Die Komplexitätsklasse NP_R (in Bsp. über Ringe $\{0,1\},\mathbb{Z},\mathbb{R}$)

Björn Deiseroth

Seminar: Reelle Komplexität
04.07.2011

TU Darmstadt
PD Dr. habil. Ulrike Brandt, Prof. Dr. Ziegler
M.Sc. Rösnick

Gliederung

1. Motivation für Komplexitätsklassen
2. Die Klasse NP_R
   - Rückblick & Vorbereitung
   - Definition der Klasse
   - Härte & Vollständigkeit
3. SA/QA-FEAS ist NP_R-vollständig
   - Sichtung & Vorbereitung
   - Zugehörigkeit,
   - Härte $\Rightarrow$ Vollständigkeit
4. Weitere Probleme und Resultate in $\mathrm{NP}_{\{0,1\}/\mathbb{Z}/\mathbb{R}}$

[Motivation für Komplexitätsklassen]

Probleme

Von Methodiken finden, zum Benutzen.

- NP mehrfach benutzt/ gehört (in $\mathbb{Z}_2$)
  - (oft) Lösung finden schwer, Verifikation jedoch einfach
- Allgemeineres Modell finden, weiter differenzieren
  - abhängig von unterliegender Struktur

- Funde: “universelle” Probleme
  - z.B. SA/QA-FEAS, SAT
- Reduktion von P = NP auf solche Probleme

Probleme

Von Methodiken finden, zum Benutzen.

- NP mehrfach benutzt/ gehört (in $\mathbb{Z}_2$)
  - (oft) Lösung finden schwer, Verifikation jedoch einfach
- Allgemeineres Modell finden, weiter differenzieren
  - abhängig von unterliegender Struktur

- Funde: “universelle” Probleme
  - z.B. SA/QA-FEAS, SAT
- Reduktion von P = NP auf solche Probleme

Probleme

Von Methodiken finden, zum Benutzen.

- NP mehrfach benutzt/ gehört (in $\mathbb{Z}_2$)
  - (oft) Lösung finden schwer, Verifikation jedoch einfach
- Allgemeineres Modell finden, weiter differenzieren
  - abhängig von unterliegender Struktur

- Funde: “universelle” Probleme
  - z.B. SA/QA-FEAS, SAT
- Reduktion von P = NP auf solche Probleme

[Die Klasse NP_R]

Maschine

Maschine über R:
endlicher, verbundener, gerichteter Graph

mit 5 Knotentypen: *input, computation, branch, output, shift*
(deren Abbildungen)

$$R^\infty = \bigsqcup_{n\geq 0}^{\infty} R^n,\ x \in R_\infty : x = (\ldots, x_{-2}, x_{-1}, x_0.x_1, x_2, \ldots),$$
$$x_i \in R,\ |k| > L \Rightarrow x_k = 0$$
$$\mathcal{I}_M, O_M \subseteq R^\infty,\ S_M \subseteq R_\infty$$
$$\Omega_T = \{x \in \mathcal{I}_M | T_M(x) \leq T\}$$

Maschine

Maschine über R:
endlicher, verbundener, gerichteter Graph

mit 5 Knotentypen: *input*, *computation*, *branch*, *output*, *shift*
(deren Abbildungen)

$$R^\infty = \bigsqcup_{n\geq 0}^{\infty} R^n,\ x \in R_\infty : x = (\ldots, x_{-2}, x_{-1}, x_0.x_1, x_2, \ldots),$$
$$x_i \in R,\ |k| > L \Rightarrow x_k = 0$$

$$\mathcal{I}_M, \mathcal{O}_M \subseteq R^\infty,\ S_M \subseteq R_\infty$$

$$\Omega_T = \{x \in \mathcal{I}_M | T_M(x) \leq T\}$$

Instrumentarium I/II

für $x \in R^n$

- $\mathrm{ht}_R(x_i)$ (z.B. $\max(\lceil \log(|p_i|+1) \rceil, \ldots)$ für $R = \mathbb{Q}$, *bit-cost*)
- $\mathrm{length}(x) = n$
- $\mathrm{size}(x) = n \cdot \mathrm{ht}_R(x) = n \cdot \max \mathrm{ht}_R(x_i)$
- $\mathrm{ht}_{max}(x)$ analog ht_R, für Zustandsbahn
- $\mathrm{cost}_M(x) = T_M(x) \times \mathrm{ht}_{max}(x)$
- guess: Befehl für nicht-determ. Eingabe

idR benutzt: *unit-cost* $\Rightarrow$ *unit height*: $\mathrm{ht}_R(x) = 1$

Instrumentarium I/II

für $x \in R^n$

- $\mathrm{ht}_R(x_i)$ (z.B. $\max(\lceil \log(|p_i|+1) \rceil, \ldots)$ für $R = \mathbb{Q}$, *bit-cost*)
- $\mathrm{length}(x) = n$
- $\mathrm{size}(x) = n \cdot \mathrm{ht}_R(x) = n \cdot \max \mathrm{ht}_R(x_i)$
- $\mathrm{ht}_{max}(x)$ analog ht_R, für Zustandsbahn
- $\mathrm{cost}_M(x) = T_M(x) \times \mathrm{ht}_{max}(x)$
- guess: Befehl für nicht-determ. Eingabe

idR benutzt: *unit-cost* $\Rightarrow$ *unit height*: $\mathrm{ht}_R(x) = 1$

Instrumentarium I/II

für $x \in R^n$

- $\mathrm{ht}_R(x_i)$ (z.B. $\max(\lceil \log(|p_i|+1) \rceil, \ldots)$ für $R = \mathbb{Q}$, *bit-cost*)
- $\mathrm{length}(x) = n$
- $\mathrm{size}(x) = n \cdot \mathrm{ht}_R(x) = n \cdot \max \mathrm{ht}_R(x_i)$
- $\mathrm{ht}_{max}(x)$ analog ht_R, für Zustandsbahn
- $\mathrm{cost}_M(x) = T_M(x) \times \mathrm{ht}_{max}(x)$
- guess: Befehl für nicht-determ. Eingabe

idR benutzt: *unit-cost* $\Rightarrow$ *unit height*: $\mathrm{ht}_R(x) = 1$

Instrumentarium II/II

$S \longleftrightarrow (X, X_{yes})$, $S, X \subseteq R^\infty, X_{yes} \subseteq X$:
Entscheidungsproblem (un)strukturiert überführbar

$\varphi : X \to Y$ p-reduzierbar: "$\hookrightarrow_p$"
strukturerhaltender Morphismus, polynomiell berechenbar

$g : R_\infty \to R_\infty$ "Dimension m" definiert durch m Polynome:
$(g(x))_i = g_i(x)$, $i = 1 \ldots m$; $(g(x))_i = x_i$ sonst
$g_i(x) = g'_i(x_1, \ldots, x_m)$ für $g'_i : R^m \to R$ Polynome

