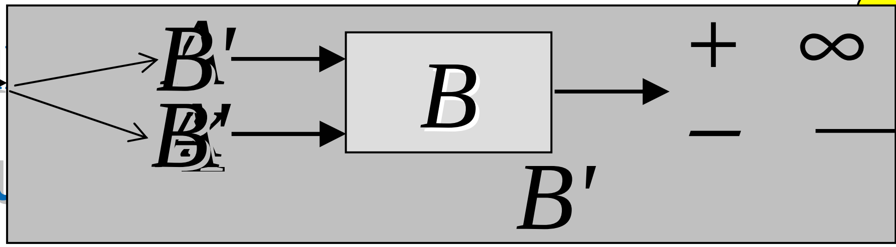
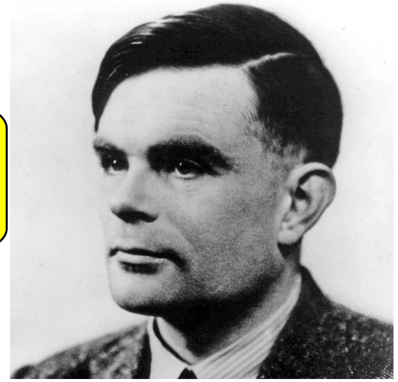
Alan M. Turing 1936 / 1946

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

- first scientific calculations on digital computers
- *What are its fundamental limitations?*
  - Uncou…
  - but cou… s'

decision problem





- Undecidable <u>Halting Problem *H*</u>: **No** algorithm *B* can always correctly ans… ~~simulator/interpreter *B*~~ ?

Given ⟨A,x⟩, does algorithm A terminate on input x?

Proof (by contradiction): Consider algo. *B'* that, on input *A*, executes *B* on ⟨*A*,*A*⟩ and, upon a positive answer, loops infinitely. How does *B'* behave on *B'* ?

- Logicians Tarski, Alonzo Church (PhD advisor)
- Kurt Gödel (1931): There exist arithmetical statements which are true but cannot be proven so.

Formalities & Tools

e.g. "Turing machine"

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

'Definition:' Algorithm A decides set $L\subseteq\{0,1\}^*$ if

all finite binary sequences

- on inputs $\underline{x}\in L$ prints 1 and terminates,
- on inputs $\underline{x}\notin L$ prints 0 and terminates.

A semi-decides if terminates on $\underline{x}\in L$, else diverge.

Hilbert Hotel | Halting Problem H only *semi*-decidable

countable! | eg. $\mathcal{U}$={ algorithms } × { inputs }

Universes $\mathcal{U}$ other than $\{0,1\}^*$ (e.g. $\mathbb{N}$): encode.

Techniques: a) simulation b) diagonalization
c) dovetailing d) reduction (in/output translation)

Theorem: L decidable iff both L, L^C semi-decidable

Infinite $L\subseteq\{0,1\}^*$ is semi-decidable iff $L=\mathrm{range}(f)$ for some computable injective $f:\mathbb{N}\to\{0,1\}^*$

Some Undecidable Problems

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

'Definition:' Algorithm A decides set $L \subseteq \{0,1\}^*$ if

- on inputs $\underline{x} \in L$ prints 1 and terminates,
- on inputs $\underline{x} \notin L$ prints 0 and terminates.

Halting problem: $H = \{ \langle A, \underline{x} \rangle : A$ terminates on $\underline{x} \}$

Hilbert's 10th: The following set is undecidable:
$\{ \langle p \rangle \mid p \in \mathbb{N}[X_1,\ldots X_n],\ n \in \mathbb{N},\ \exists x_1 \ldots x_n \in \mathbb{N}\ \ p(x_1,\ldots x_n)=0 \}$

Word Problem for finitely presented groups

Mortality Problem for two 21×21 matrices

Homeomorphy of 2 finite simplicial complexes

Universes U other than $\{0,1\}^*$ (e.g. $\mathbb{N}$): encode.

