Asymptotic Running Times

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

n	$\log_2 n \cdot$10s	$n \cdot \log n$ sec	n^2 msec	n^3 μsec	2^n nsec
10	33sec	33sec	0.1sec	1msec	1msec
100	≈1min	11min	10sec	1sec	40 Mrd. Y
1000	≈1.5min	≈3h	17min	17min	
10 000	≈2min	1.5 days	≈1 day	11 days	
100 000	≈2.5min	19 days	4 months	32 years	

- Running times of some sorting algorithms
  - BubbleSort: $O(n^2)$ comparisons and copy instr.s
  - QuickSort: typically $O(n \cdot \log n)$ steps
    but $O(n^2)$ in the *worst-case*
  - HeapSort: always at most $O(n \cdot \log n)$ operations
- Here: focus on worst-case considerations!
  - w.r.t. input size (e.g. bit length) $=: n \to \infty$

(Discrete) Complexity Classes

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.

Example: $L=\{$ 10, 11, 101, 111, 1011, 1101, ... $\}$

Def: A runs in polynom. time/space if $\exists p\in\mathbb{N}[N]$:
on input $\underline{x}\in\{0,1\}^n$ makes at most $p(n)$ steps
/ uses at most $p(n)$ bits of memory.

$\mathcal{P}$:= { $L\subseteq\{0,1\}^*$ decidable in polynomial time }

$\subseteq$ $\mathcal{NP}$:= { L verifiable in polynomial time }

$\subseteq$ $\mathcal{PSPACE}$:= { L decidable in polyn. space }

$\subseteq$ $\mathcal{EXP}$:= { L decidable in time $2^{p(n)}$ }

Example Problems (I)

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

Def: A Boolean term $\Phi(Y_1,\dots Y_n)$ is composed from variables $Y_1,\dots Y_n$, constants 0 and 1, and operations $\vee$, $\wedge$, $\neg$.

Examples:
- 0
- $(\neg x \vee y) \wedge (x \vee \neg y)$
- $(\neg x \vee y) \wedge (x \vee y) \wedge \neg y$
- $(\neg x \vee y) \wedge (x \vee \neg z) \wedge (z \vee \neg y) \wedge x \wedge (\neg y)$

Φ in 3-CNF if $\Phi = \bigwedge ((\neg)y_i \vee (\neg)y_j \vee (\neg)y_\ell)$

suitably encoded over $\{0,1\}^*$

EVAL: Given $\langle\Phi(Y_1,\dots Y_n)\rangle$ and $y_1,\dots y_n \in \{0,1\}$, does $\Phi(y_1,\dots y_n)$ evaluate to 1 ? $\in \mathcal{P}$

[*k*-] SAT: Given $\Phi(Y_1,\dots Y_n)$ [in *k*-CNF], does it hold $\exists y_1,\dots y_n \in \{0,1\}: \Phi(y_1,\dots y_n)=1$?

$\mathcal{P}$ vs $\mathcal{NP}$ Millennium Problem

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

Def: $L\subseteq\{0,1\}^*$ is verifiable in polyn. time if

$$L = \{\ \underline{x}\in\{0,1\}^n \mid n\in\mathbb{N},\ \exists \underline{y}\in\{0,1\}^{q(n)} :\ \langle \underline{x},\underline{y}\rangle \in V\ \}$$

for some $V\in\mathcal{P}$ and $q\in\mathbb{N}[N]$.

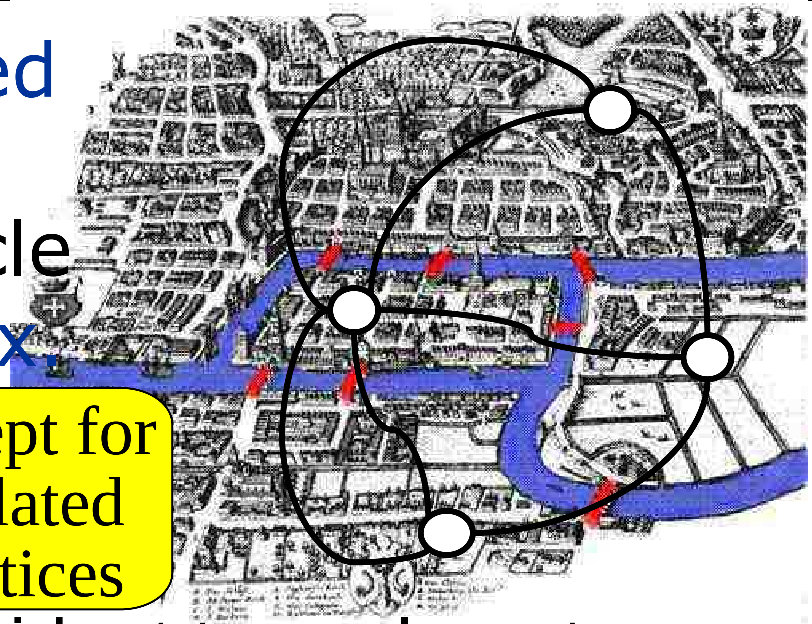
$\mathcal{P}$:= { $L\subseteq\{0,1\}^*$ decidable in polynomial time }
$\subseteq$ $\mathcal{NP}$ **:= { L verifiable in polynomial time }**
$\subseteq$ $\mathcal{PSPACE}$:= { L decidable in polyn. space }
$\subseteq$ $\mathcal{EXP}$:= { L decidable in exponential time }

