Logic of information processes

Damian Niwiński

University of Warsaw

Le culture dinanzi a Dio, Rome, June 2013

Hilbert's programme.

Mathematical thinking may involve highly abstract concepts and ideas.

But it eventually produces a **proof**: finite sequence of symbols.

$$\left(x^2 = p \cdot y^2 \ \wedge (\forall z) 1 < z < p \Rightarrow z \perp p\right) \Longrightarrow p|x.$$

$$p|x \ \Rightarrow p^2|x^2. \qquad p^2|p \cdot y^2 \ \Rightarrow p|y^2. \qquad p|y^2 \Rightarrow p|y.$$

If p is prime then $\sqrt{p}$ is irrational.

Everybody knowing few basic principles should be able to **verify** a proof "automatically". *Even computer could do!*

Does there exist an algorithm to **solve** any mathematical conjecture ?



Photo: Jon Callas

Alan Turing discovered an insurmontable barrier to Hilbert's program.

While Hilbert gave a rigorous mathematical definition of **proof**, Turing gave a rigorous mathematical definition of **computation**.

Like Goedel in his Incompleteness Theorem, Turing explored the paradox of self-reference.

> *I am lying.*
>
> *This sentence does not have a proof.*
>
> *This program validates those programs, which fail to validate themselves.*

Photo: Antoine Taveneaux

Like the Carnot engine in thermodynamics, the **universal Turing machine** is an ideal model, which exhibits both strengths and limitation of information processing.

Physical realizations were preceded by the *bombe* designed by Turing in 1939 in order to break the German Enigma code (following a previous construction by Polish cryptologists).

Today Turing is recognized as the father of computer science.

Photo: Stan Shebs

By the end of his life, Turing turned to mathematical biology. In *The Chemical Basis of Morphogenesis* he proposed a mathematical theory of pattern formation.

He was pursuing the Fibonacci pattern in phyllotaxis.

$$\begin{array}{ccccccccccccccccccc} 0 & & 1 & & 1 & & 2 & & 3 & & 5 & & 8 & & 13 & & 21 & & 34 & \ldots \\ & + & & + & & + & & + & & + & & + & & + & & + & & + & \\ & 1 & & 2 & & 3 & & 5 & & 8 & & 13 & & 21 & & 34 & & 55 & & \ldots \end{array}$$

Generating a complex structure from a single *seed* is a paradigmatic situation in mathematics.

$\frac{1}{7} = 0,142857142857142857142857142857142857\ldots$

Thue–Morse sequence

$0 \to 01$

$1 \to 10$

$$
\begin{array}{cccccccccccccccc}
0 & & & & & & & & 1 & & & & & & & \\
0 & & & & 1 & & & & 1 & & & & 0 & & & \\
0 & & 1 & & 1 & & 0 & & 1 & & 0 & & 0 & & 1 & \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & .
\end{array}
$$

01101001100101101001011001101001100101100110100101101001100101 10\ldots

Vincent Van Gogh

A common feature of such generation processes, including computations of Turing machine, which they share with some processes in nature, is that they are largely automatic — $\alpha\upsilon'\tau o\mu\alpha'\tau\eta$ — once triggered, they develop by their own.

$\ldots \kappa\alpha\iota\ o'\ \sigma\pi o'\varrho o\varsigma\ \beta\lambda\alpha\sigma\tau\alpha'\ \kappa\alpha\iota\ \mu\eta\kappa\upsilon'\nu\eta\tau\alpha\iota\ \omega\varsigma\ o\upsilon\kappa\ o\iota\delta\varepsilon\nu\ \alpha\upsilon\tau o'\varsigma$

$\alpha\upsilon'\tau o\mu\alpha'\tau\eta\ \eta'\ \gamma\eta\ \kappa\alpha\varrho\pi o\phi o\varrho\varepsilon\iota\ \pi\varrho\omega\tau o\nu\ \chi o'\varrho\tau o\nu\ \varepsilon\iota\tau\alpha\ \sigma\tau\alpha\chi\upsilon\nu \ldots$