Techniques: a) simulation b) diagonalization

c) dovetailing d) reduction (in/output translation)

For $L, L' \subseteq \{0,1\}^*$ write $L \leqslant L'$ if there is a computable
$f: \{0,1\}^* \to \{0,1\}^*$ such that $\forall \underline{x}:\ \underline{x} \in L \Leftrightarrow f(\underline{x}) \in L'$.

a) L' decidable $\Rightarrow$ so L.   b) $L \leqslant L' \leqslant L'' \Rightarrow L \leqslant L''$

Exercise Questions

Which of the following are un-/semi-/decidable?

a) Given an integer, is it a prime number?

b) Given a finite string over +,×,(,),0,1,$X_1,\ldots X_n$
is it syntactically correct?

c) Given a Boolean formula $\varphi(X_1,\ldots X_n)$,
does it have a *satisfying assignment*?

d) Given $M\in\mathbb{Z}^{n\times n}$ and $b\in\mathbb{Z}^n$,
does there exists a integer real vector $\underline{x}$ s.t. $\underline{M}\cdot\underline{x}\leq\underline{b}$?

e) Given an algorithm *A*, input $\underline{x}$, and integer *N*,
does *A* terminate on input $\underline{x}$ within *N* steps ?

f) Does a given algorithm terminate on all inputs?

g) Does given algorithm terminate on some input?

Computable Real Numbers

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

Theorem: For $r\in\mathbb{R}$, the following are equivalent:

Call $r\in\mathbb{R}$ computable if

There is an algorithm which, given $n\in\mathbb{N}$, prints $b_n\in\{0,1\}$ where $r=\sum_n b_n 2^{-n}$

a) r has a computable binary expansion

b) There is an algorithm printing, on input $n\in\mathbb{N}$, some $a\in\mathbb{Z}$ with $|r-a/2^{n+1}|\leq 2^{-n}$.

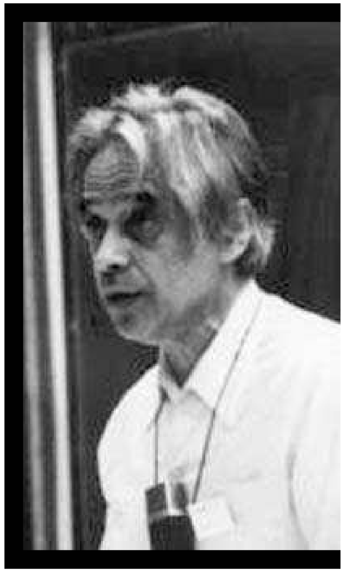
$\Leftrightarrow r\in [q_n\pm\varepsilon_n]$

c) There is an algorithm printing two sequences $(q_n)\subseteq\mathbb{Q}$ and (ε_n) with $|r-q_n|\leq\varepsilon_n\to 0$

numerators+ denominators

b) $\Leftrightarrow$ c) holds *uniformly*, $\Leftrightarrow$ a) does not [Turing'37]

interval arithmetic



Ernst Specker (1949): (c) $\Leftrightarrow$ *Halting problem* plus (d)

d) There is an algorithm printing $(q_n)\subseteq\mathbb{Q}$ with $q_n\to r$.

H := { ⟨B,$\underline{x}$⟩ : algorithm B terminates on input $\underline{x}$ } $\subseteq\mathbb{N}$

Exercises: Computable Reals

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

a) Every rational has a computable binary expansion

b) Every dyadic rational has two binary expansions

c) Computable binary expansion $\Leftrightarrow$ computable real

d) If a,b are computable, then also $a+b$, $a \cdot b$, $1/a$ $(a \neq 0)$

e) Fix $p \in \mathbb{R}[X]$. Then p's coefficients are computable
$\Leftrightarrow$ $p(x)$ is computable for all computable x.

f) The degree of every $p \in \mathbb{R}[X]$ is computable.

g) Every algebraic number is computable; and so is π.

h) If x is computable, then so are $\exp(x)$, $\sin(x)$, $\log(x)$

j) For every computable x, $\text{sign}(x)$ is computable.

k) Specker's sequence $\left(\sum_{k>n\in H} 2^{-n}\right)_k$ is computable,
its limit is uncomputable, yet naively computable.

