Über Polynomideale, ihre Komplexität, und Anwendungen

Ernst W. Mayr

Technische Universität München

Frage: Folgt aus

$$\begin{aligned} -x^3 + y &= 0\,, \\ x^2y - z &= 0 \end{aligned}$$

stets

$$xy^3 - z^2 + y^5 - z^3 = 0\ ?$$

3 verschiedene (?) Formalismen

1. Endlich dargestellte kommutative Halbgruppen
2. Polynomideale
3. Petrinetze, Vektoradditionssysteme

1. Endlich dar. komm. Halbgruppen

Gegeben:

1. endliche Menge Σ von Symbolen, kommutativ
2. endliche Menge Γ von Kongruenzen:

$$l_i \equiv r_i;\ \ i = 1, \ldots, w;\ l_i, r_i \in \Sigma^*$$

3. Zeichenreihen $u, v \in \Sigma^*$.

Problem:

Ist $u \equiv v\ (\Gamma)$?

Beispiel:

$$\begin{aligned} a^2 &\equiv b \\ b^2c &\equiv c \end{aligned}$$

Dann gilt:

$$\begin{aligned} a^4c &\equiv c \\ a^4 &\not\equiv \lambda \end{aligned}$$

2. Polynomideale

Gegeben:

Eine endliche Menge von Polynomen

$$p_1, \ldots, p_w \in \mathbb{Q}[x_1, \ldots, x_n]$$

und ein Testpolynom p.

Das von den p_i erzeugte Ideal

$$\langle p_1, \ldots, p_w \rangle$$

ist die Menge all der Polynome q, die sich in der Form

$$q = \sum_{i=1}^{w} g_i p_i$$

mit Polynomen $g_i \in \mathbb{Q}[x_1, \ldots, x_n]$ darstellen lassen.

Problem:

Ist $p \in \langle p_1, \ldots, p_w \rangle$?

Das Problem

Seien Polynome $p, p_1, \ldots, p_w \in \mathbb{Q}[x_1, \ldots, x_n]$ gegeben.

Entscheidungsproblem:

Ist $p \in \langle p_1, \ldots, p_w \rangle$?

Darstellungsproblem:

Bestimme $g_i \in \mathbb{Q}[x_1, \ldots, x_n]$ so daß
$p = \sum_{i=1}^{w} g_i p_i$.