$\ldots\kappa\alpha\iota\ o'\ \sigma\pi o'\rho o\varsigma\ \beta\lambda\alpha\sigma\tau\alpha'\ \kappa\alpha\iota\ \mu\eta\kappa\upsilon'\nu\eta\tau\alpha\iota\ \omega\varsigma\ o\upsilon\kappa\ o\iota\delta\varepsilon\nu\ \alpha\upsilon\tau o'\zeta$

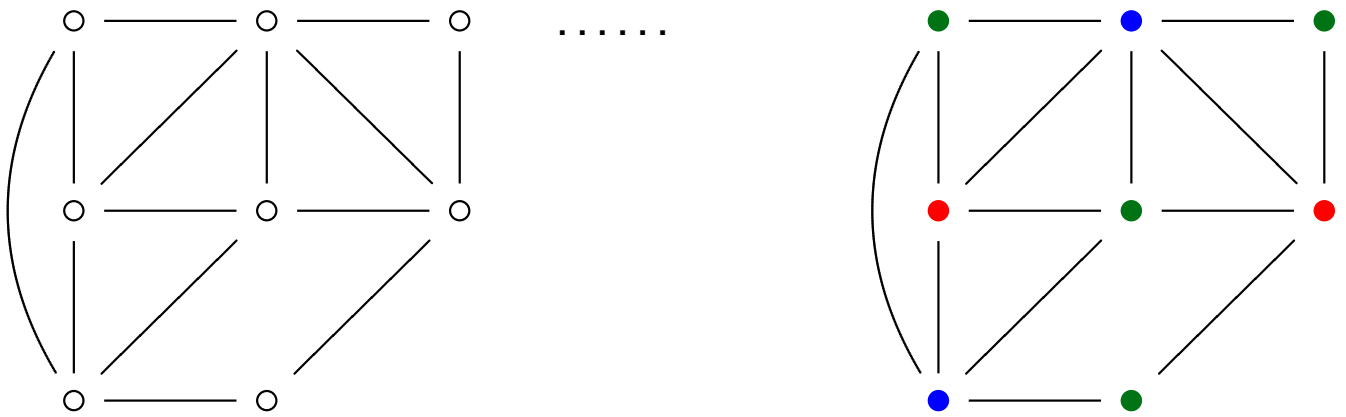
$\alpha\upsilon'\tau o\mu\alpha'\tau\eta\ \eta'\ \gamma\eta\ \kappa\alpha\rho\pi o\phi o\rho\varepsilon\iota\ \pi\rho\omega\tau o\nu\ \chi o'\rho\tau o\nu\ \varepsilon\iota\tau\alpha\ \sigma\tau\alpha\chi\upsilon\nu\ldots$

He also said, 'This is what the kingdom of God is like. A man scatters seed on the land. Night and day, while he sleeps, when he is awake, the seed is sprouting and growing; how, he does not know. Of its own accord the land produces first the shoot, then the ear, then the full grain in the ear. And when the crop is ready, at once he starts to reap because the harvest has come.'

Mark, 4, 26–29.

Whereas ideal computation models do not encounter other barrieres than those discovered by Turing, the real world computer have to face the phenomenon of **computational complexity**.

Can we color this map with 3 colors ?



A *brute force* method requires 3^n tries. For $n = 400$, it amounts to 3^{400}.

A *brute force* method requires 3^n tries. For $n = 400$, it amounts to 3^{400}.

For comparison, the age of universe is

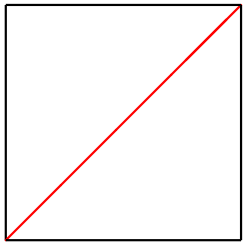
$\approx 10^{20}$ seconds $\approx 10^{60} < 3^{150}$ chronons.

The number of atoms in the universe $\approx 10^{2*39} < 3^{2.5*2*40} = 3^{200}$.

$$3^{150} * 3^{200} < 3^{400}$$

To meet the practical need of solving difficult problems, computer scientists and practitioners developed various techniques: approximation, randomization, fixed-parameter tractability, heuristics. . .

On theoretical side, proving that an efficient algorithm does **not** exists at all appears to be an extremely difficult task. The related **P** $\neq$ **NP** conjecture is among the Clay Institute *Millenium Prize Problems.*



Proving **impossibility** has been a driving force of mathematics since its origin. . .