$r \in \mathbb{R}$ **computable** iff an algorithm can print, on input $n \in \mathbb{N}$, some $d \in \mathbb{Z}$ with $|r - d/2^{n+1}| \leq 2^{-n}$

Reminder: For $r\in\mathbb{R}$, the following are equivalent:

a) ∃algorithm deciding r's bin. exp

b) ∃algorithm printing on input n
some $a\in\mathbb{Z}$ with $|r-a/2^{n+1}|\leq 2^{-n}$.

c) ∃algorithm printing $(q_n),(\varepsilon_n)\subseteq\mathbb{Q}$ with $|r-q_n|\leq\varepsilon_n\to 0$

a)⇒b)⇔c) computable transformation on algorithms
b)⇒a) 'undecidable' case split on $r\in\mathbb{Q}$

Call $(r_m)\subseteq\mathbb{R}$ computable iff an algorithm can print, on input $\langle n,m\rangle\in\mathbb{N}$, some $a\in\mathbb{Z}$ with $|r_m-a/2^{n+1}|\leq 2^{-n}$.

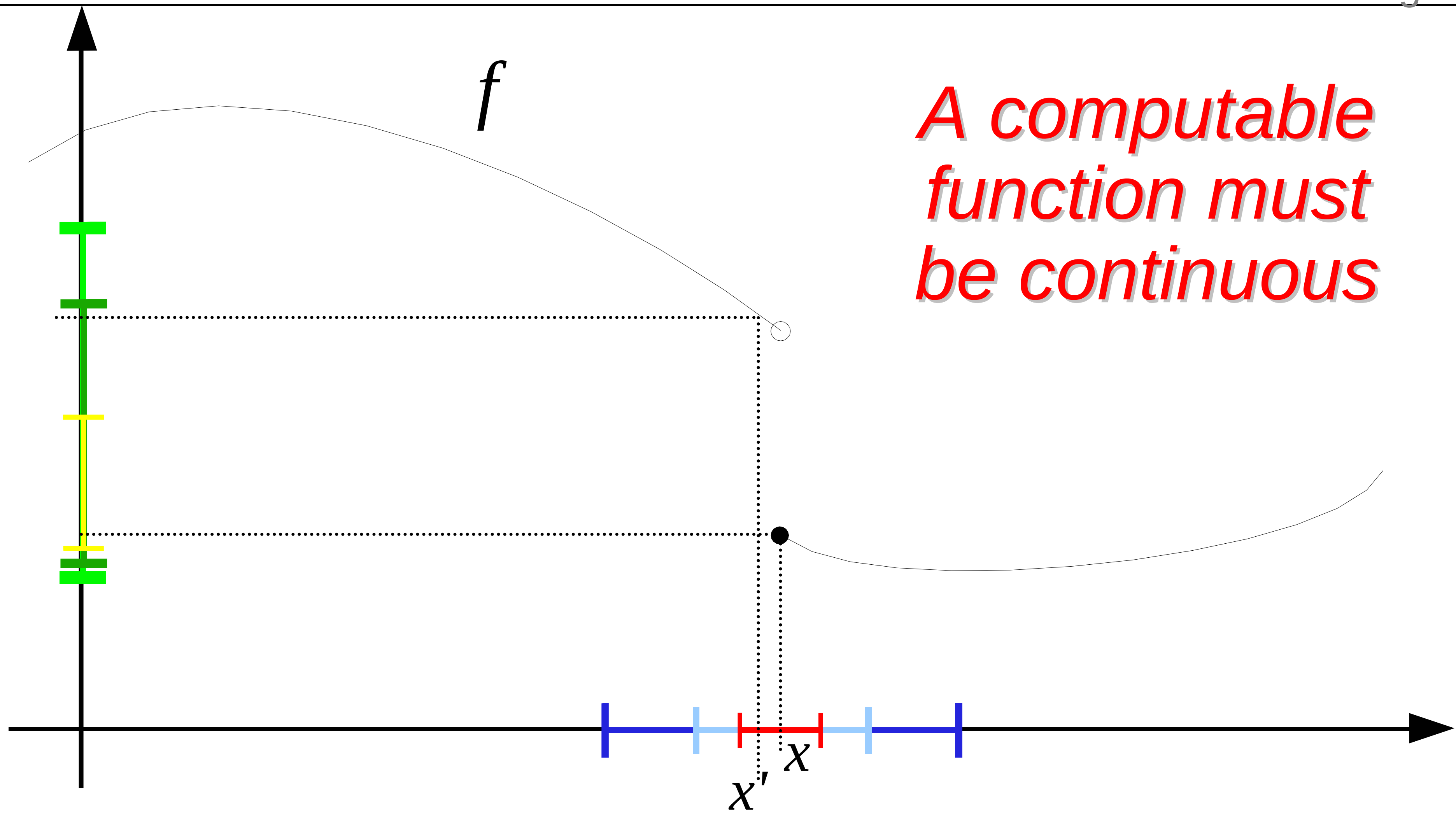
In numerics, don't test for (in-)equality!