EVAL: Given $\langle\Phi(Y_1,\ldots Y_n)\rangle$ and $y_1,\ldots y_n\in\{0,1\}$, does $\Phi(y_1,\ldots y_n)$ evaluate to 1 ? $\in\mathcal{P}$

[*k*-]SAT: Is given $\Phi(\underline{Y})$ [in *k*-CNF] satisfiable, i.e. $\exists y_1,\ldots y_n\in\{0,1\}$: $\Phi(y_1,\ldots y_n)=1$? $\in\mathcal{PSPACE}$ $\in\mathcal{NP}$

Example Problems (II)

Eulerian cycle in an undirected graph G traverses each edge precisely 1×; Hamiltonian cycle visits each vertex precisely 1×.



G admitting a Eulerian cycle is connected and has an even number of edges incident to each vertex

except for isolated vertices

vertex admits a Eulerian cycle.

$\mathcal{P}$:= { $L\subseteq\{0,1\}^*$ decidable in polynomial time }
$\subseteq \mathcal{NP}$:= { L verifiable in polynomial time }

EC := { $\langle G\rangle$ | G admits a Eulerian cycle} $\in \mathcal{NP}$
HC := { $\langle G\rangle$ | G admits Hamilton. cycle} $\in \mathcal{NP}$

More Problems in $\mathcal{NP}$

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

CLIQUE := { $\langle G,k\rangle$ | graph $G=(V,E)$ contains k pairwise adjacent vertices } **?**

IS := { $\langle G,k\rangle$ | graph $G=(V,E)$ contains k pairwise non-adjacent vertices } **?**

4-SAT: Is given $\Phi(\underline{Y})$ in 4-CNF satisfiable? **?**

3-SAT: Is given $\Phi(\underline{Y})$ in 3-CNF satisfiable? **?**

2-SAT: Is given $\Phi(\underline{Y})$ in 2-CNF satisfiable? $\in \mathcal{P}$

$\mathcal{P}$:= { $L\subseteq\{0,1\}^*$ decidable in polynomial time }
$\subseteq \mathcal{NP}$:= { L verifiable in polynomial time }