The *Computational Complexity Theory* has its roots in discoveries of mathematicians from the early 20th century, pursuing various degrees of infinity.

Cantor:	is every subset of a real line either countable or equinumerable with the whole line **?** (*Continuum hypothesis*)
Cantor & Bendixon:	true for closed sets
Alexandrov & Hausdorff:	true for Borel sets
should we	**restrict mathematics to Borel sets ?**

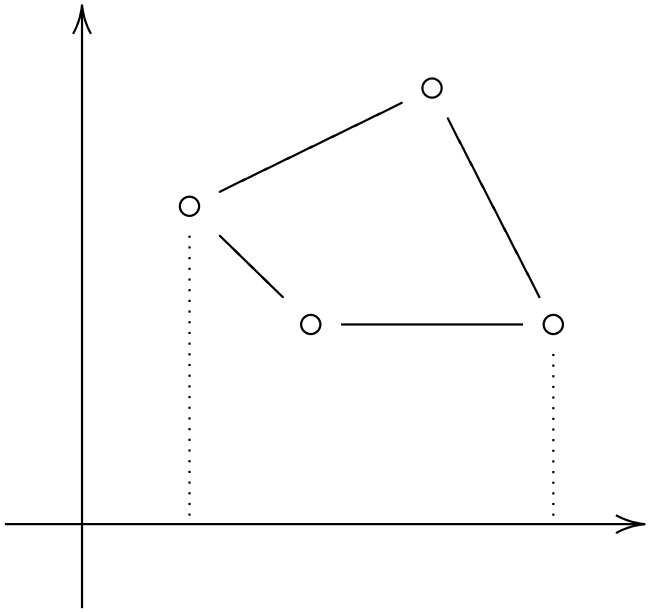
A union of open intervals $(a, b) \subseteq \mathbb{R}$ is open.

Open sets are Borel.

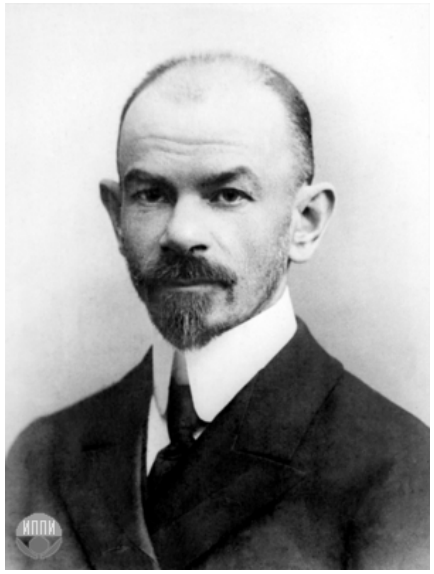
If A is Borel then so is $\mathbb{R} - A$.

If $(A_n)_{n<\omega}$ are open then so are $\bigcup_{n<\omega} A_n$, and $\bigcap_{n<\omega} A_n$.

Lusin, Suslin (1916): projection of a Borel set may be non-Borel !



This discovery gave birth to *Descriptive set theory*, which qualifies sets according to their complexity. Analogously, in *Complexity theory*, the operation of projection leads to the class **NP**.



Dmitri Egorov, the father of the Moscow Mathematical School was accused of *mixing mathematics and religion* and of *participating in a counter-revolutionary organization: the Catacomb Church*. He died in a soviet prison in 1931.

Similar accusations were raised against **Nicolai Lusin** himself. He was saved from inprisonment and death, but lost academic influence and right to teach.

