

On
Relativizations of the
 $P \stackrel{?}{=} NP$ Question
for Several Structures

Christine Gaßner
Greifswald

Hagen 2008

On Relativizations of the $P \stackrel{?}{=} NP$ Question for Several Structures

Our goal:

- **Construct several oracles with**
 $P^A \neq NP^A$
with respect to the uniform model of computation.
- **Evaluate known constructions**
using knowledge
 - of the mathematical logic,
 - about the ring over the real numbers.
- **Show difficulties in deriving a structure with**
 $P = NP$
from an oracle with $P^A = NP^A$.

On Relativizations of the $P \stackrel{?}{=} NP$ Question for Several Structures

1. The uniform model of computation
2. Diagonalization techniques and halting problems
3. Structures and oracles with $P^A \neq NP^A$
4. Structures and an oracle with $P^A = NP^A$

The uniform model of computation

A structure: $\Sigma = (U; c_1, \dots, c_u; f_1, \dots, f_v; R_1, \dots, R_w, =)$
 $\Sigma = (U; (c_i)_{i \in F}; (f_i)_{i \in G}; (R_i)_{i \in H}, =)$

Computation: $l: Z_k := f_j(Z_{k_1}, \dots, Z_{k_{m_j}});$
 $l: Z_k := c_j;$

Branching: $l: \text{if } R_j(Z_{k_1}, \dots, Z_{k_{n_j}}) \text{ then goto } l_1 \text{ else goto } l_2;$
 $l: \text{if } Z_k = Z_j \text{ then goto } l_1 \text{ else goto } l_2;$

Copy: $l: Z_{I_k} := Z_{I_j};$

Index computation: $I_k := 1; I_k := I_k + 1; \text{ if } I_k = I_j \text{ then goto } l_1 \text{ else goto } l_2;$

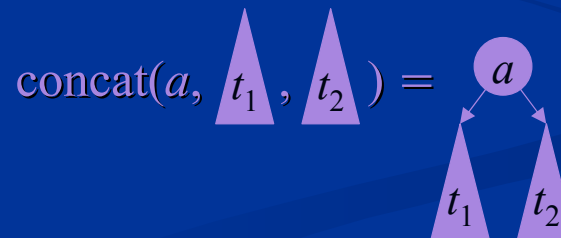
Examples for several structures

$$\mathbb{Z}_2 = (\{0, 1\}; 0, 1; +, \cdot; =) \quad (\Rightarrow \text{Turing machines})$$

$$\mathbb{R} = (\mathbb{R}; \mathbb{R}; +, -, \cdot; \leq) \quad (\Rightarrow \text{BSS model})$$

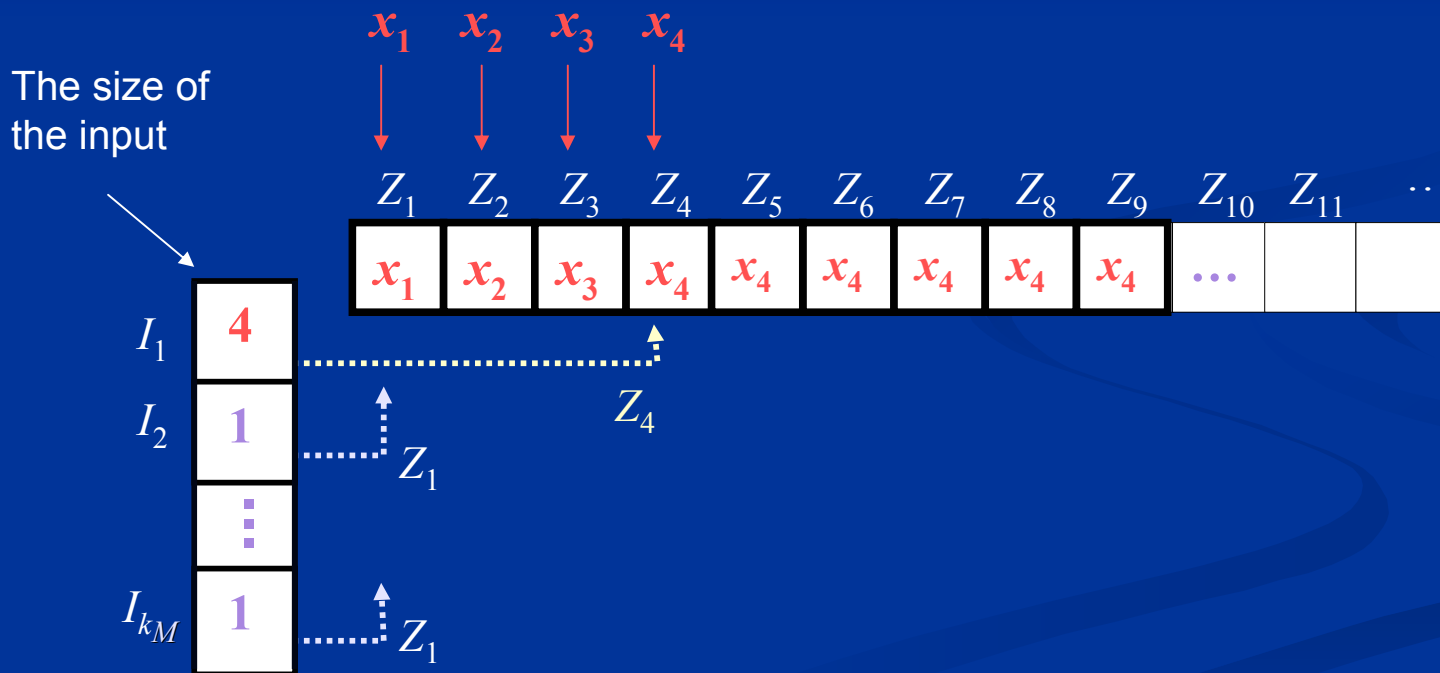
$$\Sigma_{\text{string}} = (\{0, 1\}^*; \varepsilon, 0, 1; \text{add}, \text{sub}_l, \text{sub}_r; =)$$

