NP-vollständige Probleme über $\mathbb{R}, \mathbb{C}$ und $\mathbb{Z}_2$
Zur Entscheidbarkeit von NP

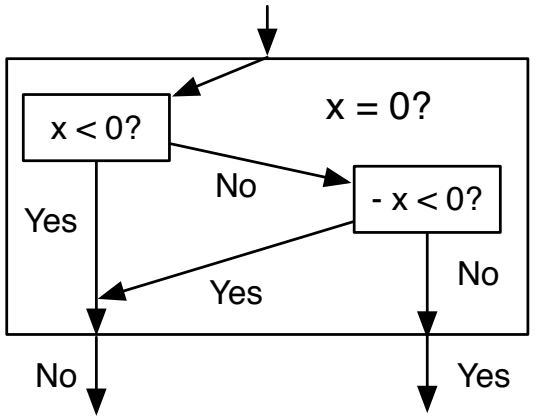
Markus Schwagenscheidt

11.07.2011

- Wir betrachten BSS-Maschinen und Probleme über den Körpern

$$(\mathbb{R}, <), \quad (\mathbb{C}, =), \quad (\mathbb{Z}_2, =),$$

  wobei $\mathbb{Z}_2 = \{0, 1\}$. Wenn an einer Stelle alle Körper stehen können, so schreiben wir R.
- Über $\mathbb{R}$ kann auch auf $=, \leq, \geq, >$ geprüft werden, z.B. für $=$ mittels:



- Unser Ziel ist es, jeweils ein NP_R-vollständiges Problem anzugeben, das (sogar in exponentieller Zeit) entscheidbar ist.
- Daraus folgt,
  - dass alle Probleme in $\mathrm{NP}_\mathbb{R}, \mathrm{NP}_\mathbb{C}$ und $\mathrm{NP}_{\mathbb{Z}_2}$ entscheidbar sind und
  - dass $\mathrm{NP}_\mathrm{R} \subseteq \mathrm{EXP}_\mathrm{R}$ gilt.

Wir schreiben $T_M(x)$ für die Anzahl der Knoten, die während der Rechnung von M bei Eingabe $x \in \mathrm{R}^\infty$ bis zum Erreichen des Ausgabeknoten besucht werden.

$$T_M(x) \quad \hat{=} \quad \text{Laufzeit von } M \text{ bei Eingabe } x.$$

Definition

- Eine Sprache $L \subseteq \mathrm{R}^\infty$ liegt in P_R, falls es ein Polynom p und eine Maschine M gibt, die L entscheidet und für die $T_M(x) \leq p(|x|)$ für alle x gilt.
- Eine Sprache $L \subseteq \mathrm{R}^\infty$ liegt in EXP_R, falls es Polynom p und eine Maschine M gibt, die L entscheidet und für die $T_M(x) \leq 2^{p(|x|)}$ für alle x gilt.
- Eine Sprache $L \subseteq \mathrm{R}^\infty$ liegt in NP_R, falls es Polynome p, q und eine Maschine M gibt mit

  $$x \in L \quad \Leftrightarrow \quad \exists w \in R^{\leq q(|x|)} : \; M(x, w) = 1$$

  und $T_M(x, w) \leq p(|x|)$, d.h. M hat polynomielle Laufzeit bzgl. des ersten Arguments.

Es gilt $\mathrm{P}_\mathrm{R} \subseteq \mathrm{NP}_\mathrm{R}$ und $\mathrm{P}_\mathrm{R} \subseteq \mathrm{EXP}_\mathrm{R}$. Die Klassen P_R und EXP_R enthalten per Definition nur entscheidbare Probleme, für NP_R ist das nicht offensichtlich.

Definition

- Wir schreiben $L' \leq_p L$, falls es eine in polynomieller Zeit berechenbare Funktion $\varphi : \mathrm{R}^\infty \to \mathrm{R}^\infty$ gibt mit

$$x \in L' \;\Leftrightarrow\; \varphi(x) \in L.$$

  φ heißt polynomielle Reduktion von L' auf L.
- Ein Problem $L \subseteq \mathrm{R}^\infty$ ist $\mathrm{NP_R}$-vollständig, wenn $L \in \mathrm{NP_R}$ ist und $L' \leq_p L$ für alle Sprachen $L' \in \mathrm{NP_R}$.