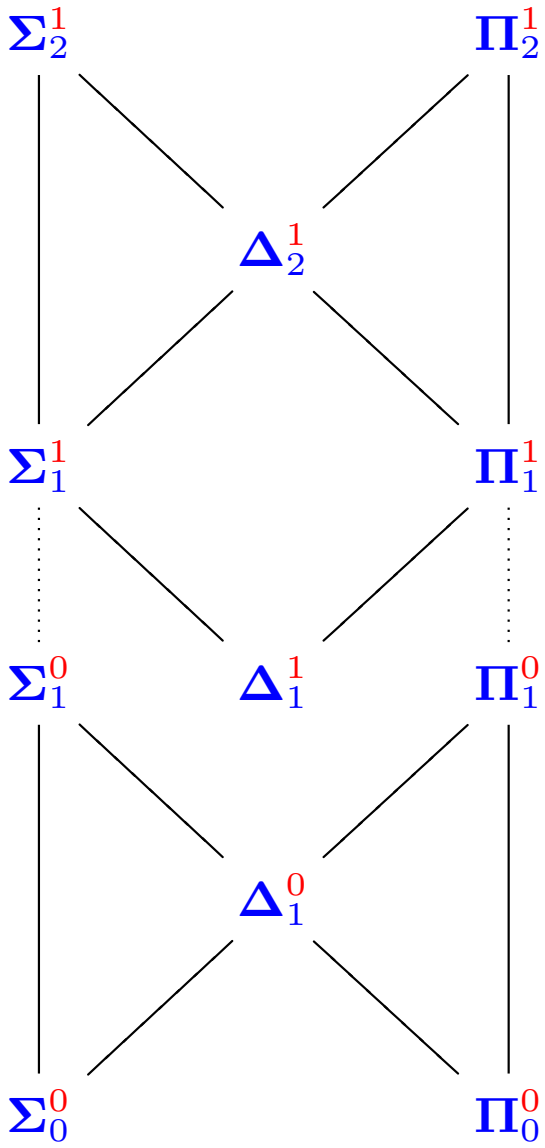
Classical definability theory

1900 Borel, Baire, Lebesgues

1917 Lusin, Suslin

1929 Tarski, Kuratowski

1940 Mostowski, Kleene



An issue which emerged in the 1930s and is of crucial importance for computer science today is **determinacy of games**.

Zermelo 1913 proved that in chess either

White has a winning strategy, or

Black has a winning strategy, or

both parties have the strategies to achieve (at least) a draw.

Not so for infinite games !

as discovered by Banach and Mazur (1930s), and independently Gale and Stewart (1953).

Idea — strategy stealing

White Mr. Kasparov •

Black Mr. Niwiński

White Mr. Niwiński

Black Mr. Karpow

Idea — strategy stealing

White Mr. Kasparov •

Black Mr. Niwiński

White Mr. Niwiński •

Black Mr. Karpow

Idea — strategy stealing

White Mr. Kasparov •

Black Mr. Niwiński

White Mr. Niwiński •

Black Mr. Karpow •

Idea — strategy stealing

White Mr. Kasparov •

Black Mr. Niwiński •

White Mr. Niwiński •

Black Mr. Karpow •

Idea — strategy stealing

White Mr. Kasparov

Black Mr. Niwiński

White Mr. Niwiński

Black Mr. Karpow

Example of undetermined game (cf. Kopczyński & N., 2012)

Let $C_E \cup C_A = \{0,1\}^\omega$ have the property that two sequences that differ in exactly one bit are winning for different players.

$$0011101101101001 \overset{1}{\not} 00101100001011 \ldots\ldots$$

By Axiom of Choice, there exist ($2^{\aleph_0}$ many) such pairs.

Eve	w_0		w_2		w_4			
Adam		w_1		w_3		w_5		

The results of the play is: $W = w_0 w_1 w_2 w_3 w_4 w_5 \ldots$

Eve wins if $W \in C_E$, otherwise Adam wins.