Fact: There exists a computable sequence $(r_m)\subseteq[0,1]$ such that $\{\, m : r_m\neq 0 \,\}$ is the Halting problem H.

$H := \{\, \langle B,\underline{x}\rangle : \text{algorithm } B \text{ terminates on input } \underline{x} \,\} \subseteq \mathbb{N}$

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

Uniformly Computable Real Functions



A computable function must be continuous

$x \in \mathbb{R}$ computable $\Leftrightarrow |x - a_n/2^{n+1}| \leq 2^{-n}$ for recursive $(a_n) \subseteq \mathbb{Z}$

Computable Weierstrass Theorem

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

Theorem: For $f:[0,1]\to\mathbb{R}$ the following are equivalent:

a) There is an algorithm <u>converting</u> any seq. $q_n\in\mathbb{D}_{n+1}$ with $|x-q_n|\leq 2^{-n}$ into $p_m\in\mathbb{D}_{m+1}$ with $|f(x)-p_m|\leq 2^{-m}$

b) There is an algorithm <u>printing</u> a sequence (of degrees and coefficient lists of) $(P_n)\subseteq\mathbb{D}[X]$ with $\|f-P_n\|\leq 2^{-n}$

c) The real sequence $f(q)$, $q\in\mathbb{D}\cap[0,1]$, is computable & f admits a computable modulus of uniform continuity

$|x-y|\leq 2^{-\mu(m)} \Rightarrow |f(x)-f(y)|\leq 2^{-m}$

Proof: a) $\Rightarrow$ c) $\Rightarrow$ b)

Call $(r_m)\subseteq\mathbb{R}$ computable iff an algorithm can print, on input $n,m\in\mathbb{N}$, some $q\in\mathbb{D}_{n+1}$ with $|r_m-q|\leq 2^{-n}$.

$\mathbb{D} := \bigcup_n \mathbb{D}_n$, $\quad\mathbb{D}_n := \{\, a/2^n : a\in\mathbb{Z}\,\}$

Exercises: Computable Real Functions

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

a) f computable $\Rightarrow$ same for any restriction

b) exp, sin, cos, $\ln(1+x)$ are computable functions

c) For a computable sequence $\underline{a}=(a_n)$,
the power series $x\to\sum_n a_n\cdot x^n$ is computable
on $(-r,r)$ for $r < R(\underline{a}) := 1/\limsup_n |a_n|^{1/n}$

uncomputable in general

d) Let $f\in C[0,1]$ be computable. Then so are
$\int f: x\to\int_0^x f(t)\,dt$ and $\max(f):x\to\max\{f(t):t\leq x\}$.

e) If $(x,m)\to f_m(x)$ computable with $|f_n-f_m|_\infty\leq 2^{-n}+2^{-m}$
then $\lim_n f_n$ is computable.

f) For computable $a\in\mathbb{R}$, $f:[0,a]\to\mathbb{R}$, and

To **compute** $f:\mathbb{R}\to\mathbb{R}$: convert any sequence $q_n\in\mathbb{D}_{n+1}$ with $|x-q_n|\leq 2^{-n}$ into $p_m\in\mathbb{D}_{m+1}$ with $|f(x)-p_m|\leq 2^{-m}$

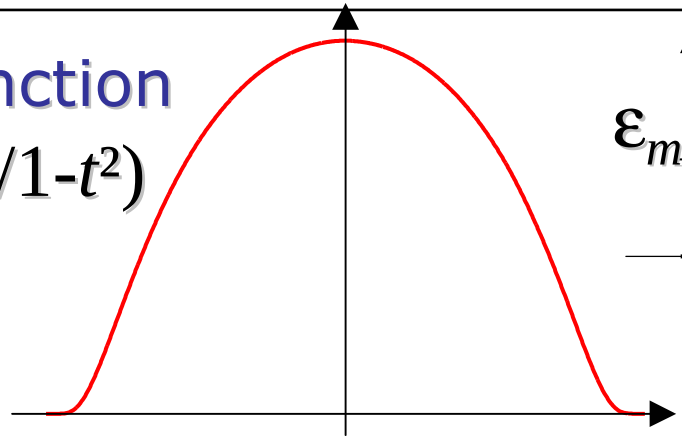
TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