$$\Sigma_{\text{tree}} = (\text{tree}(\mathbb{R}); \text{nil}; \text{concat}, \text{root}, \text{sub}_l, \text{sub}_r; =)$$



The machine and the input

The **input**: $(Z_1, \dots, Z_n) := (x_1, \dots, x_n); I_1 := n; I_2 := 1; \dots; I_{k_M} := 1;$



Computation in polynomial time

For any machine M there is some polynomial p_M such that

M halts for $x = (x_1, \dots, x_n)$ within $p_M(n)$ steps.



One operation is executed within **one** time unit.

$\Rightarrow P_\Sigma \subseteq \text{DEC}_\Sigma$ ($P_\Sigma \triangleq$ problems are decidable in polynomial time)

Why do we consider the uniform model of computation?

In describing algorithms (for instance, in the computational geometry) we often use

- models over algebraic structures with several costs for operations,
- the BSS model with unit cost measure.

Important:

to investigate

- common properties
- differences

of several models, in order to answer:

- When can we use a model over an algebraic structure?
- Which simplification can imply problems?
- Which properties are necessary in order to get a special complexity for a problem?

The non-deterministic instructions

The non-determinism:

$\text{guess}(Z_k)$; Arbitrary elements can be guessed!

$$\Rightarrow P_{\Sigma} \subseteq NP_{\Sigma}$$

Some $P_\Sigma \stackrel{?}{=} NP_\Sigma$ problems for several structures

Σ	$P_\Sigma = NP_\Sigma?$
$(\mathbb{C}; \mathbb{C}; +, -, \cdot; =)$?
$(\mathbb{R}; \mathbb{R}; +, -, \cdot; \leq)$?
$(\mathbb{R}; \mathbb{R}; +, -, \cdot; =)$	no (\leq)
$(\mathbb{R}; \mathbb{R}; +, -; \leq)$?
$(\mathbb{R}; \mathbb{R}; +, -; =)$	no (Meer / Koiran)
$(\mathbb{Z}; \mathbb{Z}; +, -; \leq)$	no (even integers)
$(\mathbb{Z}; \mathbb{Z}; +, -; =)$	no (even integers)
$(\mathbb{Z}; 1; (\varphi_s)_{s \in \mathbb{Z}}; =)$ $\varphi_s(x) = sx$	no (no NP-complete problem)

Halting problems for Σ

$$H_{\Sigma} = \{\overbrace{(x_1, \dots, x_n)}^{\mathbf{x}}, \text{Code}(M) \mid$$

$\mathbf{x} \in U^{\infty}$ & M is a deterministic Σ -machine

& M halts on \mathbf{x} \}

$$H_{\Sigma}^{\text{spec}} = \{\text{Code}(M) \mid M \text{ is a deterministic } \Sigma\text{-machine}$$

& M halts on $\text{Code}(M)$ \}

Diagonalization techniques

The undecidability of the Halting problem H_Σ (for Turing machines)

1. **The set of machines is countable.** Assume that H_Σ^{spec} is decidable.