Ein kleines Beispiel

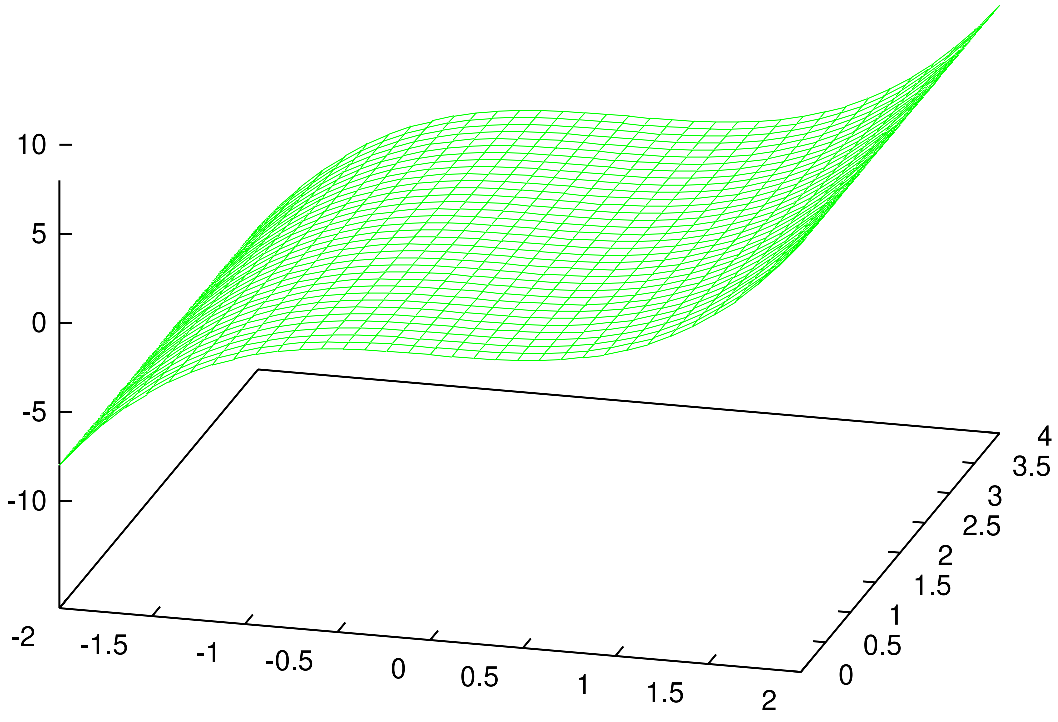
Wir betrachten das von den Polynomen

p_1: $y - x^2$, und

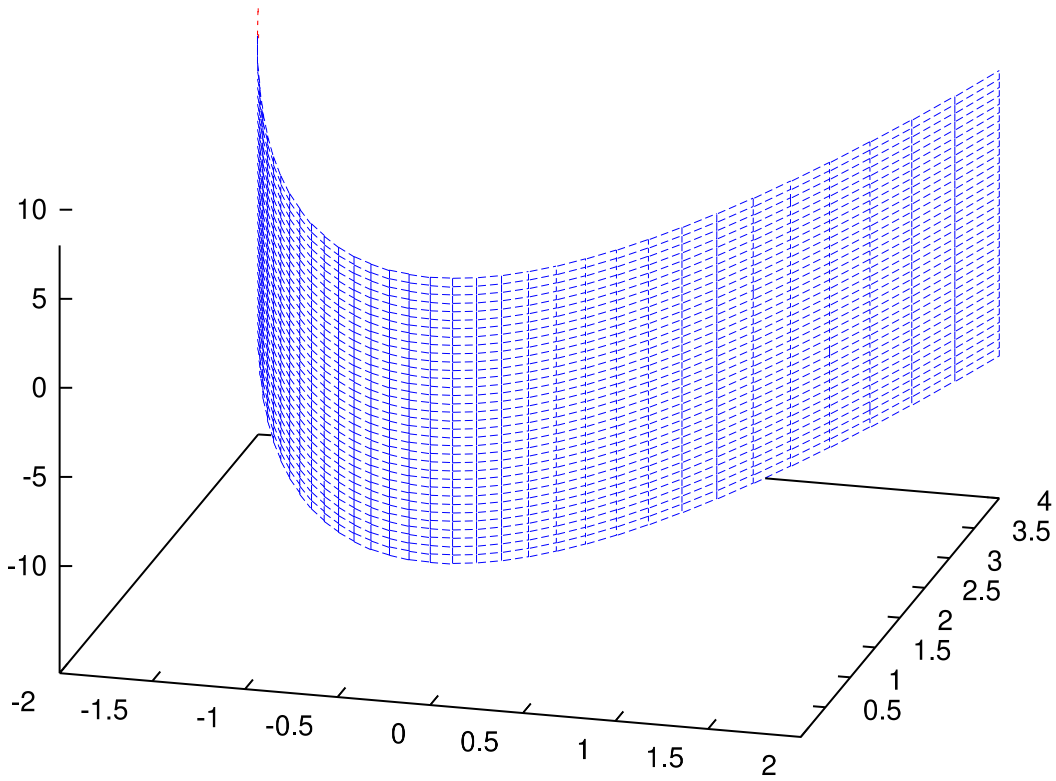
p_2: $z - x^3$

im $\mathbb{R}^3$ erzeugte Ideal.