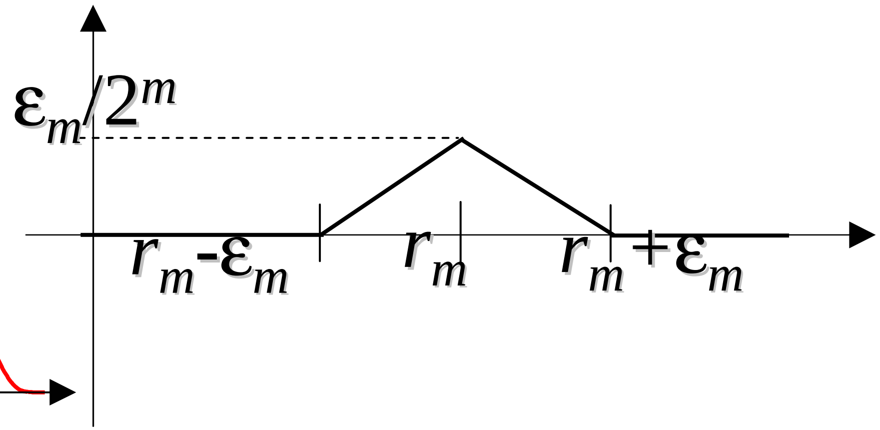
Computable Urysohn

C^∞ 'pulse' function

$\varphi(t) = \exp(-t^2/1-t^2)$

$|t|<1$





Let $(r_m)_m, (\varepsilon_m)_m \subseteq \mathbb{Q}$ be computable sequences

Then there is a computable C^∞ $f:[0;1]\to[0;1]$

s.t. $f^{-1}[0] = [0;1]\setminus\bigcup_m (r_m-\varepsilon_m, r_m+\varepsilon_m)$.

Proof: Let $f(x) := \sum_m \max(0,\varepsilon_m-|x-r_m|)/2^m$

Specker'59: Uncomputable roots

approximating a root
vs. approximate root

Lemma: There are computable sequences $(r_m)_m, (\varepsilon_m)_m \subseteq \mathbb{Q}$ s.t. $U := \bigcup_m (r_m\text{-}\varepsilon_m, r_m+\varepsilon_m)$ contains all computable reals in [0;1] and has measure <½.

Let $(r_m)_m, (\varepsilon_m)_m \subseteq \mathbb{Q}$ be computable sequences
Then there is a computable C^∞ $f:[0;1]\to[0;1]$
s.t. $f^{-1}[0] = [0;1]\setminus\bigcup_m (r_m\text{-}\varepsilon_m, r_m+\varepsilon_m)$.

Corollary: There is a computable C^∞ $f:[0;1]\to[0;1]$ s.t. $f^{-1}[0]$ has measure >½ but contains no computable real number.

Singular Covering of Computable Reals

Lemma: There are computable sequences $(r_m)_m, (\varepsilon_m)_m \subseteq \mathbb{Q}$ s.t. $U := \bigcup_m (r_m-\varepsilon_m, r_m+\varepsilon_m)$ contains all computable reals in [0;1] and has measure $<½$.

Machine computes $r\in\mathbb{R}$ iff prints seq. $a_n\subseteq\mathbb{Z}$ with $|a_n/2^{n+1} - a_m/2^{m+1}|\leq 2^{-n}+2^{-m}$.