Suppose Adam wins

Eve 0

Adam w_1

Eve $1w_1$

Adam

Suppose Adam wins

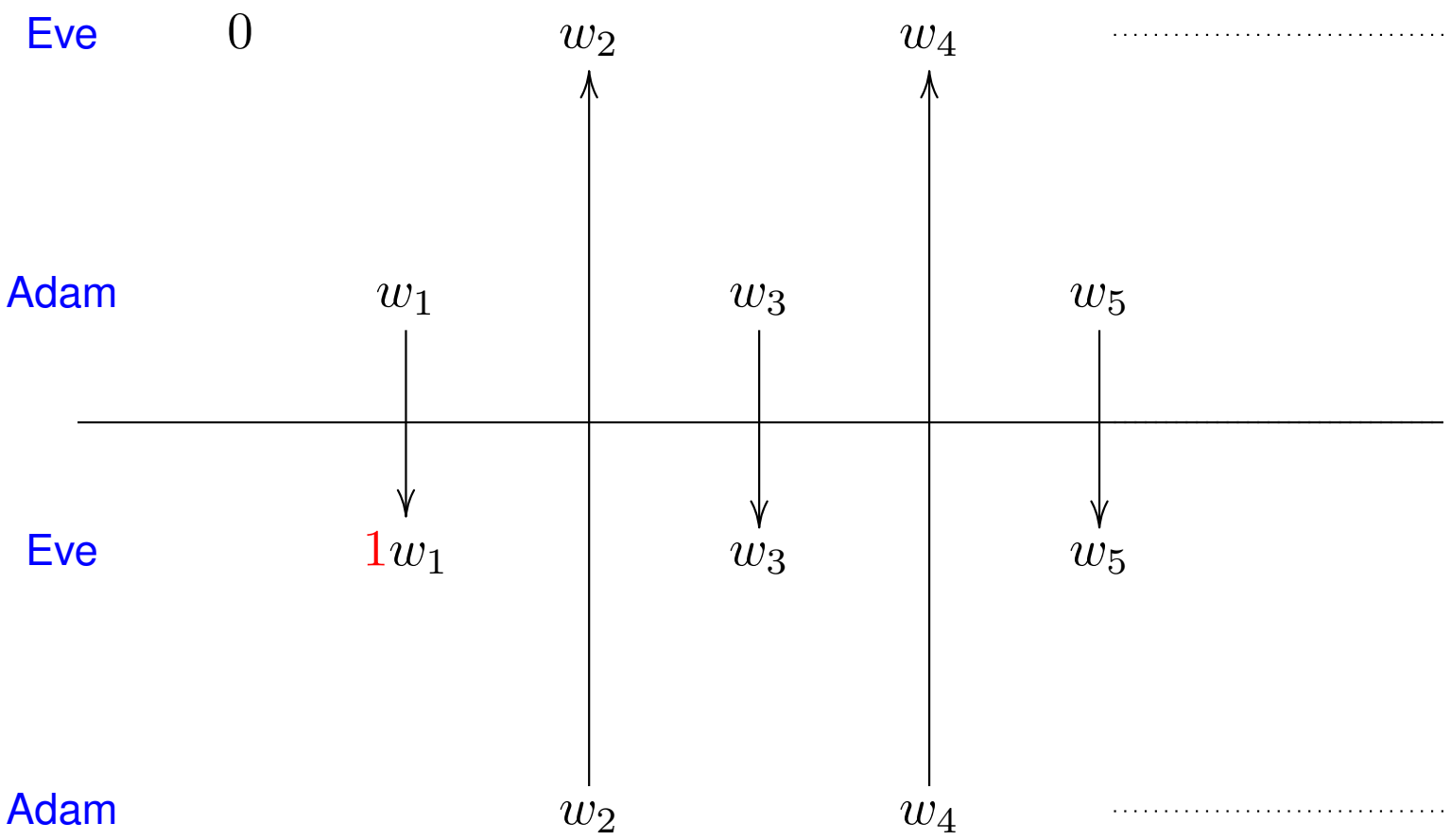
Eve 0

Adam w_1

Eve $1w_1$

Adam w_2

Suppose Adam wins



Suppose Eve wins