Branch/ Computation nodes sind Polynome in R_∞
K_M, D_M sind maximal auftretendende Dimension bzw. Grad

Instrumentarium II/II

$S \longleftrightarrow (X, X_{yes})$, $S, X \subseteq R^\infty, X_{yes} \subseteq X$:
Entscheidungsproblem (un)strukturiert überführbar

$\varphi : X \to Y$ p-reduzierbar: "$\hookrightarrow_p$"
strukturerhaltender Morphismus, polynomiell berechenbar

$g : R_\infty \to R_\infty$ "Dimension m" definiert durch m Polynome:
$(g(x))_i = g_i(x)$, $i = 1 \ldots m$; $(g(x))_i = x_i$ sonst
$g_i(x) = g'_i(x_1, \ldots, x_m)$ für $g'_i : R^m \to R$ Polynome

Branch/ Computation nodes sind Polynome in R_∞
K_M, D_M sind maximal auftretendende Dimension bzw. Grad

Instrumentarium II/II

$S \longleftrightarrow (X, X_{yes})$, $S, X \subseteq R^\infty, X_{yes} \subseteq X$:
Entscheidungsproblem (un)strukturiert überführbar

$\varphi : X \to Y$ p-reduzierbar: "$\hookrightarrow_p$"
strukturerhaltender Morphismus, polynomiell berechenbar

$g : R_\infty \to R_\infty$ "Dimension m" definiert durch m Polynome:
$(g(x))_i = g_i(x)$, $i = 1 \ldots m$; $(g(x))_i = x_i$ sonst
$g_i(x) = g'_i(x_1, \ldots, x_m)$ für $g'_i : R^m \to R$ Polynome

Branch/ Computation nodes sind Polynome in R_∞
K_M, D_M sind maximal auftretendende Dimension bzw. Grad

Instrumentarium II/II

$S \longleftrightarrow (X, X_{yes})$, $S, X \subseteq R^\infty, X_{yes} \subseteq X$:
Entscheidungsproblem (un)strukturiert überführbar

$\varphi : X \to Y$ p-reduzierbar: "$\hookrightarrow_p$"
strukturerhaltender Morphismus, polynomiell berechenbar

$g : R_\infty \to R_\infty$ "Dimension m" definiert durch m Polynome:
$(g(x))_i = g_i(x)$, $i = 1 \ldots m$; $(g(x))_i = x_i$ sonst
$g_i(x) = g'_i(x_1, \ldots, x_m)$ für $g'_i : R^m \to R$ Polynome

Branch/ Computation nodes sind Polynome in R_∞
K_M, D_M sind maximal auftretendende Dimension bzw. Grad

Formale Definition von NP_R

D1 $S \subseteq R^\infty$ Entscheidungsproblem.
$S \in \mathrm{NP}_R$, falls $\exists M$ mit $\mathcal{I}_M = R^\infty \times R^\infty, c, q \in \mathbb{N}$.

E1) $x \in S \Rightarrow \exists w \in R^\infty.\ \Phi_M(x,w) = 1,\ \mathrm{cost}_M(x,w) \leq c \cdot \mathrm{size}(x)^q$

E2) $x \notin S \Rightarrow \nexists w \in R^\infty.\ \Phi_M(x,w) = 1$

$\Rightarrow$ Spezialfall: $R = \mathbb{Z}_2$ “klassisch”

$\Rightarrow$ w reicht mit Bedingungen:
$\mathrm{size}(x,w) \leq c \cdot \mathrm{size}(x)^p + K_M,\ \mathrm{ht}_R(w) \leq c \cdot \mathrm{size}(x)^q$

$\Rightarrow$ E3) $\forall x \in X, w \in R^\infty.\ \mathrm{cost}_M(x,w) \leq c \cdot \mathrm{size}(x)^q,\ \Phi_M(x,w) \in \{0,1\}$

Formale Definition von NP_R

D1 $S \subseteq R^\infty$ Entscheidungsproblem.
$S \in \mathrm{NP}_R$, falls $\exists M$ mit $\mathcal{I}_M = R^\infty \times R^\infty, c, q \in \mathbb{N}$.

E1) $x \in S \Rightarrow \exists w \in R^\infty.\ \Phi_M(x,w) = 1,\ \mathrm{cost}_M(x,w) \leq c \cdot \mathrm{size}(x)^q$

E2) $x \notin S \Rightarrow \nexists w \in R^\infty.\ \Phi_M(x,w) = 1$

$\Rightarrow$ Spezialfall: $R = \mathbb{Z}_2$ “klassisch”

$\Rightarrow$ w reicht mit Bedingungen:
$\mathrm{size}(x,w) \leq c \cdot \mathrm{size}(x)^p + K_M,\ \mathrm{ht}_R(w) \leq c \cdot \mathrm{size}(x)^q$

$\Rightarrow$ E3) $\forall x \in X, w \in R^\infty.\ \mathrm{cost}_M(x,w) \leq c \cdot \mathrm{size}(x)^q,\ \Phi_M(x,w) \in \{0,1\}$

Formale Definition von NP_R

D1 $S \subseteq R^\infty$ Entscheidungsproblem.
$S \in \mathrm{NP}_R$, falls $\exists M$ mit $\mathcal{I}_M = R^\infty \times R^\infty, c, q \in \mathbb{N}$.

E1) $x \in S \Rightarrow \exists w \in R^\infty.\ \Phi_M(x,w) = 1,\ \mathrm{cost}_M(x,w) \leq c \cdot \mathrm{size}(x)^q$

E2) $x \notin S \Rightarrow \nexists w \in R^\infty.\ \Phi_M(x,w) = 1$

$\Rightarrow$ Spezialfall: $R = \mathbb{Z}_2$ “klassisch”

$\Rightarrow$ w reicht mit Bedingungen:
$\mathrm{size}(x,w) \leq c \cdot \mathrm{size}(x)^p + K_M,\ \mathrm{ht}_R(w) \leq c \cdot \mathrm{size}(x)^q$

$\Rightarrow$ E3) $\forall x \in X, w \in R^\infty.\ \mathrm{cost}_M(x,w) \leq c \cdot \mathrm{size}(x)^q,\ \Phi_M(x,w) \in \{0,1\}$

Reduktion von Entscheidungsproblemen

S1 $S \hookrightarrow_p S', S' \in \mathrm{NP}_R \Rightarrow S \in \mathrm{NP}_R$

B φ Reduktion in polynomieller Zeit,
M' eine NP_R Entscheidungsmaschine für S'

Maschine M:
input x
2: compute y := $\varphi(x)$
guess $w \in R^\infty$
4: compute z := $\Phi_{M'}(y, w)$
output z

Reduktion von Entscheidungsproblemen

S1 $S \hookrightarrow_p S', S' \in \mathrm{NP}_R \Rightarrow S \in \mathrm{NP}_R$