Halt?	bin(1)	...	bin(i)	...	bin(j)
M_1	yes / no						
\vdots		...					
M_i			yes				
\vdots				...			
M_j					no		
\vdots						...	
\vdots							
M	no / yes	...	no	...	yes



\Rightarrow **There is an M** recognizing the complement of H_Σ^{spec} . ⚡

Diagonalization techniques

The undecidability of the Halting problem H_Σ (for $(\mathbb{R}; \mathbb{R}; +, -, \cdot; \leq)$)

2. The codes of machines are ordered. Assume that H_Σ^{spec} is decidable.

Halt?	$Code(M_i)$...	$Code(M_j)$
⋮	...						
⋮		...					
M_i			yes				
⋮				...			
M_j					no		
⋮						...	
⋮							
M	no	...	yes



⇒ There is an M recognizing the complement of H_Σ^{spec} . ⚡

Diagonalization techniques

The undecidability of the Halting problem H_Σ (for any structure)

3. Σ arbitrary (We can generalize the result.)

Assume: H_Σ is decidable.

$\Rightarrow H_\Sigma^{\text{spec}}$ is decidable.

\Rightarrow The complement of H_Σ^{spec}
is semi-decidable by a Σ -machine M .

$\Rightarrow M$ halts on $\text{Code}(M)$

$\Leftrightarrow M$ does not halt on $\text{Code}(M)$.

$\Rightarrow \text{⚡}$



Oracle machines

Oracle query:

l : if $(Z_1, \dots, Z_{I_1}) \in B$ then goto l_1 else goto l_2 ;

The length can be computed by $I_1 := 1; I_1 := I_1 + 1; \dots$

B oracle, $B \subseteq U^\infty = \bigcup_{n \geq 1} U^n$

We will define oracles such that

$$P_\Sigma^Q \neq NP_\Sigma^Q,$$

$$P_\Sigma^O = NP_\Sigma^O.$$

(cp. also Baker, Gill, and Solovay; Emerson; ... for Turing machines...)

An oracle Q with $P_{\Sigma}^Q \neq NP_{\Sigma}^Q$

Diagonalization techniques by Baker, Gill, and Solovay

1. If the set of programs is **countable**, for any oracle $B \subseteq U^{\infty}$,

let N_i^B be the P_{Σ}^B -**machine**

- executing $p_i(n)$ instructions of program P_i for any $x \in U^n$. $a, b \in U$.
-

Proposition: $\{y \mid (\exists i \geq 1)(y \in U^{n_i} \ \& \ V_i \neq \emptyset)\} \in NP_{\Sigma}^Q \setminus P_{\Sigma}^Q$.

An oracle Q with $P_{\Sigma}^Q \neq NP_{\Sigma}^Q$

Diagonalization techniques by Baker, Gill, and Solovay

The set of programs is countable. $a, b \in U$.

P_i	p_i	n_i	Length in a query	$(a, \dots, a) \in U^{n_i}$	$Q = Q_{\Sigma} = \bigcup_{i \geq 1} W_i$
P_1	p_1	$p_1(n_1) + n_1 < 2^{n_1}$	$\leq p_1(n_1) + n_1$ $< n_2$	rejected accepted	$W_1 = \{ \mathbf{x} \mid \mathbf{x} \in U^{n_1} \ \& \ \mathbf{x} \text{ not queried...} \}$ $W_1 = \emptyset$
\vdots	\vdots				
P_i	p_i	$2^{n_i-1} < n_i$ $p_i(n_i) + n_i < 2^{n_i}$	$\leq p_i(n_i) + n_i$ $< n_{i+1}$	rejected	$W_{i+1} = W_i \cup \{ \mathbf{x} \mid \mathbf{x} \in U^{n_i} \ \& \ \mathbf{x} \text{ not queried by } N_i^{W_i} \text{ on } (a, \dots, a) \in U^{n_i} \}$
\vdots	\vdots				
P_j	p_j	$2^{n_j-1} < n_j$ $p_j(n_j) + n_j < 2^{n_j}$	$\leq p_j(n_j) + n_j$ $< n_{j+1}$	accepted	$W_{j+1} = W_j$
\vdots	\vdots			...	

$\Rightarrow N_u^{W_i}$ rejects $(a, \dots, a) \Leftrightarrow N_u^{W_{i+1}}$ rejects $(a, \dots, a) \Leftrightarrow N_u^Q$ rejects (a, \dots, a) .

