Ludwig Staiger
Martin-Luther-Universität Halle-Wittenberg

Jewels of Automata: from Mathematics to Applications
Leipzig, May, 2015

Outline

Notation: Strings and Languages

Finite Alphabet $X = \{0,\dots,r-1\}$, cardinality $|X| = r$

Finite strings (words) $w = x_1\cdots x_n \in \{0,1\}^*$, $x_i \in \{0,1\}$

Length $|w| = n$

Languages $W \subseteq X^*$

Infinite strings (ω-words) $\xi = x_1\cdots x_n\cdots \in X^\omega$

Prefixes of infinite strings $\xi[0..n] \in X^*$, $\left|\xi[0..n]\right| = n$

ω-Languages $F \subseteq X^\omega$

X^ω as CANTOR space

Metric: $\rho(\eta,\xi) := \inf\{r^{-|w|} : w \in \mathbf{pref}(\eta)\cap\mathbf{pref}(\xi)\}$

Balls: $w\cdot X^\omega = \{\eta : w \in \mathbf{pref}(\eta)\} = \{\eta : w \sqsubset \eta\}$

Diameter: $\operatorname{diam} w\cdot X^\omega = r^{-|w|}$

$\operatorname{diam} F = \inf\{r^{-|w|} : F \subseteq w\cdot X^\omega\}$

Open sets: $W\cdot X^\omega = \bigcup_{w\in W} w\cdot X^\omega$

Closure: (Smallest closed set containing F)
$\mathscr{C}(F) = \{\xi : \mathbf{pref}(\xi) \subseteq \mathbf{pref}(F)\}$

Fact

$F \subseteq X^\omega$ is closed if and only if $\mathbf{pref}(\xi) \subseteq \mathbf{pref}(F)$ implies $\xi \in F$.

Algorithmic Randomness

measure-theoretic paradigm
: An ω-word is random if and only if it is not contained in a constructive null-set.

unpredictability paradigm
: An ω-word is random if and only if no constructive predicting strategy can win against it.

incompressibility (complexity-theoretic) paradigm
: An ω-word is random if and only if one cannot constructively compress infinitely many of its prefixes.

Measure

Measure on base sets: $\mu(w \cdot X^\omega) := r^{-|w|}$

Constructive null-sets: Unions of ω-languages of the form $\bigcap_{n\in\mathbb{N}} V_n \cdot X^\omega$,

where
$V \subseteq \{(v,n) : v \in X^* \wedge n \in \mathbb{N}\}$ is constructive,
$V_n := \{v : (v,n) \in V\}$ and $\mu(V_n \cdot X^\omega) \leq r^{-n}$.

Definition (Randomness)

$\xi \in X^\omega$ is *random* if and only if no constructive null-set contains ξ.

Predicting strategy: Gambling

Our model:

- Playing against an ω-word $\xi \in X^\omega$.
- Gambling strategy $\Gamma : X^* \times X \to [0,1]$ (bet on outcome $x \in X$) $\sum_{x\in X} \Gamma(w,x) \leq 1$ for $w \in X^*$
- yields a (super-)martingale $\mathcal{V}_\Gamma : X^* \to \mathbb{R}_+$
- $\mathcal{V}_\Gamma(\xi[0..n])$ is the capital after the nth round, that is,

$$\mathcal{V}_\Gamma(\xi[0..n]) = r \cdot \Gamma(\xi[0..n], x) \cdot \mathcal{V}_\Gamma(\xi[0..n-1]), \text{ for } \xi(n) = x$$

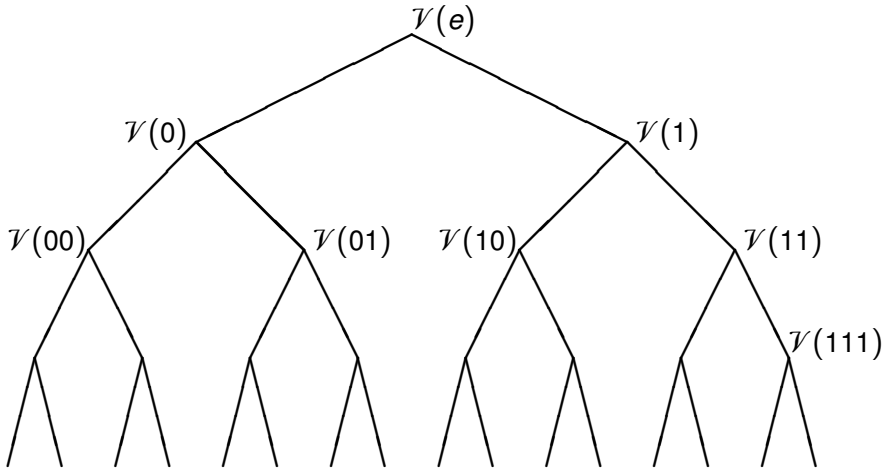
Fact (super-martingale property)