B φ Reduktion in polynomieller Zeit,
M' eine NP_R Entscheidungsmaschine für S'

Maschine M:
input x
2: compute y := $\varphi(x)$
guess $w \in R^\infty$
4: compute z := $\Phi_{M'}(y, w)$
output z

Algebraische Definition

D2 berechenbare Abbildung $\varphi : R^\infty \to R^\infty$ heisst *ehrlich* auf $V \subset R^\infty$, falls gilt: $\exists c, q \in \mathbb{N}.\ \forall v \in V.\ \mathrm{size}(v) \leq c \cdot \mathrm{size}(\varphi(v))^q$

S2 $S \in \mathrm{NP}_R \Leftrightarrow S = \varphi(V)$,
für ein $V \in \mathrm{P}_R$, φ auf V ehrlicher p-Morphismus

Algebraische Definition

D2 berechenbare Abbildung $\varphi : R^\infty \to R^\infty$ heisst *ehrlich* auf $V \subset R^\infty$, falls gilt: $\exists c, q \in \mathbb{N}.\ \forall v \in V.\ \mathrm{size}(v) \leq c \cdot \mathrm{size}(\varphi(v))^q$

S2 $S \in \mathrm{NP}_R \Leftrightarrow S = \varphi(V)$,
für ein $V \in \mathrm{P}_R$, φ auf V ehrlicher p-Morphismus

Beweis Algebraische Definition 1/4

"$S \in \mathrm{NP}_R \Rightarrow \underline{\exists \varphi.\ S = \varphi(V),\ \varphi \text{ ehrl.}}\ ,\ V \in P_R$":

$S \in \mathrm{NP}_R$ mit M, p_M Kostenschranke, $X = R^\infty \times R^\infty$,

$$V = \{(x,w) \in X \mid x \in S,\ \mathrm{size}(x,w) \leq p_M(\mathrm{size}(x)) + K_M,\ \Phi_M(x,w) = 1\}$$

$\varphi(x,w) = x$ für $(x,w) \in X$

$\varphi(V) = S$ ist ehrlicher p-Morphismus

Beweis Algebraische Definition 1/4

"$S \in \mathrm{NP}_R \Rightarrow \underline{\exists \varphi.\ S = \varphi(V),\ \varphi \text{ ehrl.}}\ ,\ V \in P_R$":

$S \in \mathrm{NP}_R$ mit M, p_M Kostenschranke, $X = R^\infty \times R^\infty$,

$$V = \{(x,w) \in X \mid\ x \in S,\ \mathrm{size}(x,w) \leq p_M(\mathrm{size}(x)) + K_M,\ \Phi_M(x,w) = 1\}$$

$\varphi(x,w) = x$ für $(x,w) \in X$

$\varphi(V) = S$ ist ehrlicher p-Morphismus

Beweis Algebraische Definition 1/4

"$S \in \mathrm{NP}_R \Rightarrow \underline{\exists \varphi.\ S = \varphi(V),\ \varphi \text{ ehrl.}}\ ,\ V \in P_R$":

$S \in \mathrm{NP}_R$ mit M, p_M Kostenschranke, $X = R^\infty \times R^\infty$,

$$V = \{(x,w) \in X \mid\ x \in S,\ \mathrm{size}(x,w) \leq p_M(\mathrm{size}(x)) + K_M,\ \Phi_M(x,w) = 1\}$$

$\varphi(x,w) = x$ für $(x,w) \in X$

$\varphi(V) = S$ ist ehrlicher p-Morphismus

Beweis Algebraische Definition 2/4

"$S \in \mathrm{NP}_R \Rightarrow \exists \varphi.\ S = \varphi(V)$, φ ehrl. , $V \in P_R$":

Maschine M^*:
input $(x, w) \in X$
2: if $\mathrm{size}(x, w) > p_M(\mathrm{size}(x)) + K_M$ output 0
else output $\Phi_M(x, w)$

✓ M^* ist plynomiell auf X
✓ $\Phi_{M^*}(V) = \{1\}$
$\Phi_{M^*}(X \setminus V) = \{0\}$

$\Rightarrow V \in \mathrm{P}_R$

Beweis Algebraische Definition 2/4

"$S \in \mathrm{NP}_R \Rightarrow \exists \varphi.\ S = \varphi(V)$, φ ehrl. , $V \in P_R$":

Maschine M^*:
input $(x, w) \in X$
2: if $\mathrm{size}(x, w) > p_M(\mathrm{size}(x)) + K_M$ output 0
else output $\Phi_M(x, w)$

✓ M^* ist plynomiell auf X

✓ $\Phi_{M^*}(V) = \{1\}$

$\Phi_{M^*}(X \setminus V) = \{0\}$

$\Rightarrow V \in \mathrm{P}_R$

Beweis Algebraische Definition 2/4

"$S \in \mathrm{NP}_R \Rightarrow \exists \varphi.\ S = \varphi(V)$, φ ehrl. , $V \in P_R$":

Maschine M^*:
input $(x, w) \in X$
2: if size$(x, w) > p_M(\text{size}(x)) + K_M$ output 0
else output $\Phi_M(x, w)$

✓ M^* ist plynomiell auf X

✓ $\Phi_{M^*}(V) = \{1\}$
$\Phi_{M^*}(X \setminus V) = \{0\}$

$\Rightarrow$ $V \in \mathrm{P}_R$

Beweis Algebraische Definition 3/4

"$S \in \mathrm{NP}_R \Leftarrow \exists \varphi.\ S = \varphi(V),\ \varphi$ ehrl. , $V \in P_R$":

$V \in \mathrm{P}_R$, M entscheidet V mit Kostenschranke: p_M,

φ ehrlicher p-Morphismus auf V, $S = \varphi(V)$,
p_φ, p_V polynomielle Schranke für Kosten und size

Beweis Algebraische Definition 4/4

"$S \in \mathrm{NP}_R \Leftarrow \exists \varphi.\ S = \varphi(V),\ \varphi$ ehrl. , $V \in P_R$":

Maschine M^*:
input $x \in R^\infty$
guess $v \in R^\infty$
if size$(v) >$ size$(x))$ output 0
else if $\Phi_M(v) = 0$ then output 0
else if $\varphi(v) = x$ then output 1
else output 0

- ✓ M^* ist polynomiell in size(x)
- ✓ $x \in S \Leftrightarrow \exists v \in V.\ \varphi(v) = x \Leftrightarrow$
  $\Phi_M(v) = 1,\ \mathrm{size}(v) \leq p_V(\mathrm{size}(x)) \Leftrightarrow \Phi_{M^*}(x, v) = 1$

Beweis Algebraische Definition 4/4

"$S \in \mathrm{NP}_R \Leftarrow \exists \varphi.\ S = \varphi(V),\ \varphi$ ehrl. , $V \in P_R$":