Bemerkung

- Die $\leq_p$-Relation ist transitiv, das heißt es gilt

$$A \leq_p B \wedge B \leq_p C \quad \Rightarrow \quad A \leq_p C.$$

- Ist L entscheidbar und $L' \leq_p L$, so ist auch L' entscheidbar.

Betrachte die folgenden Probleme:

SA-FEAS:	Gegeben eine semi-algebraische Formel, hat diese ein Lösung über $\mathbb{R}$? $(x > 0 \ \vee \ x^2 + y^2 - 1 = 0) \ \wedge \ (y > 0 \ \vee \ x^2 - 1 = 0)$
QA-FEAS:	Gegeben eine quasi-algebraische Formel, hat diese ein Lösung über R? $(xy \neq 0 \ \vee \ x^2 + y^2 - 1 = 0) \ \wedge \ (x^2 - 1 = 0)$
HN:	Gegeben ein endliches System polynomieller Gleichungen, hat dieses eine Lösung über R? $(x^2y^2 - 1 = 0) \ \wedge \ (xyz = 0) \ \wedge \ (x^2 + 1 = 0)$
QUAD:	Gegeben ein endliches System quadratischer polynomieller Gleichungen, hat dieses eine Lösung über R? $(x^2 - 4 = 0) \ \wedge \ (xy = 0)$
4-FEAS:	Gegeben ein Polynom $f \in \mathrm{R}[X_1, \ldots, X_n]$ vom Grad ≤ 4, hat f eine Nullstelle in R^n? $2xyz^2 + 4x^2y^2 + 3 = 0$
3SAT:	Gegeben eine 3CNF-Formel φ, ist φ erfüllbar? $(x_1 \vee x_2 \vee \neg x_3) \ \wedge \ (\neg x_1 \vee x_3) \ \wedge \ (x_2 \vee x_3 \vee x_4)$

Theorem

Es gilt

- SA-FEAS, QA-FEAS, HN, QUAD, 4-FEAS $\in \mathrm{NP}_{\mathbb{R}}$.
- QA-FEAS, HN, QUAD, 4-FEAS $\in \mathrm{NP}_{\mathbb{C}}$.
- QA-FEAS, HN, QUAD, 4-FEAS, 3SAT $\in \mathrm{NP}_{\mathbb{Z}_2}$.

Beweis.

- **Zeuge** w: Lösung des Systems bzw. Nullstelle des Polynoms bzw. erfüllende Belegung der Formel.
- **Überprüfer** M: Wertet bei Eingabe des Systems $f = (f_1, \ldots, f_k)$ bzw. f bzw. φ und w alle Polynome $f_j(w)$ aus und prüft, ob (Un)-Gleichungen erfüllt sind bzw. prüft, ob Belegung w die Formel erfüllt.

□

Bemerkung

Über $\mathbb{R}$ und $\mathbb{C}$ ist nicht offensichtlich, dass diese Probleme entscheidbar sind. Es ist nicht sofort klar, wie eine Lösung (d.h. ein Zeuge w) gefunden werden kann, da man nicht alle Zeugen systematisch durchprobieren kann.

Theorem

- SA-FEAS, QA-FEAS, HN, QUAD *und* 4-FEAS *sind* $\mathrm{NP}_{\mathbb{R}}$*-vollständig.*
- QA-FEAS, HN *und* QUAD *sind* $\mathrm{NP}_{\mathbb{C}}$*-vollständig.*
- QA-FEAS, HN *und* QUAD *sind* $\mathrm{NP}_{\mathbb{Z}_2}$*-vollständig.*
- 3SAT *ist* $\mathrm{NP}_{\mathbb{Z}_2}$*-vollständig.*

Bemerkungen

- SA-FEAS macht nur über $(\mathbb{R}, <)$ Sinn.
- 4-FEAS $/\mathbb{C}$ ist nicht $\mathrm{NP}_{\mathbb{C}}$-vollständig.
- d-FEAS $/\mathbb{R}$ für $d \leq 3$ liegt in $\mathrm{P}_{\mathbb{R}}$.