$$\mathcal{V}_\Gamma(w) \geq \tfrac{1}{r} \cdot \textstyle\sum_{x\in X} \mathcal{V}_\Gamma(wx)$$

Definition (Randomness)

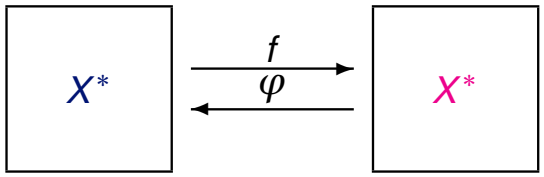
$\xi \in X^\omega$ is *random* if and only if no constructive gambling strategy Γ can win against ξ, that is, $\limsup_{n\to\infty} \mathcal{V}_\Gamma(\xi[0..n]) < \infty$.

Gambling strategies: martingale $\mathcal{V}$



Compression: The Principle of Lossless Compression

text $w \in X^*$ description (*or* program) $\pi \in X^*$



space of texts space of descriptions

f is injective and $\varphi(f(w)) = w$ for all $w \in X^*$

Complexity of w w.r.t. φ: $C_\varphi(w) := \inf\{|\pi| : \varphi(\pi) = w\}$

Definition (Randomness = Incompressibility)

$\xi \in X^\omega$ is *random* if and only if all constructive decompression functions φ satisfy $\exists c \forall n (C_\varphi(\xi[0..n])) \geq n - c$, that is, prefixes of ξ cannot be compressed.

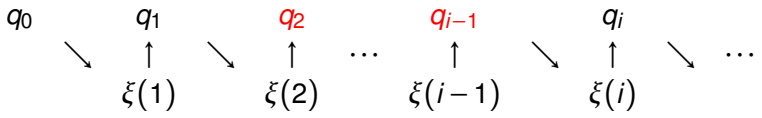
References: Algorithmic Randomness

- Calude, C.S.: *Information and Randomness. An Algorithmic Perspective*, 2nd ed., Springer, Berlin (2002).
- Downey, R., Hirschfeldt D.: *Algorithmic Randomness and Complexity*, Springer, Heidelberg (2010).
- Li M., Vitányi: *An Introduction to Kolmogorov Complexity and Its Applications*, Springer, Berlin (1993).
- Nies, A.: *Computability and Randomness*, Oxford Univ. Press, Oxford (2009).

Automata on ω-words: Büchi-automata

Automaton: $\mathscr{A} = (X, Q, \Delta, q_0, Q_{\text{fin}})$ with
$\Delta \subseteq Q \times X \times Q$, $q_0 \in Q$, $Q_{\text{fin}} \subseteq Q$

Run on ξ: $(q_i)_{i \in \mathbb{N}}$ with $\forall i \geq 0 : (q_i, \xi(i+1), q_{i+1}) \in \Delta$



$\mathscr{A}$ *accepts* ξ: $\exists (q_i)_{i \in \mathbb{N}} \quad \forall i \geq 0 : (q_i, \xi(i+1), q_{i+1}) \in \Delta \quad \wedge$
$\exists^\infty k : q_k \in Q_{\text{fin}}$

$\mathscr{A}$ *accepts* F: $F = \{\xi : \mathscr{A} \text{ accepts } \xi\}$

Regular ω-languages

Definition (Regular ω-language)

An ω-language $F \subseteq X^\omega$ is called *regular* if and only if F is accepted by a finite automaton

Theorem (Büchi 1962)

1. *An ω-language $F \subseteq X^\omega$ is regular if and only if $F = \bigcup_{i=1}^n W_i \cdot V_i^\omega$ for some $n \in \mathbb{N}$ and regular languages $W_i, V_i \subseteq X^*$.*
2. *The set of regular ω-languages over X is closed under Boolean operations.*

Regular null-sets

Theorem (*St'76,St'98*)

Let F be a regular ω-language.