EC := { $\langle G\rangle$ | G admits a Eulerian cycle} $\in \mathcal{P}$

HC := { $\langle G\rangle$ | G admits Hamilton. cycle} **?**

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

Comparing Problems: Reduction

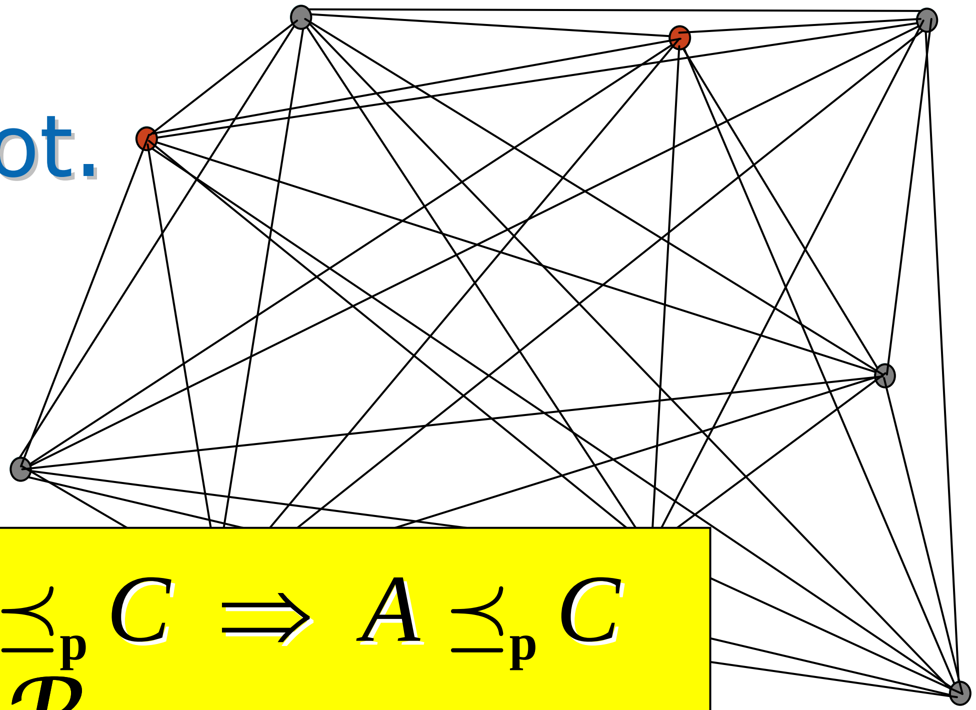
Def: Polynom. reduction from A to $B \subseteq \{0,1\}^*$ is a $f:\{0,1\}^* \to \{0,1\}^*$ computab. in poly.time s.t. $\underline{x} \in A \Leftrightarrow f(\underline{x}) \in B$. Write $A \preceq_p B$.

k pairwise non-adjacent vertices }

Don't know whether **CLIQUE, IS** $\in \mathcal{P}$ or not.

Do know: either both or none $\in \mathcal{P}$

$G=(V,E) \to (V, V\times V \setminus E)$



Lemma: i) $A \preceq_p B,\ B \preceq_p C \Rightarrow A \preceq_p C$

ii) $A \preceq_p B,\ B \in \mathcal{P} \Rightarrow A \in \mathcal{P}$

Example Reduction: 4SAT vs. 3SAT

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

Def: Polynom. reduction from A to $B \subseteq \{0,1\}^*$ is a $f:\{0,1\}^* \to \{0,1\}^*$ computab. in poly.time s.t. $\underline{x} \in A \Leftrightarrow f(\underline{x}) \in B$. Write $A \preceq_p B$.

Given $\Phi = (a \vee b \vee c \vee d) \wedge (p \vee q \vee r \vee s) \wedge \ldots$

with literals $a,b,c,d,p,q,r,s,\ldots$ (variables, possibly negated)

Introduce new variables $u,v,\ldots$ and consider

$$\Phi' := (a \vee b \vee u) \wedge (\neg u \vee c \vee d) \wedge (p \vee q \vee v) \wedge (\neg v \vee \vee r \vee s) \wedge \ldots$$

$f: \langle\Phi\rangle \to \langle\Phi'\rangle$

4-SAT: Is given $\Phi(\underline{Y})$ in 4-CNF satisfiable?
3-SAT: Is given $\Phi(\underline{Y})$ in 3-CNF satisfiable?

Reduction 3SAT $\leqslant_p$ IS

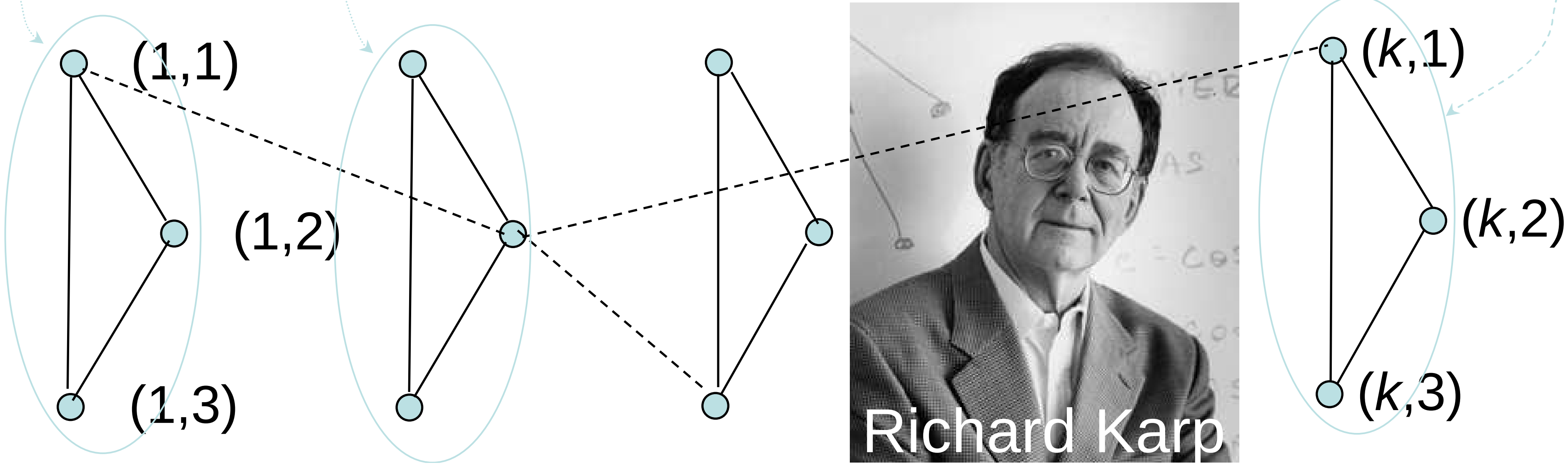
TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