- Sei $L \in \mathrm{NP}_{\mathrm{R}}$. Dann gibt es per Definition eine polynomiell zeitbeschränkte Maschine M mit

$$x \in L \quad \Leftrightarrow \quad \exists w \in R^{\leq \mathrm{poly}(|x|)} \; M(x, w) = 1.$$

- Man kann mithilfe der sogenannten Register Gleichungen zeigen, dass es eine *kurze* semi-algebraische (für $\mathbb{R}$) bzw. quasi-algebraische (für $\mathbb{C}, \mathbb{Z}_2$) Formel Φ gibt mit

$$x \in L \quad \Leftrightarrow \quad \exists w \; M(x, w) = 1 \quad \Leftrightarrow \quad \exists w \exists u \; \Phi(x, w, u).$$

  Die Länge von Φ ist durch ein Polynom in $n = |x|$ beschränkt.
- Die Maschine, die Φ konstruiert und ausgibt, ist eine polynomielle Reduktion von L auf SA-FEAS bzw. QA-FEAS.
- Daraus folgt die Vollständigkeit von SA-FEAS bzw. QA-FEAS.
- Wir wollen Φ umformen in
  - ein kurzes System polynomieller Gleichungen.
  - ein kurzes System quadratischer Gleichungen.
  - ein Polynom vom Grad ≤ 4.

Gegeben sei eine semi-algebraische Formel $\bigwedge_{j=1}^{m} \varphi_j$ mit φ_j von der Form

$$f_1(\mathbf{x}) > 0 \ \vee \cdots \vee \ f_k(\mathbf{x}) > 0 \ \vee \ g_1(\mathbf{x}) = 0 \ \vee \cdots \vee \ g_\ell(\mathbf{x}) = 0$$

in n Variablen $\mathbf{x} = x_1, \ldots, x_n$ über den reellen Zahlen $\mathbb{R}$.

- Ersetze jede Ungleichung

$$f(\mathbf{x}) > 0 \quad \text{durch} \quad f(\mathbf{x})y^2 - 1 = 0$$

  mit einer neuen reellen Variable y (für jedes f eine neue Variable).
- Man erhält eine äquivalente quasi-algebraische Formel ψ, d.h. es gilt

$$\exists \mathbf{x} \ \varphi(\mathbf{x}) \quad \Leftrightarrow \quad \exists \mathbf{w} \ \psi(\mathbf{w})$$

Beispiel

Die semi-algebraische Formel

$$\varphi(x) \ \equiv \ (x^2 - 2 > 0 \ \vee \ x - 1 = 0) \ \wedge \ (x > 0)$$

in einer Variable ist äquivalent zur quasi-algebraischen Formel

$$\psi(x, y, z) \ \equiv \ (x^2y^2 - 2y^2 - 1 = 0 \ \vee \ x - 1 = 0) \ \wedge \ (xz^2 - 1 = 0)$$

in drei Variablen.

Von quasi-algebraischen Formeln zu polynomiellen Gleichungen

Gegeben sei eine quasi-algebraische Formel $\bigwedge_{j=1}^{m} \varphi_j$ mit φ_j von der Form

$$f_1(\mathbf{x}) \neq 0 \ \vee \cdots \vee \ f_k(\mathbf{x}) \neq 0 \ \vee \ g_1(\mathbf{x}) = 0 \ \vee \cdots \vee g_\ell(\mathbf{x}) = 0$$

in n Variablen $\mathbf{x} = x_1, \ldots, x_n$ über R.

- Ersetze $f(\mathbf{x}) \neq 0$ durch $f(\mathbf{x})y - 1 = 0$ mit einer neuen Variable y.
- Ersetze φ_j durch die polynomielle Gleichung

$$p_j(\mathbf{x}) := f_1(\mathbf{x}) \cdots f_k(\mathbf{x}) = 0$$

- Man erhält das äquivalente System polynomieller Gleichungen

$$p_1(\mathbf{x}) = 0 \ \wedge \cdots \wedge \ p_m(\mathbf{x}) = 0$$

  in n Variablen $\mathbf{x} = x_1, \ldots, x_n$ über R.

Beispiel

Die quasi-algebraische Formel

$$(x^2 \neq 0 \ \vee \ xy = 0) \ \wedge \ (y = 0 \ \vee \ z - 1 = 0)$$

ist äquivalent zum polynomiellen System

$$x^3yz - xy = 0 \ \wedge \ yz - y = 0.$$

Gegeben sei ein System polynomieller Gleichungen

$$f_1(\mathbf{x}) = 0 \ \wedge \cdots \wedge \ f_m(\mathbf{x}) = 0$$

in n Variablen $\mathbf{x} = x_1, \ldots, x_n$ über R.

