Kolmogorov Complexity

\[ K(x) = \text{"length of the shortest program that outputs } x \text{"} \]

Given an oracle for \( K(\cdot) \),
we can find the shortest program
that outputs a given string \( x \).

How: run all programs of
length \( K(x) \) in parallel.

Using \( K(\cdot) \) to produce true
but unprovable statements.

" \( K(x) \geq 50000 \)"

**Theorem (Chaitin)**

\[ \exists L \text{ s.t. for all strings } x, \quad " K(x) \geq L" \text{ is unprovable in PA (any sound reasoning system that can capture TM).} \]

**Theorem (Canturing TMs using first order logic of arithmetic)**

There is a TM that given \( \langle M, w \rangle \)
produces a first-order formula \( \phi_{m,w}(y) \) in the language of arithmetic st. \( M \) accepts \( w \) iff

\[
N \models \exists y \ \phi_{m,w}(y).
\]

Take a TM that enumerates all TMs of length < \( L \), and runs them in parallel, and accepts if any of them halts and outputs \( p \). By Thm \( \Box \), this TM has a formula \( \phi_m \), a
s.t. The TM accepts iff
\[ N \models \exists y \phi_{m,n}(y) \]
so \( \forall y \phi_{m,n}(y) \) captures
the statement \( K(n) \geq L \).

Proof of Chaitin's Thm

Suppose not.

A \( L \), \( \exists a \) s.t.
"\( K(a) \geq L \)" is provable.

So now we can enumerate
proofs and search for proofs of the form "\( K(n) \geq L \)". Use this to get a small program outputting a string with big \( K(\circ) \).

\[ T_{M_L} \circ. \]

Enumerate proofs using \( LK \) starting from axioms.

When we find a statement
of the form \( K(x) \geq L \) we

halt and output \( x \).

Length of \( TM_L = C + \log_2 L \)

If \( L > C + \log_2 L \)

then we have a contradiction.

---

**Hilbert's 10th problem**

**Fermat's Last Theorem** for degree 4

\( \forall x, y, z \in \mathbb{N} \quad 121, y^4, 121 > 2 \)

so that \( x^4 + y^4 = z^4 \).
Diophantine eqn.

\[ P(x_1, \ldots, x_m) = 0 \]

where \( P \) is a polynomial.

Then Robinson, Davis, Putnam, 50s

Matiyasevich 70

This cannot be solved by TMs.

Matiyasevich's paper.
there is a \( P(x_1, \ldots, x_{26}) \) polynomial with 2 coefficients.

\[
\begin{align*}
c = ab & \iff \exists \\mathbb{Z} \\
\exists x_4, x_5, \ldots, x_{26} \text{ s.t.} \quad P(a, b, c, x_4, x_5, \ldots, x_{26}) = 0.
\end{align*}
\]

\[\text{MRDP v2} \]

For any TM \( M \), \( \exists P(x_1, \ldots, x_{26}) \) s.t. \( M \) accepts \( \iff \exists \mathbb{Z} \)
$P(w, x_2, \ldots x_{26}) = 0.$

The zero-one law for random graphs.

Language of graphs.

\[
\sim_1 =
\]

Sentences

\[
\forall x \exists y \forall x \forall y.
\]

\[
\forall x_1, x_2 \exists y_1, y_2 \land (x_1 \sim y_1) \land (x_2 \sim y_2)
\]
\( \forall (x_1 \sim y_2) \land \forall (x_2 \sim y_1) \)

Sentences define graph property.

\( G(n, p) \Rightarrow \) the graph on \( n \) vertices where for each pair of vertices \( \{x, y\}, \ x, y \in \) an edge w.p. \( p \) independently.

\[
\forall x \ p \in \left[ \frac{1}{3}, \text{eg} \right], \forall \phi (\text{sentence})
\]

\[
f(n) = \Pr \left[ G(n, p) \models \phi \right]
\]

Zero-one law for \( G(n, p) \) [Fagin 74, YRRW69]

\[
\forall x \ p, \ \forall \phi.
\]

\[
\lim_{n \to \infty} f(n) = 0 \text{ or } 1.
\]
Alice's Restaurant Property

\[ \forall x_1, x_2, \ldots, x_a \]
\[ \forall y_1, y_2, \ldots, y_b \]
\[ (x_1 \neq y_1) \land (x_1 \neq y_2) \land \ldots \land (x_a \neq y_b) \]
\[ \Rightarrow \exists z \text{ s.t. } z \sim x_1 \land z \sim x_2 \land \ldots \land z \sim x_a \land z \sim y_1 \land z \sim y_2 \land \ldots \land z \sim y_b. \]

Fact: \[ \lim_{n \to \infty} \Pr(G(n, p) \models \text{ARP}_{a, b}) = 1 \]
\[ \Phi = \sum \text{ARP} \alpha, \beta : \alpha, \beta \geq 0 \]
Using ARPs, we find an isomorphism.

Any two countable models of $\varphi$ are isomorphic.

$\Rightarrow$

the theory generated by $\varphi$ is complete.

[Namely for all $\psi$, either

$\varphi \vdash \psi$

or $\varphi \vdash \neg \psi$

] else we can add $\psi$ to $\varphi$
and \( \psi \rightarrow \psi \)

and get nonisomorphic countable models of \( \Phi \).

Take any first order sentence \( \psi \).

Case 1: \( \Phi \vdash \psi \)

Then by compactness, there is a proof of \( \psi \) using only finitely many axioms of \( \Phi \).

Take \( n \) large enough, then those finitely many axioms are satisfied by \( G(n,p) \). w.prob \( \rightarrow 1 \)

So \( \psi \) is then satisfied by \( G(n,p) \). w.prob \( \rightarrow 1 \)
Case 2 \[ \Phi \Rightarrow \Psi. \]

Similar

\[ \Psi \text{ is satisfied by} \]

\[ g(n,p) \ln \ln n \to 1 \]

So \[ \Psi \] is satisfied

by \[ g(n,p) \ln \ln n \to 0. \]