Maschine M^*:
input $x \in R^\infty$
2: guess $v \in R^\infty$
if size$(v) >$ size$(x))$ output 0
4: else if $\Phi_M(v) = 0$ then output 0
else if $\varphi(v) = x$ then output 1
6: else output 0

✓ M^* ist polynomiell in size(x)
✓ $x \in S \Leftrightarrow \exists v \in V.\ \varphi(v) = x \Leftrightarrow$
$\Phi_M(v) = 1,\ \mathrm{size}(v) \leq p_V(\mathrm{size}(x)) \Leftrightarrow \Phi_{M^*}(x, v) = 1$

Beweis Algebraische Definition 4/4

"$S \in \mathrm{NP}_R \Leftarrow \exists \varphi.\ S = \varphi(V),\ \varphi$ ehrl. , $V \in P_R$":

Maschine M^*:
input $x \in R^\infty$
2: guess $v \in R^\infty$
if size$(v) >$ size$(x))$ output 0
4: else if $\Phi_M(v) = 0$ then output 0
else if $\varphi(v) = x$ then output 1
6: else output 0

- ✓ M^* ist polynomiell in size(x)
- ✓ $x \in S \Leftrightarrow \exists v \in V.\ \varphi(v) = x \Leftrightarrow$
  $\Phi_M(v) = 1,\ \mathrm{size}(v) \leq p_V(\mathrm{size}(x)) \Leftrightarrow \Phi_{M^*}(x, v) = 1$

Folgerung algebraischer Definition

gezeigt:

$S \in \mathrm{NP}_R \Leftrightarrow \exists \varphi.\ S = \varphi(V),\ \varphi$ ehrl. , $V \in P_R$

es folgt:

$\mathrm{P}_R \subseteq \mathrm{NP}_R$

Folgerung algebraischer Definition

gezeigt:
$S \in \mathrm{NP}_R \Leftrightarrow \exists \varphi.\ S = \varphi(V),\ \varphi$ ehrl. , $V \in P_R$
es folgt:
$\mathrm{P}_R \subseteq \mathrm{NP}_R$

Folgerung algebraischer Definition

K1 Für beliebigen Ring R gilt: $\mathrm{P}_R \subseteq \mathrm{NP}_R$

B $\varphi = \mathrm{id}$ in Satz 2

! $\mathrm{NP} \subseteq \mathrm{EXP}$ nur für $\mathbb{Z}_2$ klar

Folgerung algebraischer Definition

K1 Für beliebigen Ring R gilt: $\mathrm{P}_R \subseteq \mathrm{NP}_R$

B $\varphi = \mathrm{id}$ in Satz 2

! NP $\subseteq$ EXP nur für $\mathbb{Z}_2$ klar

Härte

D3 $\widehat{S}$ heisst NP_R-*hart*, falls: $\forall S \in \mathrm{NP}_R.\ S \hookrightarrow_p \widehat{S}$

S7 $\widehat{S}$ NP_R-hart, $\widehat{S} \hookrightarrow_p S \Rightarrow S$ NP_R-hart

Härte

D3 $\widehat{S}$ heisst NP_R-*hart*, falls: $\forall S \in \mathrm{NP}_R.\ S \hookrightarrow_p \widehat{S}$

S7 $\widehat{S}$ NP_R-hart, $\widehat{S} \hookrightarrow_p S \Rightarrow S$ NP_R-hart

Vollständigkeit

D4 $\widehat{S}$ heisst NP_R-*vollständig*, falls: $\widehat{S}$ NP_R-hart, $\widehat{S} \in \mathrm{NP}_R$

S6 Sei $\widehat{S}$ NP_R-vollständig. $\widehat{S} \in \mathrm{P}_R \Leftrightarrow \mathrm{P}_R = \mathrm{NP}_R$

Vollständigkeit

D4 $\widehat{S}$ heisst NP_R-*vollständig*, falls: $\widehat{S}$ NP_R-hart, $\widehat{S} \in \mathrm{NP}_R$

S6 Sei $\widehat{S}$ NP_R-vollständig. $\widehat{S} \in \mathrm{P}_R \Leftrightarrow \mathrm{P}_R = \mathrm{NP}_R$

[SA/QA-FEAS ist NP_R-vollständig]

Begriffsdefinition SA/QA-FEAS

- “Erfüllbarkeit von semi/quasi-algebraischen Systemen”

- (X, X_{yes}) mit

$$
\begin{aligned}
X &= \{\Phi = (\varphi_1, \ldots \varphi_m) \mid \quad \varphi_j = (f_{j1}, \ldots f_{jl}, g_{j1}, \ldots, g_{jr}), \\
&\qquad\qquad f_{ji}, g_{jk} \in R[x_1, \ldots, x_n]\}, \\
\varphi'_j(x) &= \bigvee_{n=1}^{l} f_{jn}(x) > 0 \vee \bigvee_{n=1}^{r} g_{jn}(x) = 0, \\
\varphi' &= \bigwedge_{j=1}^{m} \varphi'_j, \\
X_{yes} &= \{\Phi \in X | S_{\varphi'} \neq \emptyset\}
\end{aligned}
$$

Begriffsdefinition SA/QA-FEAS

- "Erfüllbarkeit von semi/quasi-algebraischen Systemen"

- (X, X_{yes}) mit

$$
\begin{aligned}
X &= \{\Phi = (\varphi_1, \ldots \varphi_m) \mid \quad \varphi_j = (f_{j1}, \ldots f_{jl}, g_{j1}, \ldots, g_{jr}), \\
&\qquad\qquad\qquad\qquad f_{ji}, g_{jk} \in R[x_1, \ldots, x_n]\}, \\
\varphi'_j(x) &= \bigvee_{n=1}^{l} f_{jn}(x) > 0 \vee \bigvee_{n=1}^{r} g_{jn}(x) = 0, \\
\varphi' &= \bigwedge_{j=1}^{m} \varphi'_j, \\
X_{yes} &= \{\Phi \in X | S_{\varphi'} \neq \emptyset\}
\end{aligned}
$$

Beweisvorbereitung Zugehörigkeit

UPSE Sei $W = \{(f,z) | f \in R[x_1,\ldots,x_n]^m, z \in R^n, m,n \in \mathbb{N}\}$

Für $(f,z) \in W$ berechnet UPSE $f(z)$

Beweis: SA/QA-FEAS $\in NP_R$ bzgl. unit-cost

Maschine M:
input Φ
2: guess $z \in R^n$
use UPSE to compute $y := \Phi(z)$
4: if check(y) output 1
else output 0

mit check: prüfe $>/= 0$, $\wedge/\vee$ wie gefordert

✓ Integrität: $\forall\Phi.\ (\exists z.\ \Phi_M(\Phi, z) = 1 \Leftrightarrow \varphi'$ erfüllbar)
✓ polynomielle Laufzeit in size(Φ)