- Betrachte ein Monom $x_{i_1} \cdots x_{i_k}$ in einem der f_j mit mehr als zwei Variablen.
- Führe neue Variablen $y_{i_1}, \ldots, y_{i_{k-2}}$ ein.
- Ersetze das Monom durch $x_{i_1} y_{i_1}$ und füge dem System folgende Gleichungen hinzu:

$$\begin{aligned} y_{i_1} - x_{i_2} y_{i_2} &= 0, \\ y_{i_2} - x_{i_3} y_{i_3} &= 0, \\ &\ldots \\ y_{i_{k-2}} - x_{i_{k-1}} x_{i_k} &= 0. \end{aligned}$$

Beispiel

Das polynomielle System

$$x^3 - x = 0 \ \wedge \ xy^2 - 1 = 0$$

ist äquivalent zum quadratischen System

$$xz - x = 0 \ \wedge \ z - x^2 = 0 \ \wedge \ xw - 1 = 0 \ \wedge \ w - y^2 = 0.$$

Von quadratischen Gleichungen zu einem Polynom vom Grad ≤ 4 über $\mathbb{R}$

Gegeben sei ein System quadratischer Gleichungen

$$q_1(\mathbf{x}) = 0 \ \wedge \cdots \wedge \ q_m(\mathbf{x}) = 0$$

in n Variablen $\mathbf{x} = x_1, \ldots, x_n$ über $\mathbb{R}$.

Das System ist äquivalent zu der Gleichung

$$f(\mathbf{x}) := q_1^2(\mathbf{x}) + \cdots + q_m^2(\mathbf{x}) = 0.$$

vom Grad ≤ 4 über $\mathbb{R}$.

Damit haben wir:

- SA-FEAS, QA-FEAS, HN, QUAD und 4-FEAS sind $\mathrm{NP}_{\mathbb{R}}$-vollständig.
- QA-FEAS, HN und QUAD sind $\mathrm{NP}_{\mathbb{C}}$-vollständig.
- QA-FEAS, HN und QUAD sind $\mathrm{NP}_{\mathbb{Z}_2}$-vollständig.

- Wir wollen zeigen, dass das Problem

$$3\mathrm{SAT} = \{\varphi \in 3\mathrm{CNF} : \varphi \text{ erfüllbar}\}$$

  $\mathrm{NP}_{\mathbb{Z}_2}$-vollständig ist. Dabei ist 3CNF die Menge aller aussagenlogischen Formeln in konjunktiver Normalform mit höchstens 3 Literalen pro Klausel. Zum Beispiel:

$$\varphi \equiv (x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_1 \vee x_4)$$

- Dazu reduzieren wir QUAD $/\mathbb{Z}_2$ auf 3SAT.
- Die $\mathrm{NP}_{\mathbb{Z}_2}$-Vollständigkeit von 3SAT folgt dann mit der Transitivität der Reduktionen, denn für $L \in \mathrm{NP}_{\mathbb{Z}_2}$ gilt dann

$$L \leq_p \mathrm{QUAD} \leq_p 3\mathrm{SAT}\,.$$

- Wir müssen also zu jedem System quadratischer Gleichungen

$$q_1(\mathbf{x}) = 0 \ \wedge \cdots \wedge \ q_m(\mathbf{x}) = 0$$

  eine äquivalente 3CNF-Formel φ konstruieren, d.h. es soll gelten:

$$\exists \mathbf{x} \ \ q_1(\mathbf{x}) = 0 \ \wedge \cdots \wedge \ q_m(\mathbf{x}) = 0 \quad \Leftrightarrow \quad \exists b \ \varphi(b)$$

Betrachte ein quadratisches Polynom q über $\mathbb{Z}_2$ in n Variablen. Schreibe q als:

$$q(\mathbf{x}) = \underbrace{\sum_{i=1}^{s} \sigma_i}_{S} + \underbrace{\sum_{j=1}^{t} \tau_j}_{T} + e$$

wobei σ_i die Form $x_k x_\ell$ und τ_j die Form x_k hat und $e \in \mathbb{Z}_2$ ist. Zum Beispiel:

$$q(x_1, x_2, x_3) = \underbrace{x_1 x_2 + x_2 x_3}_{\sigma_1+\sigma_2} + \underbrace{x_1 + x_3}_{\tau_1+\tau_2} + \underbrace{1}_{e}$$