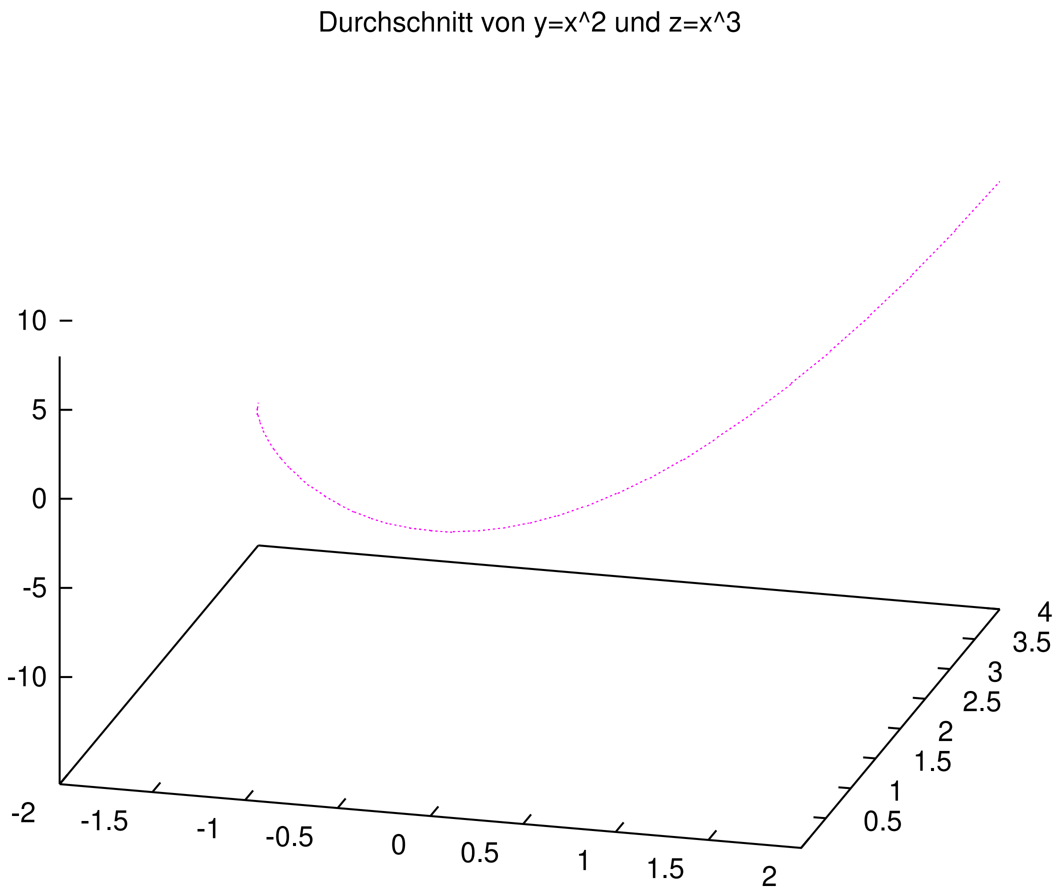
Die Nullstellen von $z - x^3$



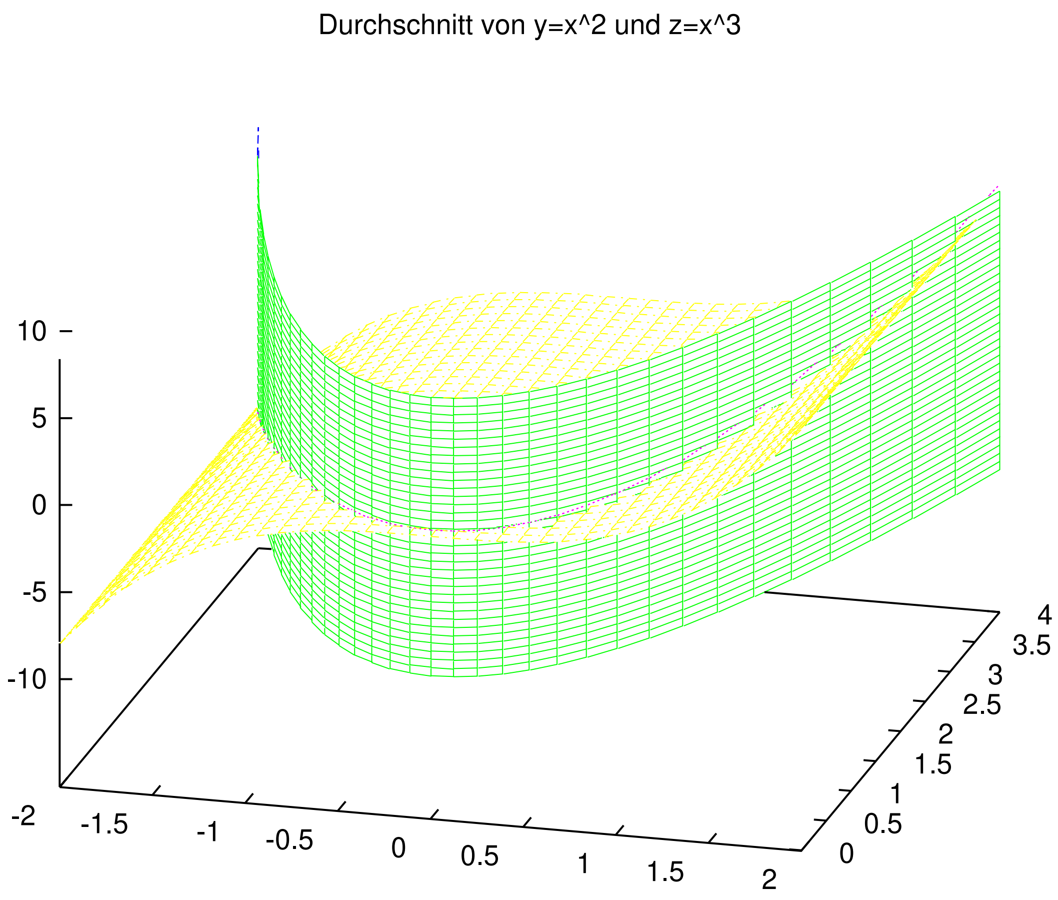
. . . und die Nullstellen von $y - x^2$



. . . und der Durchschnitt der beiden Flächen



Der Durchschnitt von $y = x^2$ und $z = x^3$



Es gilt:

$$\begin{aligned} y^2 - xz &= (y + x^2)(y - x^2) - x(z - x^3) \\ &= (y + x^2) \cdot p_1 - x \cdot p_2 \\ &\in \langle p_1, p_2 \rangle \end{aligned}$$