Beweis: SA/QA-FEAS $\in NP_R$ bzgl. unit-cost

Maschine M:
input Φ
2: guess $z \in R^n$
use UPSE to compute $y := \Phi(z)$
4: if check(y) output 1
else output 0

mit check: prüfe $>/= 0$, $\wedge/\vee$ wie gefordert

✓ Integrität: $\forall\Phi.\ (\exists z.\ \Phi_M(\Phi, z) = 1 \Leftrightarrow \varphi'$ erfüllbar)

✓ polynomielle Laufzeit in size(Φ)

Beweis: SA/QA-FEAS $\in NP_R$ bzgl. unit-cost

Maschine M:
input Φ
2: guess $z \in R^n$
use UPSE to compute $y := \Phi(z)$
4: if check(y) output 1
else output 0

mit check: prüfe $>/= 0$, $\wedge/\vee$ wie gefordert

✓ Integrität: $\forall\Phi.\ (\exists z.\ \Phi_M(\Phi, z) = 1 \Leftrightarrow \varphi'$ erfüllbar)
✓ polynomielle Laufzeit in size(Φ)

Beweisvorb. Härte 1/6 : Reduktion endl. Masch.

- Berechnungsendomorphismus: $H : \mathcal{N} \times S \to \mathcal{N} \times S$,
  Berechnungen: $z^0 = (1, \mathcal{I}(x)), \ldots, z^k = (\eta^k, x^k) = H^k(z^0), \ldots$

- $\gamma(k)$ nutzt maximal $K_M + k$ Koordination von $S = R_\infty$
  $\gamma \in \Gamma_T$: "basic active state space" $S_m = R^{2m}, m = K_m + T$

Beweisvorb. Härte 1/6 : Reduktion endl. Masch.

- Berechnungsendomorphismus: $H : \mathcal{N} \times S \to \mathcal{N} \times S$,
  Berechnungen: $z^0 = (1, \mathcal{I}(x)), \ldots, z^k = (\eta^k, x^k) = H^k(z^0), \ldots$

- $\gamma(k)$ nutzt maximal $K_M + k$ Koordination von $S = R_\infty$
  $\gamma \in \Gamma_T$: “basic active state space” $S_m = R^{2m}, m = K_m + T$

Beweisvorb. Härte 2/6 : Neue Abbildungen

- $\widetilde{\pi} : S = R_\infty \to S_m = R^{2m},\ x \mapsto (x_{-(m-1)}, \ldots x_0, x_1, \ldots x_m)$
  $\widetilde{\iota} : S_m \to S,\ x \mapsto (\ldots, 0, x_{-(m-1)}, \ldots x_0 . x_1, \ldots x_m, 0, \ldots)$
- $\widetilde{\mathcal{I}} = \widetilde{\pi} \circ \mathcal{I},\ \widetilde{\mathcal{O}} = \mathcal{O} \circ \widetilde{\iota}$
- $\widetilde{g}_\eta = \widetilde{\pi} \circ g_\eta \circ \widetilde{\iota} : S_m \to S_m,$

1. $\eta = 1, N,$ oder branch : $\widetilde{g}_\eta = \mathrm{id}$
2. η computation:
   $\widetilde{g}_\eta(x) = (x_{-(m-1)}, \ldots, x_0, g'_1(x'), \ldots, g'_{K_M}(x'), x_{K_M+1}, \ldots, x_m),$
   $x' = (x_1, \ldots, x_{K_M})$
3. η shift, $g_\eta = \sigma_l$ (σ_r analog) :
   $\widetilde{g}_\eta(x_{-(m-1)}, \ldots x_0, x_1, \ldots x_m) = (x_{-(m-2)}, \ldots x_0, x_1, \ldots x_m, 0)$

Beweisvorb. Härte 2/6 : Neue Abbildungen

- $\widetilde{\pi} : S = R_\infty \to S_m = R^{2m},\ x \mapsto (x_{-(m-1)}, \ldots x_0, x_1, \ldots x_m)$
  $\widetilde{\iota} : S_m \to S,\ x \mapsto (\ldots, 0, x_{-(m-1)}, \ldots x_0 . x_1, \ldots x_m, 0, \ldots)$
- $\widetilde{\mathcal{I}} = \widetilde{\pi} \circ \mathcal{I},\ \widetilde{\mathcal{O}} = \mathcal{O} \circ \widetilde{\iota}$

- $\widetilde{g}_\eta = \widetilde{\pi} \circ g_\eta \circ \widetilde{\iota} : S_m \to S_m$,

1. $\eta = 1, N$, oder branch : $\widetilde{g}_\eta = \mathrm{id}$
2. η computation:
   $\widetilde{g}_\eta(x) = (x_{-(m-1)}, \ldots, x_0, g'_1(x'), \ldots, g'_{K_M}(x'), x_{K_M+1}, \ldots, x_m)$,
   $x' = (x_1, \ldots, x_{K_M})$
3. η shift, $g_\eta = \sigma_l$ (σ_r analog) :
   $\widetilde{g}_\eta(x_{-(m-1)}, \ldots x_0, x_1, \ldots x_m) = (x_{-(m-2)}, \ldots x_0, x_1, \ldots x_m, 0)$

Beweisvorb. Härte 2/6 : Neue Abbildungen

- $\widetilde{\pi} : S = R_\infty \to S_m = R^{2m},\ x \mapsto (x_{-(m-1)}, \dots x_0, x_1, \dots x_m)$
  $\widetilde{\iota} : S_m \to S,\ x \mapsto (\dots, 0, x_{-(m-1)}, \dots x_0.x_1, \dots x_m, 0, \dots)$
- $\widetilde{\mathcal{I}} = \widetilde{\pi} \circ \mathcal{I},\ \widetilde{\mathcal{O}} = \mathcal{O} \circ \widetilde{\iota}$

- $\widetilde{g}_\eta = \widetilde{\pi} \circ g_\eta \circ \widetilde{\iota} : S_m \to S_m,$

1 $\eta = 1, N,$ oder branch : $\widetilde{g}_\eta = \mathrm{id}$

2 η computation:
$\widetilde{g}_\eta(x) = (x_{-(m-1)}, \dots, x_0, g'_1(x'), \dots, g'_{K_M}(x'), x_{K_M+1}, \dots, x_m),$
$x' = (x_1, \dots, x_{K_M})$

3 η shift, $g_\eta = \sigma_l$ (σ_r analog) :
$\widetilde{g}_\eta(x_{-(m-1)}, \dots x_0, x_1, \dots x_m) = (x_{-(m-2)}, \dots x_0, x_1, \dots x_m, 0)$