1. *If F is closed then $\mu(F) = 0$ if and only if there is word $w \in X^*$ such that*
$$F \subseteq X^\omega \setminus X^* \cdot w \cdot X^\omega .$$
2. *$\mu(F) = 0$ if and only if*
$$F \subseteq \bigcup_{w \in X^*} X^\omega \setminus X^* \cdot w \cdot X^\omega .$$

Remark

This theorem holds for a much larger class of finite measures on X^ω.

Definition (Randomness = Disjunctivity)

An ω-word $\xi \in X^\omega$ is called *disjunctive* (or *rich* or *saturated*) if and only if it contains every word $w \in X^*$ as subword (infix) [$\mathbf{infix}(\xi) = X^*$].

Partial randomness: Subword complexity

Definition (Asymptotic subword complexity)

$$\tau(\xi) := \limsup_{n\to\infty} \frac{\log_r |\mathbf{infix}(\xi) \cap X^n|}{n}$$

$$\mathbf{infix}(\xi) \cap X^{n+m} \subseteq (\mathbf{infix}(\xi) \cap X^n) \cdot (\mathbf{infix}(\xi) \cap X^m)$$

Fact

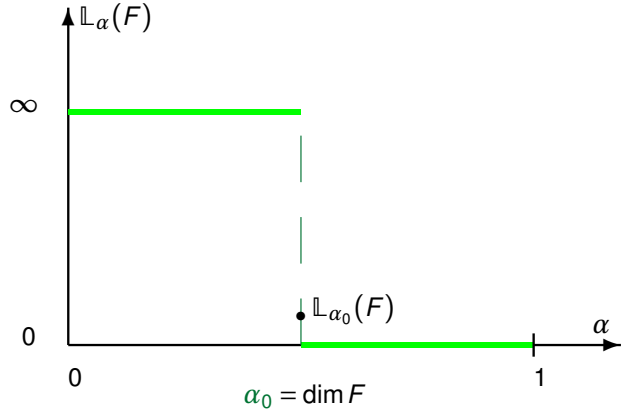
The limit exists and equals $\tau(\xi) = \inf\left\{\frac{\log_r |\mathbf{infix}(\xi)\cap X^n|}{n} : n \in \mathbb{N}\right\}$.

Proposition

$0 \le \tau(\xi) \le 1$ *and an ω-word $\xi \in X^\omega$ is disjunctive if and only if* $\tau(\xi) = 1$.

Hausdorff dimension I

$$\mathbb{L}_\alpha(F) := \lim_{n\to\infty} \inf\Big\{\sum_{v\in V} r^{-\alpha\cdot|v|} : F \subseteq \bigcup_{v\in V} v\cdot X^\omega \wedge \min_{v\in V}|v| \ge n\Big\}$$



$$\dim F := \inf\{\alpha : \mathbb{L}_\alpha(F) = 0\} = \sup\{\alpha : \mathbb{L}_\alpha(F) = \infty\}$$

Hausdorff dimension II

Fact

1. $\dim \bigcup_{i\in\mathbb{N}} F_i = \sup\{\dim F_i : i \in \mathbb{N}\}$ *and* $\dim\{\xi\} = 0$
2. *If* $\mu(F) > 0$ *then* $\dim F = 1$.
3. *If F is regular then* $\dim F = 1$ *implies* $\mu(F) > 0$.

Fact

$\mathbb{Q} \subset \{\dim F : F$ *is a regular ω-language*$\}$

Partial randomness: The hierarchy

Lemma

If $F \subseteq X^\omega$ is a regular ω-language and $\xi \in F$ then $\tau(\xi) \leq \dim F$.

Theorem

1. $\tau(\xi) = \inf\{\dim F : \xi \in F \wedge F \text{ is a regular } \omega\text{-language}\}$
2. *If $\alpha = \dim F$ for some regular ω-language then there is a ξ such that $\tau(\xi) = \alpha$.*
3. *For all $\alpha, \gamma, 0 \leq \alpha < \gamma \leq 1$, the level sets $F_\alpha^{(\tau)} := \{\xi : \tau(\xi) \leq \alpha\}$ satisfy $F_\alpha^{(\tau)} \subset F_\gamma^{(\tau)}$.*

Open question

Does there, for every $\alpha, 0 \leq \alpha \leq 1$, exist a ξ with $\tau(\xi) = \alpha$.