Es ist q äquivalent zu folgendem System

$$S + T + e = 0 \tag{1}$$

$$\sigma_i + x_k x_\ell = 0,\ (i = 1, \ldots, s), \quad \tau_j + x_k = 0,\ (j = 1, \ldots, t) \tag{2}$$

$$S + \sigma_1 + y_1 = 0,\ y_1 + \sigma_2 + y_2 = 0,\ \ldots\ , y_{s-2} + \sigma_{s-1} + \sigma_s = 0 \tag{3}$$

$$T + \tau_1 + w_1 = 0,\ w_1 + \tau_2 + w_2 = 0,\ \ldots\ , w_{t-2} + \tau_{t-1} + \tau_t = 0 \tag{4}$$

in Variablen $S, T, \sigma_i, \tau_j, y_k, w_\ell$. Beachte dazu $a = -a$ für $a \in \mathbb{Z}_2$. Die Anzahl der neuen Variablen und Gleichungen ist polynomiell in der Länge von q.

- Die Gleichungen sind alle von der Form

$$a + b + c = 0 \quad \text{oder} \quad a + bc = 0.$$

- Es ist $a + b + c = 0$ äquivalent zu den 4 Gleichungen

$abc = 0 \wedge a(b+1)(c+1) = 0 \wedge (a+1)b(c+1) = 0 \wedge (a+1)(b+1)c = 0$

und $a + bc = 0$ äquivalent zu den 3 Gleichungen

$$a(b+1) = 0 \ \wedge \ a(c+1) = 0 \ \wedge \ (a+1)bc = 0.$$

- Insgesamt ist q äquivalent zu einem System mit Gleichungen der Form

$$w_1 w_2 w_3 = 0$$

mit w_j entweder gleich 1, einer Variable u_i oder $u_i + 1$.

- Definiere zu $w_1 w_2 w_3$ eine Klausel $v_1 \vee v_2 \vee v_3$ mit

$$v_j = \begin{cases} u_i, & \text{falls } w_j = u_i + 1 \\ \neg u_i, & \text{falls } w_j = u_i \\ 0, & \text{falls } w_j = 1 \end{cases}$$

Dann ist $w_1 w_2 w_3 = 0$ genau dann wenn $v_1 \vee v_2 \vee v_3 = 1$.

- Wir haben damit eine 3CNF-Formel φ_q zu q konstruiert mit

$$\exists \mathbf{x} \;\; q(\mathbf{x}) = 0 \quad \Leftrightarrow \exists \mathbf{u} \; \varphi_q(\mathbf{u})$$

- Einem quadratischen System

$$q_1(\mathbf{x}) = 0 \;\; \wedge \cdots \wedge \;\; q_m(\mathbf{x}) = 0$$

ordnen wir nun die 3CNF-Formel

$$\varphi_{q_1} \;\; \wedge \cdots \wedge \;\; \varphi_{q_m}$$

zu.

- Das quadratische System hat genau dann eine Lösung, wenn die zugehörige Formel erfüllbar ist.
- Die Länge der Formel ist polynomiell in der Länge des quadratischen Systems.
- Es folgt QUAD $\leq_p$ 3SAT.
- Mit der Vollständigkeit von QUAD und der Transitivität von $\leq_p$ folgt die Vollständigkeit von 3SAT.

Zusammenfassung

- 4-FEAS $/\mathbb{R}$, HN $/\mathbb{C}$ und 3SAT $/\mathbb{Z}_2$ sind NP-vollständig.
- Ist eines der Probleme in P_R (bzgl. passendem R), so gilt $\mathsf{P}_\mathsf{R} = \mathsf{NP}_\mathsf{R}$.
- Aber: Per Definition sind Probleme in P_R entscheidbar. Es ist nicht klar, ob auch alle Probleme in NP_R entscheidbar sind.
- Existieren unentscheidbare Probleme in NP_R, so ist $\mathsf{P}_\mathsf{R} \neq \mathsf{NP}_\mathsf{R}$.
- Andernfalls: Gilt $\mathsf{NP}_\mathsf{R} \subseteq \mathsf{EXP}_\mathsf{R}$?
- Wegen der Vollständigkeit genügt es, 4-FEAS, HN und 3SAT zu betrachten.

Theorem

a) 4-FEAS $/\mathbb{R}$ *ist entscheidbar und liegt in* $\mathrm{EXP}_{\mathbb{R}}$.

b) HN $/\mathbb{C}$ *ist entscheidbar und liegt in* $\mathrm{EXP}_{\mathbb{C}}$.

c) 3SAT $/\mathbb{Z}_2$ *ist entscheidbar und liegt in* $\mathrm{EXP}_{\mathbb{Z}_2}$.