Beweisvorb. Härte 3/6 : Registergleichungen I/II

1st $g : \mathcal{N} \times S \to S,\ (\eta, x) \mapsto g_\eta(x),$

$$\beta : \mathcal{N} \times S \to \mathcal{N},\ (\eta, x) \mapsto \begin{cases} \beta_\eta & ,\eta \in C \\ \beta_\eta^- & ,\eta \in \mathcal{B}, x_1 < 0 \\ \beta_\eta^+ & ,\eta \in \mathcal{B}, x_1 \geq 0 \end{cases},$$

$$H(\eta, x) = (\beta(\eta, x), g(\eta, x))$$

2nd $\beta : \mathcal{N} \times S \to \mathcal{N},\ g : \mathcal{N} \times S \to S$

$x \in \Omega_T \Leftrightarrow ((\eta^0, x^0), \ldots, (\eta^T, x^T)) \in (\mathcal{N} \times S)^{T+1}$

$\eta^k = \beta(\eta^{k-1}, x^{k-1}),\ x^k = g(\eta^{k-1}, x^{k-1})\ (k = 1, \ldots T)$

$(\eta^0, x^0) = (1, \mathcal{I}(x)),\ \eta^T = N$

Beweisvorb. Härte 3/6 : Registergleichungen I/II

1st $g : \mathcal{N} \times S \to S,\ (\eta, x) \mapsto g_\eta(x),$

$$\beta : \mathcal{N} \times S \to \mathcal{N},\ (\eta, x) \mapsto \begin{cases} \beta_\eta & ,\eta \in C \\ \beta_\eta^- & ,\eta \in \mathcal{B}, x_1 < 0 \\ \beta_\eta^+ & ,\eta \in \mathcal{B}, x_1 \geq 0 \end{cases},$$

$$H(\eta, x) = (\beta(\eta, x), g(\eta, x))$$

2nd $\beta : \mathcal{N} \times S \to \mathcal{N},\ g : \mathcal{N} \times S \to S$

$$x \in \Omega_T \Leftrightarrow ((\eta^0, x^0), \ldots, (\eta^T, x^T)) \in (\mathcal{N} \times S)^{T+1}$$

$$\eta^k = \beta(\eta^{k-1}, x^{k-1}),\ x^k = g(\eta^{k-1}, x^{k-1})\ (k = 1, \ldots T)$$

$$(\eta^0, x^0) = (1, \mathcal{I}(x)),\ \eta^T = N$$

Beweisvorb. Härte 4/6 : Registergleichungen II/II

Betrachte $S = R_\infty$ als $S_m = R^{2m}$

Berechnbarkeit über R durch $\mathcal{N} \hookrightarrow R^N, j \mapsto e_j$:

$\widehat{\beta} : R^N \times R^{2m} \to R^N$, $\widehat{g} : R^N \times R^{2m} \to R^{2m}$,

$\widehat{\beta}(\alpha, x) = \sum_{j=1}^{N} \alpha_j e_{\widetilde{\beta}(j,x)}$, $\widehat{g}(\alpha, x) = \sum_{j=1}^{N} \alpha_j \widetilde{g}(j, x)$,

$\widehat{H} = (\widehat{\beta}, \widehat{g}) : R^N \times R^{2m} \to R^N \times R^{2m}$

3^{rd} $\alpha^k - \widehat{\beta}(\alpha^{k-1}, x^{k-1}) = 0$, $x^k - \widehat{g}(\alpha^{k-1}, x^{k-1}) = 0$ $(k = 1, \ldots T)$

$(\alpha^0, x^0) - (e_1, \widetilde{\mathcal{I}}(x)) = 0$, $\alpha^T - e_N = 0$

Optional: $x_0^T = x_1^T = 1, x_{-1}^T = 0$

$\mathcal{R}$ Für $x = (x_1, \ldots x_n), z = (\alpha^0, x^0, \ldots \alpha^T, x^T)$ heissen $1^{st}/2^{nd}/3^{rd}$ "Zeit-T Registergleichungen" $\mathcal{R}_T(x, z)$

Beweisvorb. Härte 4/6 : Registergleichungen II/II

Betrachte $S = R_\infty$ als $S_m = R^{2m}$

Berechnbarkeit über R durch $\mathcal{N} \hookrightarrow R^N, j \mapsto e_j$:

$\widehat{\beta} : R^N \times R^{2m} \to R^N$, $\widehat{g} : R^N \times R^{2m} \to R^{2m}$,

$\widehat{\beta}(\alpha, x) = \sum_{j=1}^{N} \alpha_j e_{\widetilde{\beta}(j,x)}$, $\widehat{g}(\alpha, x) = \sum_{j=1}^{N} \alpha_j \widetilde{g}(j, x)$,

$\widehat{H} = (\widehat{\beta}, \widehat{g}) : R^N \times R^{2m} \to R^N \times R^{2m}$

3^{rd} $\alpha^k - \widehat{\beta}(\alpha^{k-1}, x^{k-1}) = 0$, $x^k - \widehat{g}(\alpha^{k-1}, x^{k-1}) = 0$ $(k = 1, \ldots T)$

$(\alpha^0, x^0) - (e_1, \widetilde{\mathcal{I}}(x)) = 0$, $\alpha^T - e_N = 0$

Optional: $x_0^T = x_1^T = 1, x_{-1}^T = 0$

$\mathcal{R}$ Für $x = (x_1, \ldots x_n), z = (\alpha^0, x^0, \ldots \alpha^T, x^T)$ heissen $1^{st}/2^{nd}/3^{rd}$ "Zeit-T Registergleichungen" $\mathcal{R}_T(x, z)$

Beweisvorb. Härte 4/6 : Registergleichungen II/II

Betrachte $S = R_\infty$ als $S_m = R^{2m}$

Berechnbarkeit über R durch $\mathcal{N} \hookrightarrow R^N, j \mapsto e_j$:

$\widehat{\beta} : R^N \times R^{2m} \to R^N$, $\widehat{g} : R^N \times R^{2m} \to R^{2m}$,

$\widehat{\beta}(\alpha, x) = \sum_{j=1}^{N} \alpha_j e_{\widetilde{\beta}(j,x)}$, $\widehat{g}(\alpha, x) = \sum_{j=1}^{N} \alpha_j \widetilde{g}(j, x)$,

$\widehat{H} = (\widehat{\beta}, \widehat{g}) : R^N \times R^{2m} \to R^N \times R^{2m}$

3^{rd} $\alpha^k - \widehat{\beta}(\alpha^{k-1}, x^{k-1}) = 0$, $x^k - \widehat{g}(\alpha^{k-1}, x^{k-1}) = 0$ $(k = 1, \ldots T)$

$(\alpha^0, x^0) - (e_1, \widetilde{\mathcal{I}}(x)) = 0$, $\alpha^T - e_N = 0$

Optional: $x_0^T = x_1^T = 1, x_{-1}^T = 0$

$\mathcal{R}$ Für $x = (x_1, \ldots x_n), z = (\alpha^0, x^0, \ldots \alpha^T, x^T)$ heissen $1^{st}/2^{nd}/3^{rd}$ "Zeit-T Registergleichungen" $\mathcal{R}_T(x, z)$