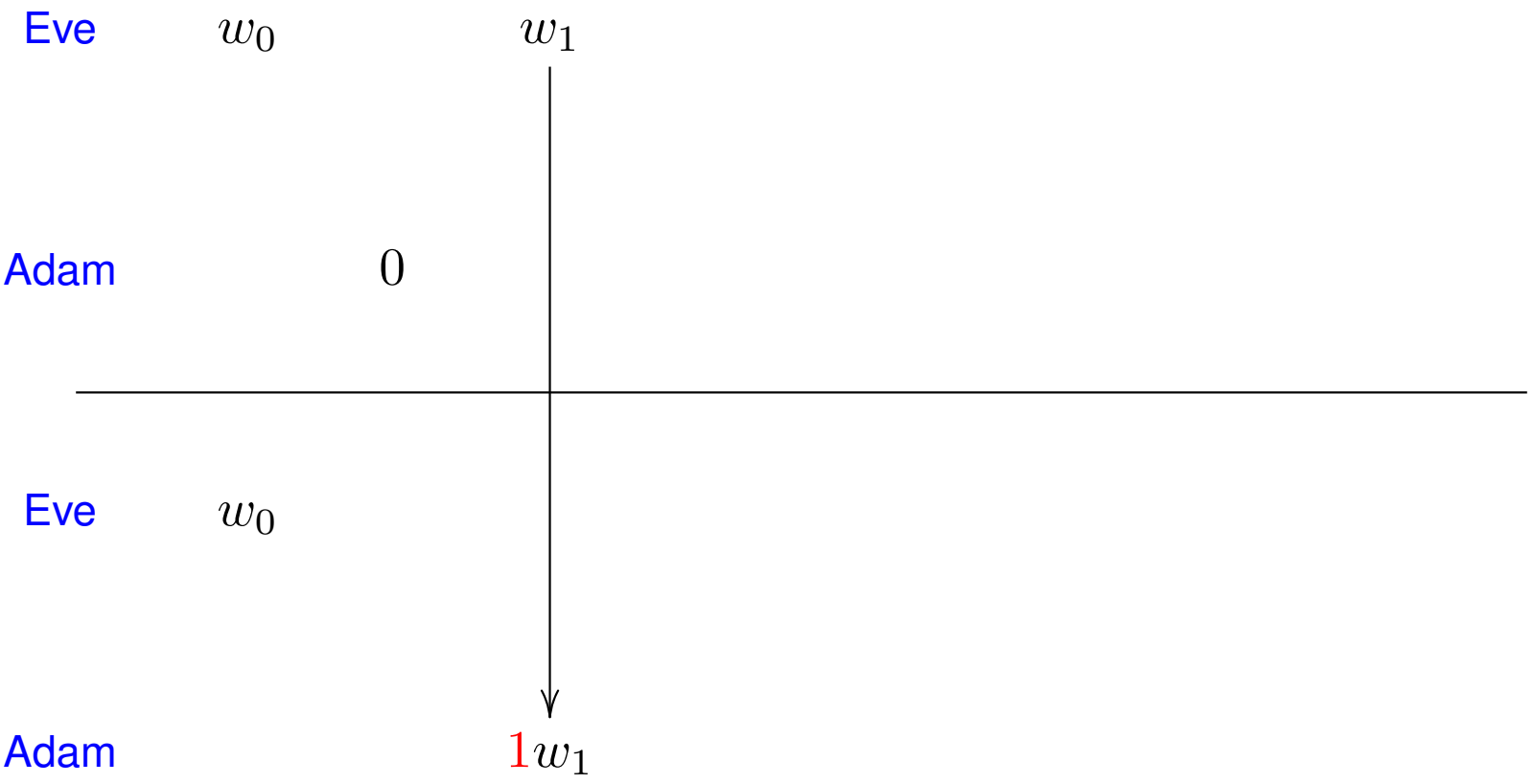
Eve w_0 w_1

Adam 0

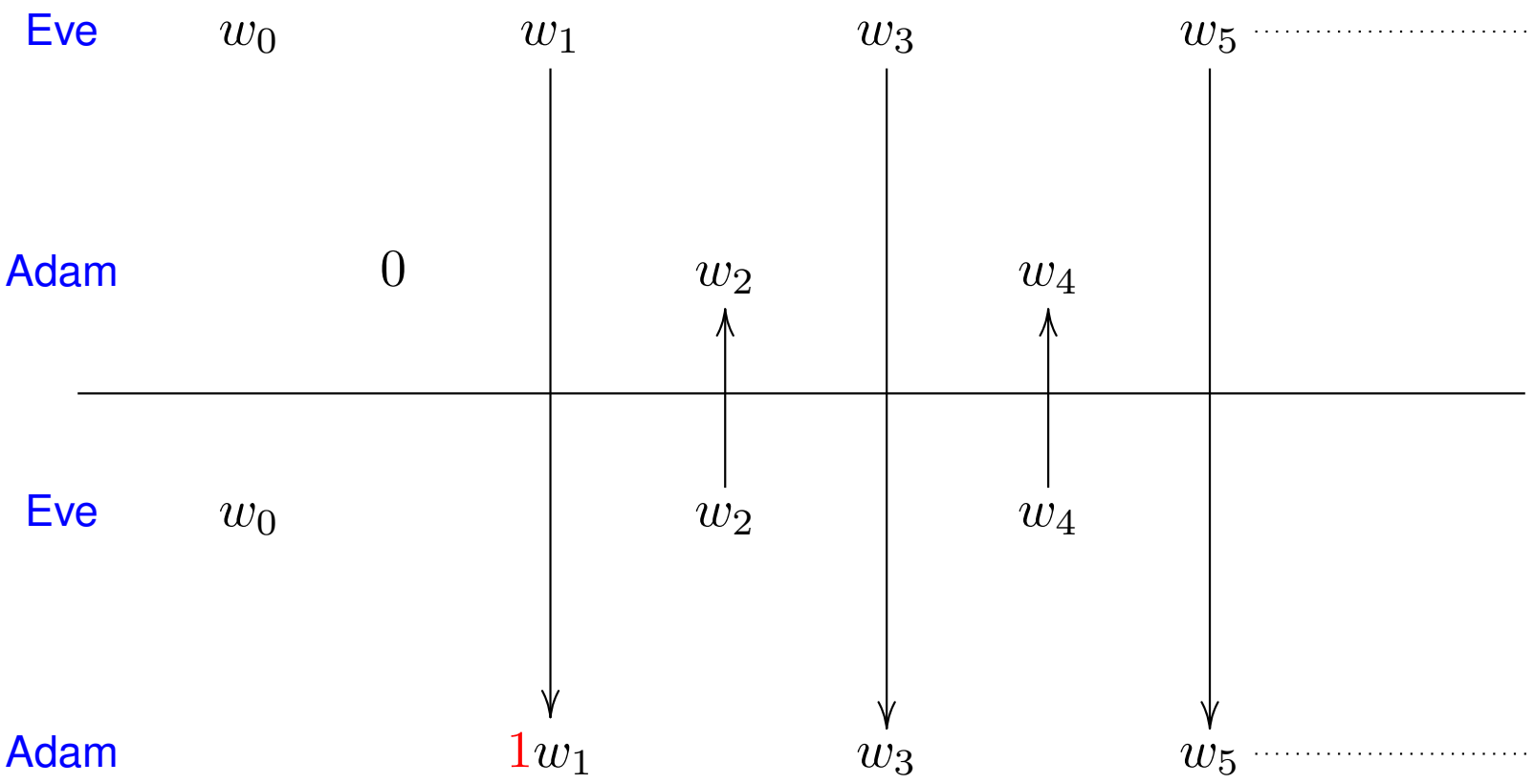
Eve w_0

Adam

Suppose Eve wins



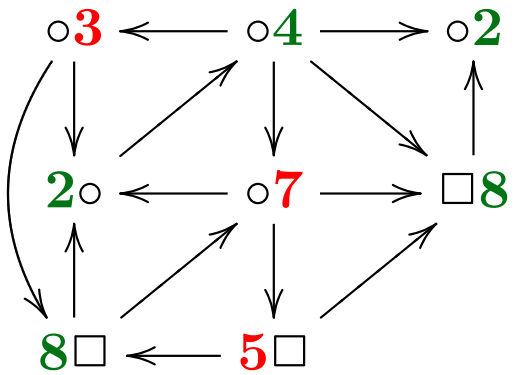
Suppose Eve wins



However, most of “natural” games *are* determined.

By **Martin’s Theorem** (1975), games with **Borel** criteria are always determined.

Games can model interaction of a computer system with environment.