Daraus folgt:

Korollar

Alle Probleme in NP_{R} sind entscheidbar und es gilt $\mathrm{NP}_{\mathrm{R}} \subseteq \mathrm{EXP}_{\mathrm{R}}$.

Zum Beweis des Theorems

- *Beweis von c):* Ist φ eine 3CNF-Formel in n Variablen, so kann man alle 2^n möglichen Belegungen in $\mathbb{Z}_2^n$ durchprobieren und jeweis prüfen, ob φ erfüllt ist. Damit ist 3SAT sogar in exponentieller Zeit entscheidbar.
- Für den Beweis von a) und b) benötigen wir tiefer liegende Resultate der Logik und der algebraischen Geometrie, die im Folgenden (ohne Beweis) vorgestellt werden.

- Es ist genau dann $f \in$ 4-FEAS wenn folgender Satz wahr ist:

$$\exists x_1 \ldots \exists x_n \; f(x_1, \ldots, x_n) = 0.$$

- Betrachte zunächst allgemeiner Formeln der Gestalt

$$\varphi(\mathbf{z}) \equiv Q_1 x_1 \ldots Q_k x_k \; \rho(x_1, \ldots, x_k, z) \qquad (*)$$

mit freien reellen Variablen $\mathbf{z} = (z_1, \ldots, z_n)$ und Quantoren $Q_i \in \{\forall, \exists\}$, wobei ρ eine quantorenfreie, boolesche Formel mit atomaren Prädikaten der Form

$$f_i(x_1, \ldots, x_k, \mathbf{z}) = 0 \qquad (\text{ oder } \leq 0, < 0),$$

mit rellen Polynomen f_i ist.

Beispiel

$$\varphi(z) \quad \equiv \quad \forall x \exists y \; (x^2 - \sqrt{2}z = 0 \; \vee \; xy + \frac{1}{2} < 0) \; \wedge \; x^3 yz + x^2 - 1 = 0$$

Theorem (Tarski)

Der Körper der reellen Zahlen $\mathbb{R}$ *erlaubt* **effektive Quantorenelimination**, *das heißt, zu jeder* **quantifizierten** *Formel* $\varphi(\mathbf{z})$ *der Form* $(*)$ *gibt es eine äquivalente,* **quantorenfreie** *Formel* $\psi(\mathbf{z})$ *mit denselben freien Variablen und der gleichen Bauart, und das Eliminiationsverfahren ist von einer BSS-Maschine berechenbar.*

Dabei bedeutet Äquivalenz der Formeln

$$\forall \mathbf{z}\ (\varphi(\mathbf{z}) \Leftrightarrow \psi(\mathbf{z})),$$

das heißt φ ist genau dann wahr wenn ψ wahr ist.

Beispiel

Die quantifizierte Formel

$$\varphi(a, b, c) \ \equiv\ \exists x : ax^2 + bx + c = 0$$

ist äquivalent zur quantorenfreien Formel

$$\psi(a, b, c) \ \equiv\ 0 \leq b^2 - 4ac.$$

Bei Eingabe eines Polynoms $f \in \mathbb{R}[X_1, \ldots, X_n]$ vom Grad ≤ 4:

- Führe den quantifizierten Satz

$$\exists x_1 \ldots \exists x_n \; f(x_1, \ldots, x_n) = 0.$$

  mit Hilfe der Quantorenelimination auf einen quantorenfreien Satz zurück.
- Prüfe den Wahrheitswert des quantorenfreien Satzes.

Beispiel

Der quantifizierte Satz

$$\exists x : 3x^2 - \pi x + \frac{1}{2} = 0$$

könnte beispielsweise zu

$$(-\pi)^2 - 4 \cdot 3 \cdot \frac{1}{2} \geq 0$$

werden.

Zur Komplexität des Verfahrens:

- Tarskis ursprünglicher Algorithmus zur Quantorenelimination läuft nicht in exponentieller Zeit.
- Es wurden Algorithmen vorgestellt, die 4-FEAS (allerdings mit einem anderen Verfahren) in exponentieller Zeit entscheiden.