Beweisvorb. Härte 4/6 : Registergleichungen II/II

Betrachte $S = R_\infty$ als $S_m = R^{2m}$

Berechnbarkeit über R durch $\mathcal{N} \hookrightarrow R^N, j \mapsto e_j$:

$\widehat{\beta} : R^N \times R^{2m} \to R^N$, $\widehat{g} : R^N \times R^{2m} \to R^{2m}$,

$\widehat{\beta}(\alpha, x) = \sum_{j=1}^{N} \alpha_j e_{\widetilde{\beta}(j,x)}$, $\widehat{g}(\alpha, x) = \sum_{j=1}^{N} \alpha_j \widetilde{g}(j, x)$,

$\widehat{H} = (\widehat{\beta}, \widehat{g}) : R^N \times R^{2m} \to R^N \times R^{2m}$

3^{rd} $\alpha^k - \widehat{\beta}(\alpha^{k-1}, x^{k-1}) = 0$, $x^k - \widehat{g}(\alpha^{k-1}, x^{k-1}) = 0$ $(k = 1, \ldots T)$

$(\alpha^0, x^0) - (e_1, \widetilde{\mathcal{I}}(x)) = 0$, $\alpha^T - e_N = 0$

Optional: $x_0^T = x_1^T = 1, x_{-1}^T = 0$

$\mathcal{R}$ Für $x = (x_1, \ldots x_n), z = (\alpha^0, x^0, \ldots \alpha^T, x^T)$ heissen $1^{st}/2^{nd}/3^{rd}$ “Zeit-T Registergleichungen” $\mathcal{R}_T(x, z)$

Beweisvorb. Härte 5/6 : Folgerungen I/II

$x \in \Omega_T \Leftrightarrow \mathcal{R}_T(x,z)$ lösbar über R

S01 $\mathcal{R}_T(x,z)$ ist äquivalent zu semi/quasi-algebraischem System $\Phi_T(x,z)$, mit

.1 # R-Variablen $\leq n + cT^2$
.2 # polynomieller Gleichungen $\leq cT^2$, jedes hat Grad $\leq c$
.3 # linearer Ungleichungen $\leq 2T$

wobei c nur von N, D_M, K_M abhängt

...

Beweisvorb. Härte 5/6 : Folgerungen I/II

$x \in \Omega_T \Leftrightarrow \mathcal{R}_T(x,z)$ lösbar über R

S01 $\mathcal{R}_T(x,z)$ ist äquivalent zu semi/quasi-algebraischem System $\Phi_T(x,z)$, mit

.1 # R-Variablen $\leq n + cT^2$
.2 # polynomieller Gleichungen $\leq cT^2$, jedes hat Grad $\leq c$
.3 # linearer Ungleichungen $\leq 2T$

wobei c nur von N, D_M, K_M abhängt

...

Beweisvorb. Härte 6/6 : Folgerungen II/II

$\mathcal{R}(x,z)$ heisst n-äquivalent zu $\Phi(x,w)$, falls
$\pi_n(S_\mathcal{R}) = \pi_n(S_\Phi)$, mit
$S_\mathcal{R} = \{(x,z) \in R^{n+t} | \mathcal{R}(x,z)$ erfüllt über R $\}$
$S_\Phi = \{(x,w) \in R^{n+s} | \Phi(x,w)$ erfüllt über R $\}$

S02 Auf $(F,=)$ sowie $(\mathbb{Z},<),(\mathbb{Q},<),(\mathbb{R},<)$ gilt:

a) $\mathcal{R}_T(x,z)$ ist n-äquivalent zu algebraischem System $\Phi_T(x,w)$, mit Schranken wie in S01.

...

Beweis: SA/QA-FEAS ist NP_R-hart 1/5

"$\forall S \in \mathrm{NP}_R.\ S \hookrightarrow_p$ SA/QA-FEAS"

Sei (Y, Y_{yes}) SA/QA-FEAS, $(X, X_{yes}) \in \mathrm{NP}_R$.

Benötigt: p-Morphismus $\varphi : X \to Y$ mit
$\forall x \in X.\ x \in X_{yes} \Leftrightarrow \varphi(x) \in Y_{yes}$.

Anwendung der Registergleichungen auf NP_R-Maschine M für (X, X_{yes}), mit $c, q > 0, \mathrm{cost}_M(x,w) \leq c \cdot \mathrm{size}(x)^q$

$\Rightarrow$ Für $(x,w), T > 0$ berechne z; $\mathcal{R}_T^{(1)}((x,w),z)$ sind die Zeit-T Registergleichungen, sodass Ausgabewert = 1 gilt

Beweis: SA/QA-FEAS ist NP_R-hart 1/5

"$\forall S \in \mathrm{NP}_R.\ S \hookrightarrow_p$ SA/QA-FEAS"

Sei (Y, Y_{yes}) SA/QA-FEAS, $(X, X_{yes}) \in \mathrm{NP}_R$.

Benötigt: p-Morphismus $\varphi : X \to Y$ mit
$\forall x \in X.\ x \in X_{yes} \Leftrightarrow \varphi(x) \in Y_{yes}$.

Anwendung der Registergleichungen auf NP_R-Maschine M für (X, X_{yes}), mit $c, q > 0, \mathrm{cost}_M(x, w) \leq c \cdot \mathrm{size}(x)^q$

⇒ Für $(x, w), T > 0$ berechne z; $\mathcal{R}_T^{(1)}((x, w), z)$ sind die Zeit-T Registergleichungen, sodass Ausgabewert = 1 gilt

Beweis: SA/QA-FEAS ist NP_R-hart 1/5

"$\forall S \in \mathrm{NP}_R.\ S \hookrightarrow_p$ SA/QA-FEAS"

Sei (Y, Y_{yes}) SA/QA-FEAS, $(X, X_{yes}) \in \mathrm{NP}_R$.

Benötigt: p-Morphismus $\varphi : X \to Y$ mit
$\forall x \in X.\ x \in X_{yes} \Leftrightarrow \varphi(x) \in Y_{yes}$.

Anwendung der Registergleichungen auf NP_R-Maschine M für (X, X_{yes}), mit $c, q > 0, \mathrm{cost}_M(x, w) \leq c \cdot \mathrm{size}(x)^q$

⇒ Für $(x, w), T > 0$ berechne z; $\mathcal{R}_T^{(1)}((x, w), z)$ sind die Zeit-T Registergleichungen, sodass Ausgabewert = 1 gilt

Beweis: SA/QA-FEAS ist NP_R-hart 2/5

"$\forall S \in \mathrm{NP}_R.\ S \hookrightarrow_p$ SA/QA-FEAS"

$\mathcal{R}_T^{(1)}(x,w,z)$ ist äquivalent zu semi/quasi-algebraischen System $\Phi_T^{(1)}(x,w,z)$, d.h.