An oracle Q with $P_{\Sigma}^Q \neq NP_{\Sigma}^Q$

Diagonalization techniques by Baker, Gill, and Solovay

1. If the set of programs is **countable**, for any oracle $B \subseteq U^{\infty}$,

let N_i^B be the P_{Σ}^B -**machine**

- executing $p_i(n)$ instructions of program P_i for any $x \in U^n$. $a, b \in U$.

$V_0 = \emptyset, m_0 = 0$.

Stage $i \geq 1$: Let $n_i > m_{i-1}$, $m_i = 2^{n_i}$, $p_i(n_i) + n_i < m_i$.

$W_i = \cup_{j < i} V_j$

$V_i = \{x \in U^{n_i} \mid N_i^{W_i} \text{ rejects } (a, \dots, a) \in U^{n_i}$

& x is not queried by $N_i^{W_i}$ on $(a, \dots, a) \in U^{n_i}\}$

$Q = Q_{\Sigma} = \cup_{i \geq 1} W_i$

Proposition: $\{y \mid (\exists i \geq 1)(y \in U^{n_i} \ \& \ V_i \neq \emptyset)\} \in NP_{\Sigma}^Q \setminus P_{\Sigma}^Q$.

Diagonalization
technique

An oracle Q with $P_{\Sigma}^Q \neq NP_{\Sigma}^Q$

Diagonalization techniques by Emerson

2. If U is **ordered**, for suitable codes $u \in U \subseteq U^{\infty}$ and any oracle $B \subseteq U^{\infty}$,

let N_u^B be the P_{Σ}^B -**machine**

- executing $p_u(n)$ instructions of program P_u for any $x \in U^n$.

$\mathbb{N} \subseteq U$.

Proposition: $\{y \mid (\exists n \geq 2) ((n, y) \in Q_{\Sigma})\} \in NP_{\Sigma}^Q \setminus P_{\Sigma}^Q$.

An oracle Q with $P_{\Sigma}^Q \neq NP_{\Sigma}^Q$

Diagonalization techniques by Emerson

U ordered and $\mathbb{N} \subseteq U$.

K_i	elements in a query on $u \in K_i$ within a time period bounded by $p_u(u)$	$Q = Q_{\Sigma} = \bigcup_{i \geq 1} W_i$
K_1	≤ 1	$W_1 = \emptyset$
\vdots		
K_i	$\leq i$	$W_{i+1} = W_i \cup \{(i+1, u) \mid u \in K_i \ \& \ N_u^{W_i} \text{ rejects } u\}$
\vdots		

$\Rightarrow N_u^{W_i}$ rejects $u \iff N_u^Q$ rejects u .

An oracle Q with $P_{\Sigma}^Q \neq NP_{\Sigma}^Q$

Diagonalization techniques by Emerson

2. If U is **ordered**, for suitable codes $u \in U \subseteq U^\infty$ and any oracle $B \subseteq U^\infty$,

let N_u^B be the P_{Σ}^B -**machine**

- executing $p_u(n)$ instructions of program P_u for any $x \in U^n$.

$\mathbb{N} \subseteq U$.

$V_0 = \emptyset$.

Stage $i \geq 1$:

$K_i = \{u \in U \mid (\forall j > i)(\forall B \subseteq U^\infty)$
 $(j \in U \text{ is not queried by } N_u^B \text{ on } u)\}$

$W_{i+1} = W_i \cup \{(i+1, u) \mid u \in K_i \ \& \ N_u^{W_i} \text{ rejects } u\}$

$Q = Q_{\Sigma} = \cup_{i \geq 1} W_i$

Proposition: $\{y \mid (\exists n \geq 2) ((n, y) \in Q_{\Sigma})\} \in NP_{\Sigma}^Q \setminus P_{\Sigma}^Q$.

An oracle Q with $P_{\Sigma}^Q \neq NP_{\Sigma}^Q$

Diagonalization techniques (a generalization)

3. If U is **infinite**, for suitable codes $u \in U \subseteq U^{\infty}$ and any oracle $B \subseteq U^{\infty}$, let N_u^B be the P_{Σ}^B -**machine**
- executing $p_u(n)$ instructions of program P_u for any $x \in U^n$.
- $\alpha_1, \alpha_2, \alpha_3, \dots \in U$.
-

Proposition: $\{y \mid (\exists n \geq 2) ((\alpha_n, y) \in Q_{\Sigma})\} \in NP_{\Sigma}^Q \setminus P_{\Sigma}^Q$.