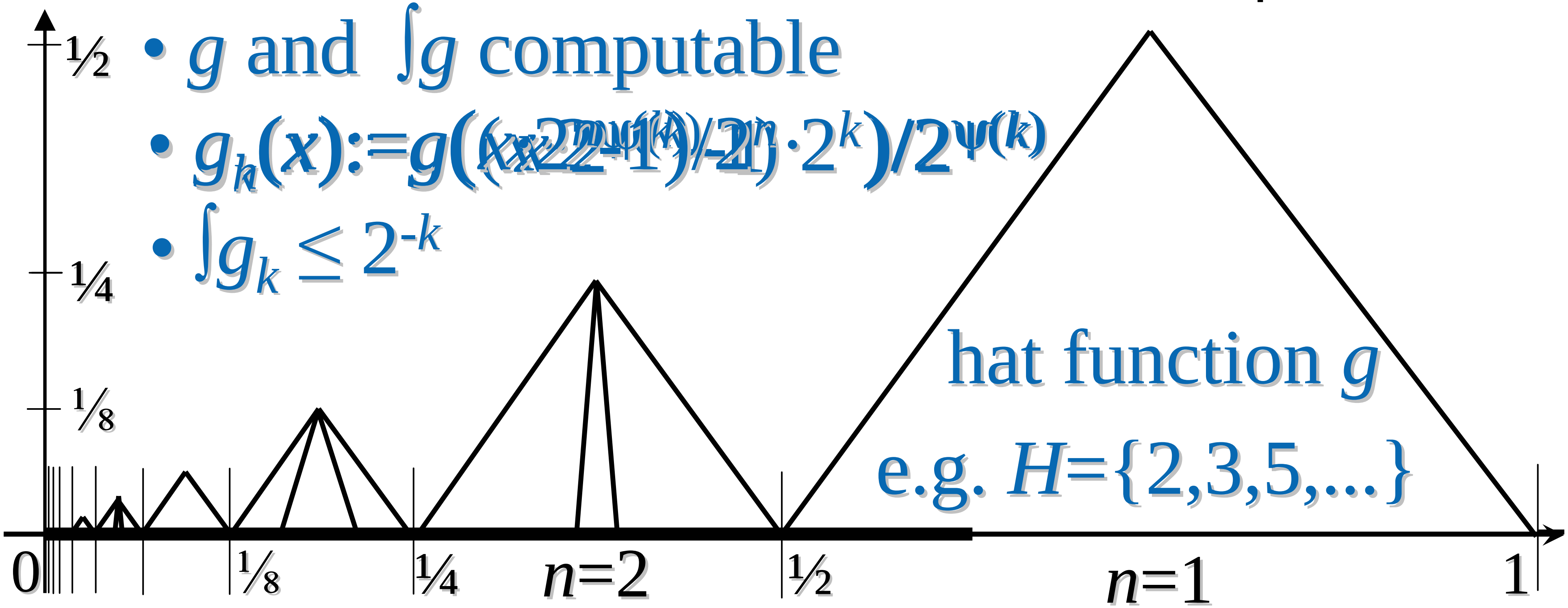
Proof: Dove-tailing w.r.t. (M,t):
If Turing machine $\#M$ within t (but not t-1) steps prints $a_1,\ldots a_{M+5}$ s.t. $|a_k/2^{k+1}-a_\ell/2^{\ell+1}| \leq 2^{-k}+2^{-\ell}$ $\forall 1\leq k,\ell\leq M+5$ then let $r_{\langle M,t\rangle} := a_{M+5}/2^{M+6}$ and $\varepsilon_{\langle M,t\rangle} := 2^{-M-5}$, else $r_{\langle M,t\rangle} := 0$ and $\varepsilon_{\langle M,t\rangle} := 2^{-\langle M,t\rangle-3}$.

Myhill'71: uncomputable ∂ on $C^1[0,1]$

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

Fact : ∃ computable bijection $\psi:\mathbb{N}\to H$

- g and $\int g$ computable
- $g_k(x):=g\big((x\cdot 2^k-1)\cdot 2^k\big)/2^{\psi(k)}$
- $\int g_k \le 2^{-k}$



$h' := \sum_{n\in H} g_n$ continuous, incomputable,

yet $h:=\int h' \in C^1[0;1]$ computable.

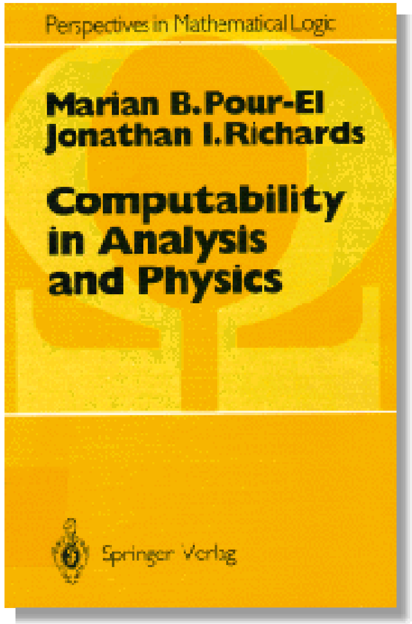
q.e.d.

