Kolmogorov Complexity

$K(x)$ = "length of the shortest program that outputs x"

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.

" $K(x) \geq 50000$ "

Thm (Chiatin)

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

Thm $\circledast$ Capturing TMs using first order logic of arithmetic

There is a TM that given $\langle M \rangle, w$

produces a firstorder formula $\phi_{M,w}(y)$ in the language of arithmetic

s.t. M accepts w iff

$\mathbb{N} \models \exists y \; \phi_{M,w}(y)$.

Take a TM that enumerates all TMs of length $< L$, and runs them in parallel, and accepts if any of them halts and outputs x. By Thm $*$, this TM has a formula $\phi_{M,x}$

s.t. The TM accepts iff

$\mathbb{N} \models \exists y \; \phi_{M,x}(y)$

So $\neg \exists y \; \phi_{M,x}(y)$ captures

the statement $K(x) \geq L$.

Proof of Chiatin's Thm

Suppose not.

$\forall L$, $\exists$ some x s.t.

"$K(x) \geq L$" is provable.

So now we can enumerate

proofs and search for proofs of the form "$K(x) \geq L$". Use this to get a small program outputting a string with big $K(\cdot)$.

TM_L:

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 Thm for degree 4

$\nexists\ x, y, z \in \mathbb{N} \quad |x|, |y|, |z| \geq 2$

s.t. $\quad x^4 + y^4 = z^4$.

Diophantine eqn.

$\exists x_1 \dots x_m \in \mathbb{Z}$ s.t.

$P(x_1, \dots, x_m) = 0$?

where P is a polynomial.

Thm Robinson, Davis, Putnam, 50s
Matiyasevich 70

This cannot be solved by TMs.

Matiyasevich's part:

there is a $P(x_1 \ldots x_{26})$ polynomial with $\mathbb{Z}$ coeffs.

s.t.

$c = a^b$ iff

$\exists\, x_4, x_5, \ldots, x_{26} \in \mathbb{Z}$ s.t.

$P(a, b, c, x_4, x_5, \ldots x_{26}) = 0.$

MRDP v2

For any TM M, $\exists$ $P(x_1 \ldots x_{26})$ polynomial

s.t. M accepts w iff

$\exists\, x_2, \ldots x_{26} \in \mathbb{Z}$ s.t.

$$P(\omega, x_2, \dots x_{26}) = 0.$$

The zero-one law for random graphs.

Language of graphs.

$\sim$, $=$

Sentences

$\forall x \; \exists y \quad x \sim y.$

$\forall x_1, x_2 \; \exists y_1 \, y_2 \quad$ s.t

$(x_1 \sim y_1) \wedge (x_2 \sim y_2)$

$\wedge \neg(x_1 \sim y_2) \wedge \neg(x_2 \sim y_1)$

Sentences define graph property.

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

Fix p ($= 1/3$ eg). Fix ϕ (sentence).

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

<u>Zero-one law for $G(n,p)$</u> [Fagin 74, YRRW69]

Fix p, fix ϕ.

$$\lim_{n\to\infty} f(n) = 0 \text{ or } 1.$$

Alice's Restaurant Property

$\exists$ a. d. distinct vertices A

$$\mathrm{ARP}_{a,b}\ \Big(\forall x_1 x_2 \cdots x_a$$

$$\forall y_1 y_2, \cdots y_b$$

$$\Big[(x_1 \neq y_1) \wedge (x_1 \neq y_2) \wedge \cdots \cdots (x_a \neq y_b)$$

$$\rightarrow \exists z \text{ s.t. } z \sim x_1 \wedge$$
$$z \sim x_2 \wedge$$
$$\vdots$$
$$z \sim x_a \wedge$$
$$\neg(z \sim y_1) \wedge$$
$$\neg(z \sim y_2) \wedge$$
$$\vdots$$
$$\neg(z \sim y_b).\Big]\Big)$$

$\forall a, b.$

<u>Fact</u> $\quad \lim_{n \to \infty} \Pr[G(n,p) \models \mathrm{ARP}_{a,b}] = 1$

$$\Phi = \{ ARP_{a,b} : a,b \geq 0 \}$$

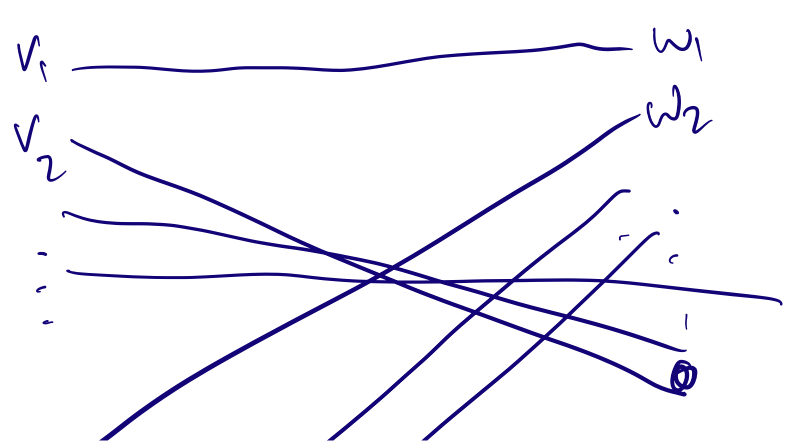
Q Is Φ satisfiable?

A: Yes: because every finite subset is satisfiable (by $G(n,p)$ for a very large n).

$\exists$ Countable mode satisfying it.

Lemma Any two countable model for Φ are isomorphic.

Proof Model 1 Model 2



$\emptyset$

Using ARPs, we find an isomorphism.

Any two countable models of Φ are isomorphic

$\Rightarrow$

the theory generated by Φ is complete.

[Namely for all ψ either

$$\Phi \vdash \psi$$

or $\Phi \vdash \neg\psi$]

Else we can add ψ to Φ

and $\neg\Psi$ to Φ

and get nonisomorphic countable models of Φ.

Take any first order sentence Ψ.

Case 1 $\quad \Phi \vdash \Psi$

Then by compactness, there is a proof of Ψ using only finitely many axioms of Φ.

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

So Ψ is then satisfied by $G(n,p)$. w. prob $\to 1$

Case 2 $\Phi \vdash \neg\Psi$.

Similar

$\neg\Psi$ is satisfied by

$G(n,p)$ w.prob $\to 1$

So Ψ is satisfied

by $G(n,p)$ w.prob $\to 0$.