$(x,w) \in \Omega_T(1) \Leftrightarrow \Phi_T^{(1)}((x,w),z')$ ist erfüllbar.

Beweis: SA/QA-FEAS ist NP_R-hart 3/5

"$\forall S \in \mathrm{NP}_R.\ S \hookrightarrow_p$ SA/QA-FEAS"

Konstruiere p-Reduktion:

Für $x \in X$ sei $\varphi(x) = \Phi_T^{(1)}(x,(w,z))$, mit $T = c \cdot \mathrm{size}(x)^q$,
und $w = (w_1,\ldots,w_m)$, $m = c \cdot \mathrm{size}(x)^q + K_M$

Für $n = \mathrm{length}(x) + m$ ist
$\mathrm{length}(z)$, # poly. (Un-)Gleich. in $\Phi_T^{(1)}(x,w,z) \leq \mathit{Poly}.(n,T)$,
n,T selber polynomiell in $\mathrm{size}(x)$

Beweis: SA/QA-FEAS ist NP_R-hart 3/5

"$\forall S \in \mathrm{NP}_R.\ S \hookrightarrow_p$ SA/QA-FEAS"

Konstruiere p-Reduktion:

Für $x \in X$ sei $\varphi(x) = \Phi_T^{(1)}(x,(w,z))$, mit $T = c \cdot \mathrm{size}(x)^q$,
und $w = (w_1,\ldots,w_m)$, $m = c \cdot \mathrm{size}(x)^q + K_M$

Für $n = \mathrm{length}(x) + m$ ist

$\mathrm{length}(z)$, # poly. (Un-)Gleich. in $\Phi_T^{(1)}(x,w,z) \leq \mathit{Poly}.(n,T)$,

n, T selber polynomiell in $\mathrm{size}(x)$

Beweis: SA/QA-FEAS ist NP_R-hart 4/5

"$\forall S \in \mathrm{NP}_R.\ S \hookrightarrow_p$ SA/QA-FEAS"

$\Rightarrow$ size$(\Phi_T^{(1)}(x,w,z))$ ist durch Polynom in size(x) beschränkt,

✓ φ ist also p-Morphismus

Beweis: SA/QA-FEAS ist NP_R-hart 5/5

"$\forall S \in \mathrm{NP}_R.\ S \hookrightarrow_p$ SA/QA-FEAS"

φ ist Reduktion:

$$x \in X_{yes} \quad \overset{\text{D1, } T = c \cdot size(x)^q}{\Leftrightarrow}$$

$$\exists w \in R^{\infty},\ \text{length}(w) = m.\ \Phi_M(x,w) = 1,\ \text{cost}_M(x,w) \leq T \ \Leftrightarrow$$

$$(x,w) \in \Omega_T(1) \ \Leftrightarrow$$

✓ $\Phi_T^{(1)}(x,(w,z))$ erfüllbar.

[Weitere Probleme und Resultate in $\mathrm{NP}_{\{0,1\}/\mathbb{Z}/\mathbb{R}}$]

Problemdefinitionen

HN Gegeben Menge von Polynomen, Koeffizienten aus $\mathbb{C}$, entscheide ob diese gleiche Nullstelle haben

4-FEAS Polynome limitiert auf Grad 4, Koeffizienten in $\mathbb{R}$

QUAD Verallgemeinert auf Ring R, Lösung quadratischer Gleichungen

SAT Erfüllbarkeit aussagenlogischer Formel

Resultate

- QA/SA-FEAS sind NP-hart auf $(R, =\ /\ <)$ (vollst. bzgl *unit*)

- HN ist NP-hart auf $(F, =)$,
- QUAD auch,
- mit 4-FEAS auch auf $(\mathbb{Z}/\mathbb{Q}/\mathbb{R}, <)$ (vollst. bzgl *unit*)

- HN $\notin \mathrm{DEC}_{(\mathbb{Z},<)}$ (Matiyasevich's)
- Turingmasch. Halteproblem $\notin NP$, aber NP-hart
- Faktorisierung ist $\in NP$, nicht(?) NP-hart

- $P_R = NP_R$ reduziert auf Teilprobleme: z.B. $HN \in P_R$

Ausblick: Cook's Theorem

SAT ist NP-vollständig

Ausblick

nächste Woche: 4-FEAS/ SAT(?) sind NP-vollständig

Abbildung: Quelle: Complexity and Real Computation

Ausblick

nächste Woche: 4-FEAS/ SAT(?) sind NP-vollständig

Status of P = NP?

RING	BRANCH	COST	HN ∈ DEC	HN ∈ NP	NP ⊆ EXP	P = NP
$\mathbb{Z}$	$<$	unit	No	Yes	No	No
$\mathbb{Z}$	$<$	bit	No	No	Yes	?
$\mathbb{Z}$	$=$	unit	No	Yes	No	No
$\mathbb{Z}$	$=$	bit	No	No	Yes	No
$\mathbb{Q}$	$<$	unit	?	Yes	No	No
$\mathbb{R}$	$<$	unit	Yes	Yes	Yes	?
$\mathbb{C}$	$=$	unit	Yes	Yes	Yes	?
$\mathbb{Z}_2$	$=$	unit	Yes	Yes	Yes	?

Abbildung: Quelle: Complexity and Real Computation

any questions?

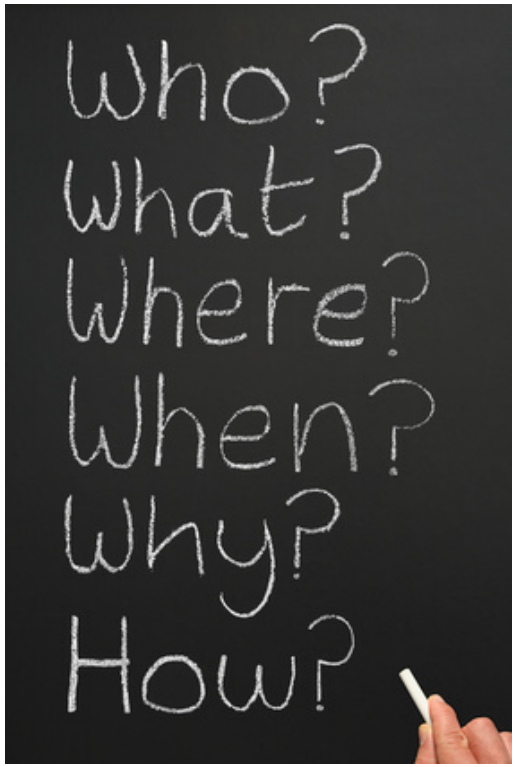

Abbildung: no caption

http://adjunctassistance.com/wp-content/uploads/2010/05/WhoWhatWhere.png

Quellen

- Complexity and Real Computation, 97
  Blum, Cucker, Shub, Smale

- On the Complexity of Quantifier Elimination:
  the Structural Approach, 93, Cucker