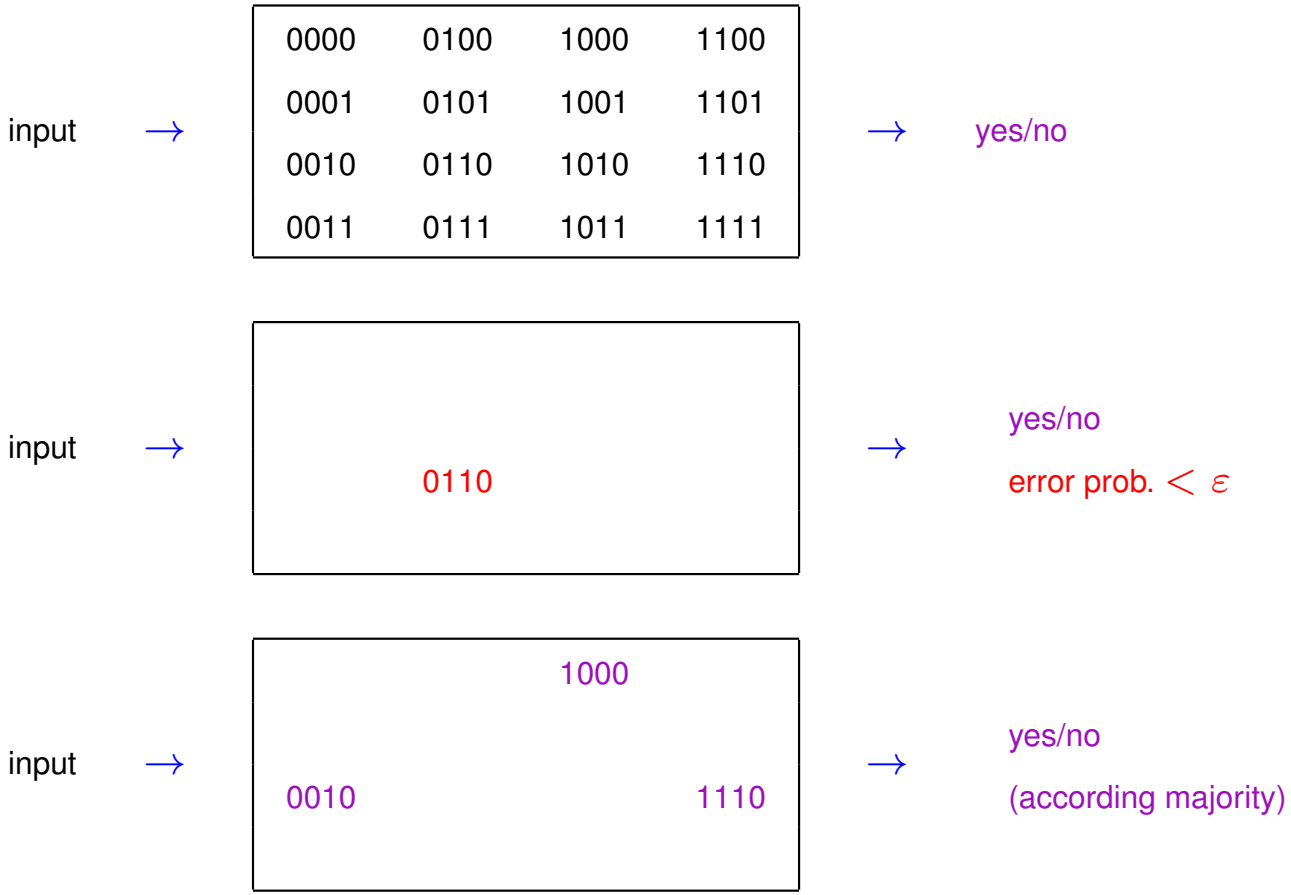


They induce several algorithmic problems, like

- determine (in finite time) who wins the game,
- play (in infinite time) with **minimal memory**.

Positive use of computational complexity

Cryptography, pseudorandom generators. Paradoxically, difficulty of one problem can speed-up solution of another one.



Conclusion

Information processes are largely automatic ($\alpha\upsilon'\tau o\mu\alpha'\tau\eta$) which does not mean trivial.

Coming down from ideal to physical world, they encounter *complexity barriers*, usually expressed in terms of time and memory. To understand the logic behind complexity, we recall ideas of the pioneers of set theory.

We may like regularity, symmetry, harmony. But mathematics sometimes surprises us with the opposite: discontinuity, limitations, crack.

There is a crack in everything. That's how the light gets in.

Leonard Cohen, *Anthem*