References: Automata and Measure

- Staiger, L.: Reguläre Nullmengen, *Elektron. Informationsverarb. Kybernet.* EIK 12: 307–311 (1976).
- Staiger, L.: Kolmogorov complexity and Hausdorff dimension. *Inform. and Comput.*, 103(2):159–194, (1993).
- Staiger, L.: Rich ω-words and monadic second-order arithmetic. In Mogens Nielsen and Wolfgang Thomas, editors, *Computer Science Logic (Aarhus, 1997)*, LNCS 1414, Springer, 478–490 (1998).
- Staiger, L.: Asymptotic Subword Complexity, In *Languages Alive 2012*, LNCS 7300, Springer, 236–245 (2012).

Gambling finite automaton

Definition (Betting automaton)

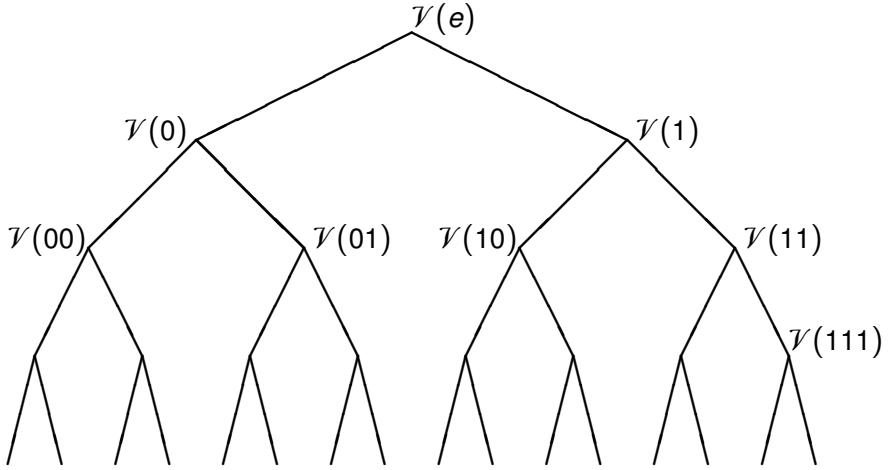
$\mathscr{A} = [X, Q, \mathbb{R}_{\geq 0}, q_0, \delta, \nu]$ is a finite-state betting automaton : $\Longleftrightarrow$

1. S is a finite set (of states), $q_0 \in Q$,
2. $\delta : Q \times X \to Q$,
3. $\nu : Q \times X \to \mathbb{R}_{\geq 0}$ and $\sum_{x \in X} \nu(q, x) \leq 1$, for all $q \in Q$.

Definition (Capital function of $\mathscr{A}$)

$$\begin{aligned} \mathcal{V}_{\mathscr{A}}(e) &:= 1, \text{ and} \\ \mathcal{V}_{\mathscr{A}}(wx) &:= r \cdot \nu(\delta(q_0, w), x) \cdot \mathcal{V}_{\mathscr{A}}(w) \end{aligned}$$

Again: Gambling strategies: martingale $\mathcal{V} = \mathcal{V}_{\mathscr{A}}$



BOREL normality

Definition

An ω-word $\xi \in X^\omega$ is BOREL *normal* iff every subword (infix) $w \in X^*$ appears with the same frequency.

$$\forall w \Big(\lim_{n\to\infty} \frac{|\{i : i \le n \wedge \xi[0..i] \in X^* \cdot w\}|}{n} \Big) = r^{-|w|}$$

Fact

Every BOREL *normal* ω*-word is disjunctive.*

Example

The ω-word $\eta = \prod_{w\in X^*} 0^{|w|} \cdot w$ is disjunctive but not BOREL normal.

The Theorem of SCHNORR and STIMM

Theorem (SCHNORR and STIMM '72)

If $\xi \in X^\omega$ is BOREL *normal then for every finite automaton $\mathscr{A}$ it holds*

1. $\forall^\infty n (n \in \mathbb{N} \to \mathcal{V}_{\mathscr{A}}(\xi[0..n]) = \mathcal{V}_{\mathscr{A}}(\xi[0..n+1]))$, *or*
2. $\exists \rho (0 \le \rho < 1 \wedge \forall^\infty n (n \in \mathbb{N} \to \mathcal{V}_{\mathscr{A}}(\xi[0..n]) \le \rho^n))$.