Produce, given a 3-CNF term Φ, within polynomial time a graph G and integer k such that it holds: Φ *is satisfiable iff* G *contains* k *pairwise non-adjacent vertices.*

e.g. $(\, u \vee .. \vee .. \,) \wedge (\, .. \vee \neg u \vee .. \,) \wedge (\, .. \vee .. \vee u \,) \wedge (\, u \vee .. \vee .. \,)$

$\Phi = C_1 \wedge C_2 \ldots \wedge C_k$, $C_i = x_{i1} \vee x_{i2} \vee x_{i3}$, x_{is} literals

$V := \{\, (i,1),\ldots(i,3) : i \leq k \,\}$, $E := \{\, \{(i,s),(j,t)\} : i=j \text{ or } \overline{x_{is}} = x_{jt} \,\}$



Discrete Complexity Picture

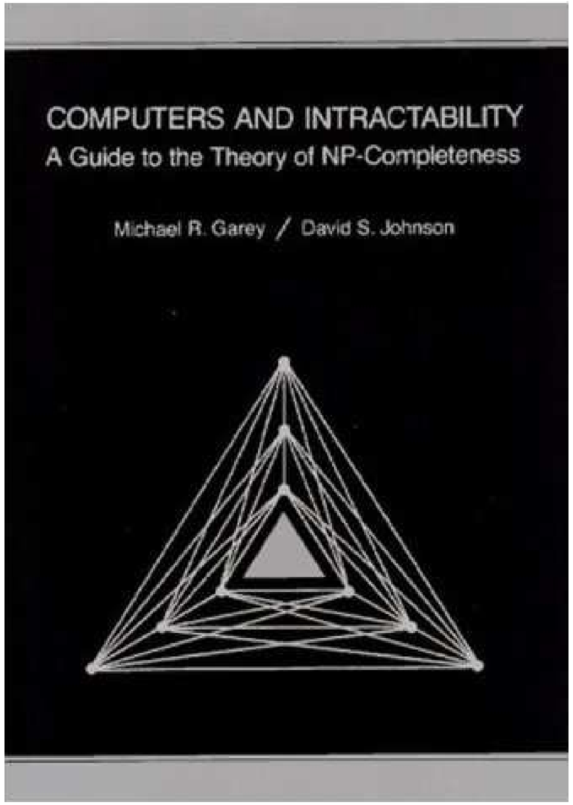
TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

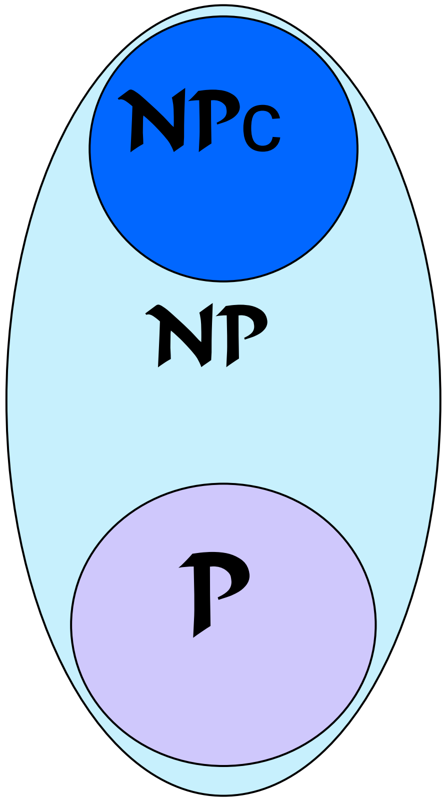
Have shown: **CLIQUE** $\equiv_p$ **IS** $\leqslant_p$ **SAT** $\equiv_p$ **3SAT** $\leqslant_p$ **IS**.