Theorem (Effektiver Hilbertscher Nullstellensatz)

Seien $f_1, \ldots, f_k \in \mathbb{C}[X_1, \ldots, X_n]$. Die f_j haben genau dann **keine** *gemeinsame Nullstelle, wenn es $g_1, \ldots, g_k \in \mathbb{C}[X_1, \ldots, X_n]$ gibt mit*

$$\sum_{j=0}^{k} g_j f_j = 1.$$

Dabei können die g_j so gewählt werden, dass $\operatorname{grad} g_j \leq D$ *gilt, wobei D eine aus n und dem Grad der f_j berechenbare Zahl ist.*

Beispiel

Die beiden Polynome $f_1, f_2 \in \mathbb{C}[x, y]$ mit

$$f_1(x, y) = x^2 + xy + 1, \qquad f_2(x, y) = x + y$$

haben keine gemeinsame Nullstelle, denn es ist

$$\underbrace{1}_{g_1} \cdot f_1 + \underbrace{(-x)}_{g_2} \cdot f_2 = 1.$$

Betrachte die Polynome $f_1, f_2 \in \mathbb{R}[x, y]$ mit

$$f_1(x, y) = xy + 1, \quad f_2(x, y) = y.$$

Es wird zuerst die Gradschranke D für die g_j berechnet. Wir wählen der Einfachheit halber $D = 1$. Mache den Ansatz

$$g_1 = \sum_{|\alpha| \leq D} b_\alpha X^\alpha = b_{00} + b_{01} y + b_{10} x$$

$$g_2 = \sum_{|\alpha| \leq D} c_\alpha X^\alpha = c_{00} + c_{01} y + c_{10} x.$$

Gesucht sind nun die b_{ij}, c_{ij}, so dass $g_1 f_1 + g_2 f_2 = 1$. Es ist

$$\begin{aligned} g_1 f_1 + g_2 f_2 &= (b_{00} xy + b_{00} + b_{01} xy^2 + b_{01} y + b_{10} x^2 y + b_{10} x) \\ &\quad + (c_{00} y + c_{01} y^2 + c_{10} xy) \\ &= b_{00} + (b_{01} + c_{00}) y + c_{01} y^2 + b_{10} x + (b_{00} + c_{10}) xy + b_{01} xy^2 + b_{10} x^2 y. \end{aligned}$$

Löse nun (im Allgemeinen mit Gaußeliminiation):

$$b_{00} = 1, \ b_{01} + c_{00} = 0, \ c_{01} = 0, \ b_{10} = 0, \ b_{00} + c_{10} = 0, \ b_{01} = 0, \ b_{10} = 0.$$

Das liefert $g_1 = 1, \ g_2 = -x$.

Zusammenfassung

- Wir haben einige NP-vollständige Probleme über $\mathbb{R}, \mathbb{C}$ und $\mathbb{Z}_2$ kennengelernt, die Fragen zur Lösbarkeit polynomieller Gleichungen und Ungleichungen bzw. zur Erfüllbarkeit boolescher Formeln behandeln.
- Das Problem P_R vs. NP_R reduziert sich auf die Frage, ob ein vollständiges Problem in P_R liegt.
- Alle Probleme in $\mathrm{NP}_\mathbb{R}, \mathrm{NP}_\mathbb{C}$ und $\mathrm{NP}_{\mathbb{Z}_2}$ sind entscheidbar.
- Es gilt $\mathrm{NP}_\mathbb{R} \subseteq \mathrm{EXP}_\mathbb{R}$ und $\mathrm{NP}_\mathbb{C} \subseteq \mathrm{EXP}_\mathbb{C}$ und $\mathrm{NP}_{\mathbb{Z}_2} \subseteq \mathrm{EXP}_{\mathbb{Z}_2}$.
- Beweise benutzen nicht-triviale Resultate der Logik (Quantorenelimination) und der algebraischen Geometrie (effektiver Hilbertscher Nullstellensatz).
- Es gibt Ringe (z.B. $(\mathbb{Z}, =)$ und $(\mathbb{Q}, <)$) über denen $\mathrm{P} \neq \mathrm{NP}$ und $\mathrm{NP} \not\subset \mathrm{EXP}$ gilt.

- Blum, Cucker, Shub, Smale: *Complexity and Real Computation*.
- Cucker: *On the Complexity of Quantifier Elimination: the Structural Approach*,
  URL: http://comjnl.oxfordjournals.org/content/36/5/400.abstract
- Makowski: *Existential Theory of the Real Numbers*,
  URL: www.cs.technion.ac.il/∼janos/COURSES/THPR/tarskiproof.ps