If $\xi \in X^\omega$ is ***not*** BOREL *normal then there are a finite automaton $\mathscr{A}$ and $\rho > 1$ such that*

3. $\forall^\infty n (n \in \mathbb{N} \to \mathcal{V}_{\mathscr{A}}(\xi[0..n]) \ge \rho^n)$.

Partial Randomness: Finite-state dimension [DAI ET AL.'04]

Finite-state dimension tries to measure, for $\xi \in X^\omega$, the largest exponent α with

$$\mathcal{V}_{\mathscr{A}}(\xi[0..n]) \approx r^{\alpha \cdot n + o(n)}.$$

for some finite automaton $\mathscr{A}$ *'best fitted'* to ξ.

More precisely, $\dim_{FS}(\xi) = 1 - \alpha :\iff$

$$\exists \mathscr{A} \big(\mathcal{V}_{\mathscr{A}}(\xi[0..n]) \ge_{i.o.} r^{\alpha' \cdot n + o(n)} \quad \text{for } \alpha' < \alpha \big) \text{, and}$$

$$\forall \mathscr{A} \big(\mathcal{V}_{\mathscr{A}}(\xi[0..n]) \le r^{\alpha' \cdot n + o(n)} \quad \text{for } \alpha' > \alpha \big).$$

Observe

The higher the dimension $\dim_{FS}(\xi)$ the '*more random*' the ω-word.

Finite-state dimension: The hierarchy

$$\dim_{FS}(F) := \sup\{\dim_{FS}(\xi) : \xi \in F\}$$

Fact

1. $0 \le \dim_{FS}(\xi) \le \tau(\xi) \le 1$.
2. $\xi \in X^\omega$ *is* BOREL *normal if and only if* $\dim_{FS}(\xi) = 1$
3. $\dim_{FS}(F) \ge \dim F$

Theorem

Let $F \subseteq X^\omega$ be a regular ω-language. Then the following hold.

1. *There is a $\xi \in F$ such that* $\dim_{FS}(\xi) = \dim F$.
2. $\dim_{FS}(F) = \dim F$
3. $\mathbb{Q} \subset \{\dim_{FS} F : F \text{ is a regular } \omega\text{-language}\}$

Finite-state dimension: Frequency

Let $h(\alpha) := -\alpha \cdot \log_2 \alpha - (1-\alpha) \cdot \log_2(1-\alpha)$ be the binary SHANNON entropy and let

$$\mathrm{FREQ}(\alpha) := \left\{\xi : \xi \in \{0,1\}^\omega \wedge \lim_{n\to\infty} \frac{|\xi[0..n]|_1}{n} = \alpha\right\}$$

Theorem (DAI ET AL.'04)

Let $\alpha \in [0,1]$ be rational. Then the following hold.

1. *There is an ω-word $\xi \in X^\omega$ having $\dim_{FS}(\xi) = \alpha$, and*
2. $\dim_{FS}(\mathrm{FREQ}(\alpha)) = \dim \mathrm{FREQ}(\alpha) = h(\alpha)$.

Predicting automaton

- Playing against an ω-word $\xi \in X^\omega$.
- Knowing $\xi[0..n-1]$ predict the next symbol $\xi(n)$ or Skip.
- Predict infinitely often.
- All but finitely many precictions have to be correct!

Definition (Predicting automaton)

$\mathscr{A} = [X, Q, q_0, \delta, \lambda]$ is a finite-state predicting automaton : $\Longleftrightarrow$

1. Q is a finite set (of states), $q_0 \in Q$,
2. $\delta : Q \times X \to Q$,
3. $\lambda : Q \to X^*$. [e – empty word, that is, Skip]

Prediction

Definition (Tadaki '14)

A predicting automaton $\mathscr{A} = [X, Q, q_0, \delta, \lambda]$ *predicts* $\xi \in X^\omega$ if and only if there is an $n_\xi \in \mathbb{N}$ such that

1. $\lambda(\delta(q_0, \xi[0..n-1])) = \xi(n)$ for infinitely many $n \geq n_\xi$, and
2. if $\lambda(\delta(q_0, \xi[0..n-1])) \neq \xi(n)$ then $\lambda(\delta(q_0, \xi[0..n-1])) = e$.