An oracle Q with $P_{\Sigma}^Q \neq NP_{\Sigma}^Q$

Diagonalization techniques (a generalization)

Σ arbitrary, $\alpha_1, \alpha_2, \alpha_3, \dots \in U$.

K_i	elements in a query on $u \in K_i$ within a time period bounded by $p_u(u)$	$Q = Q_{\Sigma} = \bigcup_{i \geq 1} W_i$
K_1	$\notin \{\alpha_1, \alpha_2, \alpha_3, \dots\}$	$W_1 = \emptyset$
\vdots		
K_i	$\notin \{\alpha_{i+1}, \alpha_{i+2}, \alpha_{i+3}, \dots\}$	$W_{i+1} = W_i \cup \{(\alpha_{i+1}, u) \mid u \in K_i \text{ \& } N_u^{W_i} \text{ rejects } u\}$
\vdots		

$$\Rightarrow N_u^{W_i} \text{ rejects } u \iff N_u^Q \text{ rejects } u.$$

An oracle Q with $P_\Sigma^Q \neq NP_\Sigma^Q$

Diagonalization techniques (a generalization)

3. If U is infinite, for suitable codes $u \in U \subseteq U^\infty$ and any oracle $B \subseteq U^\infty$, let N_u^B be the P_Σ^B -machine

- executing $p_u(n)$ instructions of program P_u for any $x \in U^n$.

$\alpha_1, \alpha_2, \alpha_3, \dots \in U$.

$$V_0 = \emptyset.$$

Stage $i \geq 1$:

$$K_i = \{u \in U \mid (\forall j > i)(\forall B \subseteq U^\infty) \\ (N_u^B \text{ does not compute or use the value } \alpha_j \text{ on } u)\}$$

$$W_{i+1} = W_i \cup \{(\alpha_{i+1}, u) \mid u \in K_i \text{ \& } N_u^{W_i} \text{ rejects } u\}$$

$$Q = Q_\Sigma = \bigcup_{i \geq 1} W_i$$

Proposition: $\{y \mid (\exists n \geq 2) ((\alpha_n, y) \in Q_\Sigma)\} \in NP_\Sigma^Q \setminus P_\Sigma^Q$.

An oracle Q with $P_{\Sigma}^Q \neq NP_{\Sigma}^Q$

Using the undecidability of the Halting problem H_{Σ}

4. U infinite,
a finite number of operations and relations,

$\{\alpha_1, \alpha_2, \alpha_3, \dots\} \subseteq U$ enumerable and decidable.

$$Q = Q_{\Sigma} = \{ (\alpha_t, \mathbf{x}, Code(M)) \mid$$

$\mathbf{x} \in U^{\infty}$ & M is a deterministic Σ -machine

& $M(\mathbf{x}) \downarrow^t$

M accepts $\mathbf{x} = (x_1, \dots, x_n) \in U^{\infty}$ within t steps.

Proposition: $H_{\Sigma} \in NP_{\Sigma}^Q \setminus P_{\Sigma}^Q$. $(P_{\Sigma}^Q \subseteq DEC_{\Sigma})$

An oracle O_Σ with $P_\Sigma^{O_\Sigma} = NP_\Sigma^{O_\Sigma}$

A universal oracle:

$$O = O_\Sigma = \{ (\overbrace{b, \dots, b}^{\in U^t}, \mathbf{x}, \text{Code}(M)) \mid$$

$\mathbf{x} \in U^\infty$ & M is a non-deterministic Σ -machine using O

& $M(\mathbf{x}) \downarrow^t \}$

Proposition: $P_\Sigma^O = NP_\Sigma^O$.

An oracle O_Σ containing only tuples of length 1
with $P_\Sigma^{O_\Sigma} = NP_\Sigma^{O_\Sigma}$?

Structures over strings

$\Sigma = (U^*; \varepsilon, a, b, c_3, \dots, c_u; \text{add}, \text{sub}_l, \text{sub}_r, f_1, \dots, f_v; R_1, \dots, R_w, =)$

$(d_1, \dots, d_k) \in U^k \subset U^\infty$ stored in k registers

$s = d_1 \cdots d_k \in U^*$ stored in **one** register

$d \in U$



$\text{add}(s, d) = sd$

$\text{sub}_l(sd) = s$

$\text{sub}_r(sd) = d$

An oracle O_Σ containing only tuples of length 1 with $P_\Sigma^{O_\Sigma} = NP_\Sigma^{O_\Sigma}$?