Theorem (Cook'72/Levin'71):

For every $L \in \mathcal{NP}$ it holds $L \leqslant_p$ **SAT**

Now know ≈500 natural problems all polynom.-time equivalent to **SAT**.





Real Function Complexity

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

1RRAM (GMP/MPFR)

Function $f:[0,1]\to\mathbb{R}$ computable in time $t(n)$
if some TM can, on input of $n\in\mathbb{N}$ and of
$(a_m)\subseteq\mathbb{Z}$ with $|x-a_m/2^{m+1}|<2^{-m}$
in time $t(n)$ output $b\in\mathbb{Z}$ with $|f(x)-b/2^{n+1}|<2^{-n}$.

Examples: a) $+$, $\times$, $\exp$ polytime on $[0;1]$!

b) $f(x)\equiv\sum_{n\in L} 4^{-n}$ iff $L\subseteq\{0,1\}^*$ polytime-decidable

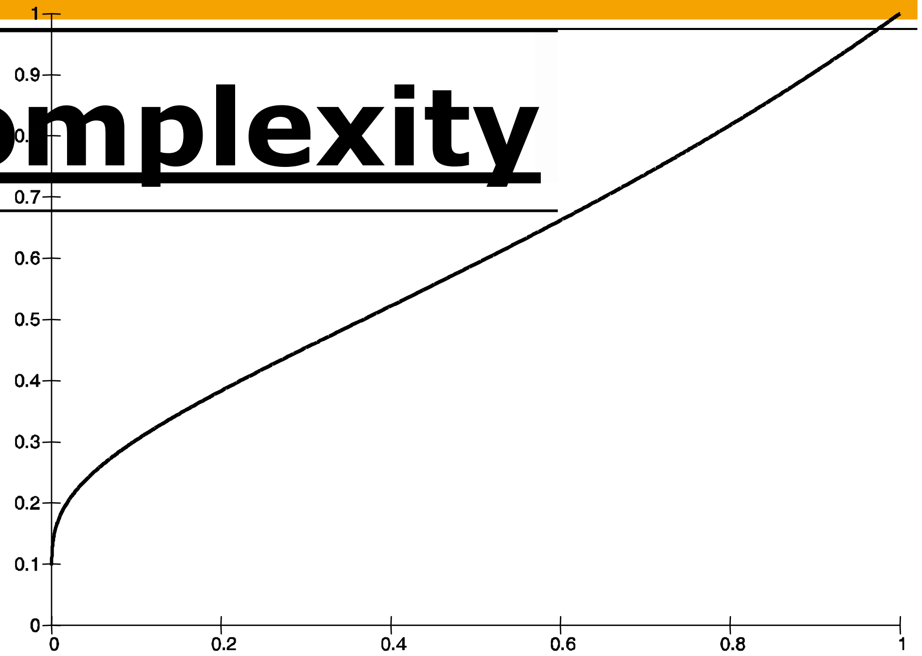
c) sgn(Heaviside) not computable
c) $1/\ln(x)$ exptime, not polytime-computable

Observation: If f computable in time $t(n)$, then $\mu(n)=t(n+2)$ is a modulus of uniform continuity of f:

$$\forall x,y:\ |x-y|\le 2^{-\mu(n)} \Rightarrow |f(x)-f(y)|\le 2^{-n}.$$

$\mathbb{D}_n := \{ k/2^n : k\in\mathbb{Z} \}$, $\mathbb{D} = \bigcup_n \mathbb{D}_n$ dyadic rationals

Real Function Complexity



a) Multivalued 'functions'

b) Discrete 'advice'

c) Parameterized complexity

3rd effect

Examples: a) $+, \times, \exp$ polytime on $[0;1]$!
computable in time $\mathrm{poly}(n+k)$ on $[-k,k]$

c) $1/\ln(e/x)$ exptime, not polytime-computable

Observation: If f computable in time $t(n)$, then $\mu(n)=t(n+2)$ is a modulus of uniform continuity of f:

$$\forall x,y: \; |x-y|\leq 2^{-\mu(n)} \;\Rightarrow\; |f(x)-f(y)|\leq 2^{-n}.$$