Theorem

Let $\mathscr{A} = [X, Q, q_0, \delta, \lambda]$ be a predicting automaton.

1. *If $\mathscr{A}$ predicts ξ then ξ is not disjunctive.*
2. *If, moreover, $X = \{0,1\}$ then every non-disjunctive ξ is predicted by some automaton $\mathscr{A}_\xi$.*

Weak Prediction

Definition

A predicting automaton $\mathscr{A} = [X, Q, q_0, \delta, \lambda]$ *weakly predicts* $\xi \in X^\omega$ if and only if there is an $n_\xi \in \mathbb{N}$ such that

1. $\lambda(\delta(q_0, \xi[0..n-1])) \in X$ for infinitely many $n \geq n_\xi$, and
2. if $\lambda(\delta(q_0, \xi[0..n-1])) \in X$ then $\lambda(\delta(q_0, \xi[0..n-1])) \neq \xi(n)$.

Theorem

An ω-word ξ is weakly predictable by some automaton $\mathscr{A} = [X, Q, q_0, \delta, \lambda]$ if and only if it is non-disjunctive.

Finite-state genericity [AMBOS-SPIES and BUSSE'03]

Let $\mathscr{A} = [X, Q, q_0, \delta, \lambda]$ be a predicting automaton.

Definition

An ω-word $\xi \in X^\omega$ *meets* $\mathscr{A}$ if and only if

$$\xi[0..n] \cdot \lambda(\delta(q_0, \xi[0..n])) \sqsubset \xi$$

for some $n \in \mathbb{N}$.

Theorem

An ω-word ξ is non-disjunctive if and only if it is met by every predicting automaton $\mathscr{A} = [X, Q, q_0, \delta, \lambda]$.

Why does 'genericity ≡ measure' hold?

Definition (AMBOS-SPIES, BUSSE'03)

F is *generic* : $\iff \forall w \exists v \big(v \in X^* \wedge F \cap wv \cdot X^\omega = \emptyset \big)$

Fact

$F \subseteq X^\omega$ is generic if and only if F is nowhere dense in CANTOR *space.*

For regular ω-languages $F \subseteq X^\omega$ the following equivalences between 'measure' and 'genericity' hold ([*St'76, '98*]).

	Measure	**Category (Density)**
very large	$\mu(F) = \mu(X^\omega)$	F is residual (co-meagre)
large	$\mu(F) \neq 0$	F is of 2nd BAIRE category
small	$\mu(F) = 0$	F is of 1st BAIRE category (meagre)
very small	$\mu(\mathscr{C}(F)) = 0$	F is nowhere dense

References: Unpredictability

- Ambos-Spies, K., Busse, E.: Automatic forcing and genericity: On the diagonalization strength of finite automata, *Proceedings of DMTCS 2003*, LNCS 2731, Springer, 97–108 (2003).
- Bourke, C., Hitchcock, J. M., Vinodchandran, N. V.: Entropy rates and finite-state dimension, *Theoretical Computer Science* 349, 3: 392–406 (2005).
- Dai, J.J., Lathrop, J.I, Lutz, J.H., Mayordomo, E.: Finite-state dimension, *Theoretical Computer Science* 310: 1–33 (2004).
- Schnorr, C. P., Stimm, H.: Endliche Automaten und Zufallsfolgen, *Acta Informatica* 1: 345–359 (1972).
- Staiger, L.: Reguläre Nullmengen, *Elektron. Informationsverarb. Kybernet.* EIK 12: 307–311 (1976).
- Staiger, L.: Rich ω-words and monadic second-order arithmetic. In Mogens Nielsen and Wolfgang Thomas, editors, *Computer Science Logic (Aarhus, 1997)*, LNCS 1414, Springer, 478–490 (1998).
- Tadaki, K.: Phase transition and strong predictability. In O. H. Ibarra, L. Kari, and St. Kopecki, editors, *Unconventional Computation and Natural Computation*, LNCS 8553, Springer, 340–352 (2014).