Recall: $P_\Sigma^{O_\Sigma} = NP_\Sigma^{O_\Sigma}$ and $P_\Sigma^{Q_\Sigma} \neq NP_\Sigma^{Q_\Sigma}$ for

$O_\Sigma = \{ (\underbrace{b, \dots, b}_{t \times}, x, Code(M)) \mid x \in (U^*)^\infty \}$
& M is a non-deterministic Σ -machine using O_Σ & $M(x) \downarrow^t$

$Q_\Sigma = \{ (\underbrace{b \cdots b}_{t \times}, x, Code(M)) \mid x \in (U^*)^\infty \}$
& M is a deterministic Σ -machine & $M(x) \downarrow^t$

Theorem: There is **not** an oracle O with

$b \cdots b \cdot \text{string}(x) \cdot \text{string}(Code(M)) \in O$

$\Leftrightarrow x \in (U^*)^\infty$

& M is a non-deterministic Σ -machine using O

& $M(x) \downarrow^t$.



Structures with $P = NP$

An additional relation R
on **padded** codes
of the members of a universal oracle O
with $P_{\Sigma^O} = NP_{\Sigma^O}$

$P = NP$
for

Binary trees
with decidable identity
relation
(Gaßner, Dagstuhl 2004)

$P = NP$
for

Strings
with operations for
adding and deleting the
last character
(Gaßner, CiE 2007)

\mathbb{Z} as oracle with $P_{\mathbb{R}}^{\mathbb{Z}} \neq NP_{\mathbb{R}}^{\mathbb{Z}}$

Using the properties of $(\mathbb{R}; \mathbb{R}; +, -, \cdot; \leq)$

5. $\Sigma = (\mathbb{R}; \mathbb{R}; +, -, \cdot; \leq)$ or $\Sigma = (\mathbb{R}; \mathbb{R}; +, -, \cdot; =)$

$Q \in NP_{\mathbb{R}}^{\mathbb{Z}}$.

Program: guess(y_1); guess(y_2); if $y_1, y_2 \in \mathbb{Z}, y_1 \neq 0$ and $y_1 x = y_2$ then output 1.

Proposition: $P_{\mathbb{R}}^{\mathbb{Z}} \neq NP_{\mathbb{R}}^{\mathbb{Z}}$.

\mathbb{Z} as oracle with $\mathbf{P}_{\mathbb{R}}^{\mathbb{Z}} \neq \mathbf{NP}_{\mathbb{R}}^{\mathbb{Z}}$

Using the properties of $(\mathbb{R}; \mathbb{R}; +, -, \cdot; \leq)$

5. $\Sigma = (\mathbb{R}; \mathbb{R}; +, -, \cdot; \leq)$ or $\Sigma = (\mathbb{R}; \mathbb{R}; +, -, \cdot; =)$

$\mathbb{Q} \in \mathbf{NP}_{\mathbb{R}}^{\mathbb{Z}}$.

Program: guess(y_1); guess(y_2); if $y_1, y_2 \in \mathbb{Z}, y_1 \neq 0$ and $y_1 x = y_2$ then output 1.

Assume that \mathbb{Q} is decidable by a machine M .

Description of any computation path by a system of conditions of the form

$$p_k(x) \in \mathbb{Z} \quad p_k(x) \notin \mathbb{Z} \quad p_k(x) \leq 0 \quad p_k(x) < 0 \quad (k \leq m).$$

\Rightarrow There are $r \notin \mathbb{Q} \cup \{x \mid p_k(x) \in \mathbb{Z}\}$ and $(q_i)_{i \in \mathbb{N}}$ such that $q_i \in \mathbb{Q}$ and $q_i \rightarrow r$.

$\Rightarrow r$ and some q_j satisfy the same conditions $p_k(x) \notin \mathbb{Z}$ and $p_k(x) < 0$.

$\Rightarrow r$ and q_j are rejected. $\Rightarrow \zeta$

Proposition: $\mathbf{P}_{\mathbb{R}}^{\mathbb{Z}} \neq \mathbf{NP}_{\mathbb{R}}^{\mathbb{Z}}$.

On Relativizations of the $P \stackrel{?}{=} NP$ Question for Several Structures

Thank you for your attention!

Christine Gaßner
Greifswald.

Thanks also to

Robert Bialowons,
Volkmar Liebscher,
Rainer Schimming.