The Case of the Wave Equation

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

Myhill'71: computable $h \in C^1[0,1]$ with uncomputable $h'(1)$

Pour-El&Richards'81 construct a computable $f \in C^1(\mathbb{R}^3)$ such that for $g:=0$ the unique solution is *in*computable at $t=1$ and $\underline{x}=(0,0,0)$.



Church-Turing Hypothesis (Kleene):
Everything that can be computed by a Turing machine can also be computed by a physical device – and vice versa!

$$\partial^2/\partial t^2\, u(\underline{x},t) = \Delta u(\underline{x},t), \quad u(\underline{x},0)=f(\underline{x}), \quad \partial/\partial t\, u(\underline{x},0)=g(\underline{x})$$

The Case of the Wave Equation

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

Myhill'71: computable $h \in C^1[0,1]$ with uncomputable $h'(1)$

Pour-El&Richards'81 construct a computable $f \in C^1(\mathbb{R}^3)$ such that for g:=0 the unique solution is *in*computable.

Kirchhoff's formula:

$$u(t,\vec{x}) = \frac{\partial}{\partial t}\left(\frac{1}{4\pi t}\int_{|\vec{y}-\vec{x}|=t} f(\vec{y})\, d\sigma(\vec{y})\right) + \frac{1}{4\pi t}\int_{|\vec{y}-\vec{x}|=t} g(\vec{y})\, d\sigma(\vec{y})$$

$$f(\vec{x}) := h(|\vec{x}|^2)$$

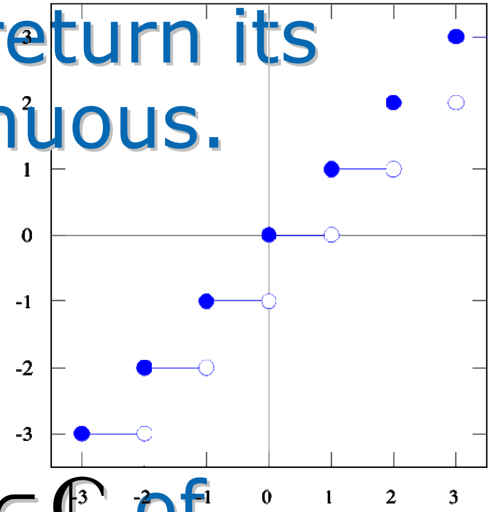
$$u(t,0) = \frac{d}{dt}\left(h(t^2)\cdot t\right) = h'(t^2)\cdot 2t^2 + h(t^2)$$

$\partial^2/\partial t^2\, u(\underline{x},t) = \Delta u(\underline{x},t)$, $u(\underline{x},0)=f(\underline{x})$, $\partial/\partial t\, u(\underline{x},0)=g(\underline{x})$

Two Effects in Real Computability

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

a) Multivalued 'functions'



Example floor function: given $x \in \mathbb{R}$, return its least integer upper bound — discontinuous.

Given x, return <u>some</u> integer upper bound: computable!

Example fund. theorem of algebra:
Given $a_0, \ldots a_{d-1} \in \mathbb{C}$, return roots $x_1, \ldots x_d \in \mathbb{C}$ of $a_0 + a_1 \cdot X + \ldots + a_{d-1} \cdot X^{d-1} + X^d \in \mathbb{C}[X]$ incl. multiplicities

up to permutation [Specker'67]

b) Discrete 'advice'

Example matrix diagonalization: given $A \in \mathbb{R}^{d \cdot (d-1)/2}$, return a basis of eigenvectors — discontinuous:

$$\varepsilon \cdot \begin{pmatrix} \cos(1/\varepsilon) & \sin(1/\varepsilon) \\ \sin(1/\varepsilon) & -\cos(1/\varepsilon) \end{pmatrix}$$

Thm: Computable knowing $|\sigma(A)|$.