Complexity of Real Operators

TECHNISCHE UNIVERSITÄT DARMSTADT

f:[0;1]→[0;1] polytime computable (⇒ continuous)

- Max: $f \to \mathrm{Max}(f): t \to \max\{ f(s): s \le t\}$

  Max(f) computable in exponential time;
  polytime-computable iff $\mathcal{P}=\mathcal{NP}$

- $\int: f \to \int f: t \to \int_0^t f(s)\, ds$

  $\int f$ computable in exponential time;
  "#$\mathcal{P}$-complete"

even when restricting to $f \in C^\infty$ **but for analytic f polytime**

[Friedman&Ko'80ies]

- dsolve: $C[0;1]\times[-1;1] \ni f \to z$: $\dot z(t)=f(t,z)$, $z(0)=0$.

- in general no computable solution $z(t)$
- for $f \in C^1$ "$\mathcal{PSPACE}$-complete"
- for $f \in C^k$ "$\mathcal{CH}$-hard"

other famous complexity classes

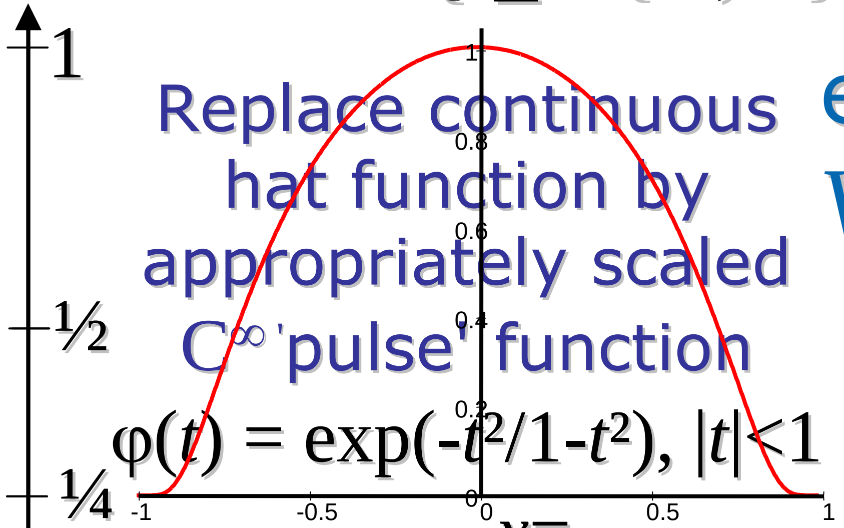
'Max is $\mathcal{NP}$-hard'

TECHNISCHE UNIVERSITÄT DARMSTADT
Martin Ziegler

$\mathcal{NP} \ni L = \{ \underline{x} \in \{0,1\}^n \mid \exists \underline{y} \in \{0,1\}^{p(n)}: \langle \underline{x},\underline{y} \rangle \in V \}$

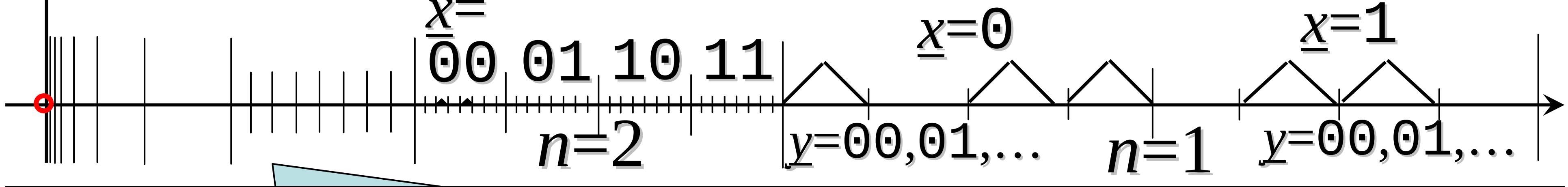
Replace continuous hat function by appropriately scaled C^∞ 'pulse' function

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



e.g. $p(1)=2$, $p(2)=3$,

$V = \{ \langle 0,00\rangle, \langle 0,10\rangle, \langle 0,11\rangle, \langle 1,01\rangle, \langle 1,10\rangle, \langle 00,010\rangle, \langle 00,100\rangle, \ldots \}$



To every $L \in \mathcal{NP}$ there exists a polytime computable **continuous** function $f_L:[0,1]\to\mathbb{R}$ s.t.:

$[0,1] \ni t \to \max f_L|_{[0,t]}$ again polytime iff $L \in \mathcal{P}$