Compression by transducers

Definition

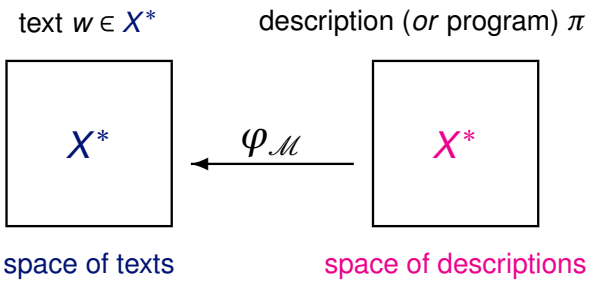
$\mathscr{M} = [X, Y, Q, q_0, \delta, \lambda]$ is a *generalised sequential machine* (or *finite transducer*) : $\iff$

1. S is a finite set (of states), $q_0 \in S$,
2. $\delta : Q \times X \to Q$,
3. $\lambda : Q \times X \to Y^*$.

φ is the mapping related to $\mathscr{M}$ if $\varphi(w) = \lambda(q_0, w)$.

In the sequel we will only consider transducers with $Y = X$.

Compression: Complexity



Complexity of w w.r.t. to the transducer $\mathscr{M}$:

$$C_{\mathscr{M}}(w) := \inf\{|\pi| : \varphi_{\mathscr{M}}(\pi) = w\}$$

The single transducer case [Doty and Moser'06]

Definition (Compression along an input)

$$\vartheta_{\mathscr{M}}(\eta) := \liminf_{n\to\infty} \frac{n}{|\varphi(\eta[0..n])|},$$

where $\mathscr{M}$ is a finite transducer and φ its related mapping.

Let $\overline{\varphi}(\eta) := \lim_{v\to\eta} \varphi(v)$ or $\mathbf{pref}(\overline{\varphi}(\eta)) = \mathbf{pref}(\varphi(\mathbf{pref}(\eta)))$

Theorem

$$\dim_{FS}(\xi) = \inf\{\vartheta_{\mathscr{M}}(\eta) : \mathscr{M} \text{ finite transducer } \wedge \xi = \overline{\varphi}(\eta)\}$$

The case of many transducers [Calude, *St* and Stephan'14]

Denote by $\mathscr{T}$ be the set of all finite transducers.

Definition (Finite-state complexity)

Let $S : X^* \to \mathscr{T}$ be computable enumeration of $\mathscr{T}$. Then

$$C_S(w) := \inf\{|\sigma| + |\pi| : S(\sigma) = \mathscr{M} \wedge \varphi_{\mathscr{M}}(\pi) = w\}$$

is the *finite-state complexity* of the word w w.r.t. the enumeration S.

Here the decompression function $\varphi_{\mathscr{M}}$ is realised by the transducer $\mathscr{M}$, and the size (length) of σ of the transducer $\mathscr{M} = S(\sigma)$ is taken into account.
Observe that there are only $\leq r^{n+1}$ transducers of size $\leq n$.

Enumerations of transducers

Definition (Calude, K. Salomaa and Roblot)

A *perfect enumeration* S of all transducers is a partially computable function with a prefix-free and computable domain mapping each $\sigma \in \mathrm{dom}(S)$ to an admissible transducer $S(\sigma)$ in an onto way.

MARTIN-LÖF randomness

Definition (Martin-Löf random)

An ω-word ξ is MARTIN-LÖF *random* if and only if $\xi \notin \bigcap_{n\in\mathbb{N}} V_n \cdot X^\omega$ for all computably enumerable sets $V \subseteq X^* \times \mathbb{N}$ such that $\mu(V_n \cdot X^\omega) \leq r^{-n}$

Theorem

The following statements are equivalent:

1. *The ω-word ξ is not* MARTIN-LÖF *random;*
2. *There is a perfect enumeration S such that for every $c > 0$ and almost all $n > 0$ we have $C_S(\xi[0..n]) < n - c$;*
3. *There is a perfect enumeration S such that for every $c > 0$ there exists an $n > 0$ with $C_S(\xi[0..n]) < n - c$.*

References: Incompressibility

- Calude, C. S., Salomaa, K., Roblot, T. K.: Finite state complexity, *Theoretical Computer Science* 412: 5668–5677 (2011).
- Calude, C. S., Staiger, L., Stephan, F.: Finite state incompressible infinite sequences, In *Proceedings of TAMC 2014*, LNCS 8402, Springer, 50-66 (2014).
- Doty, D., Moser, P.: Finite-state dimension and lossy compressors, `arxiv:cs/0609096v2` (2006).
- Martin-Löf, P.: The definition of random sequences, *Information and Control* 9: 602-619 (1966).