Dies hätten wir auch aus der Parameterisierung (u, u^2, u^3) des Durchschnitts der beiden Flächen $p_1 = 0$ und $p_2 = 0$ sehen können: Diese Kurve liegt ganz in der durch

$$y^2 - xz = 0$$

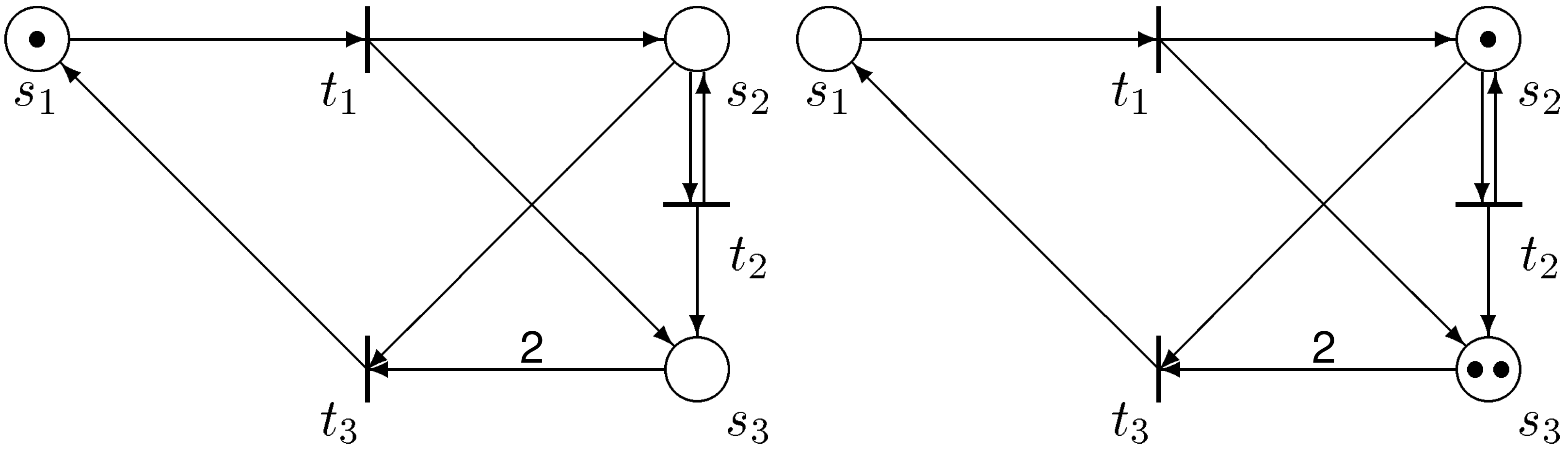
gegebenen Fläche.

Hilbert's Nullstellensatz

Theorem: *Sei k ein algebraisch abgeschlossener Körper, und seien $p, p_1, \ldots, p_w \in k[x_1, \ldots, x_n]$. Falls p auf allen gemeinsamen Nullstellen der p_i verschwindet, dann gibt es ein $e \in \mathbb{N}$, so daß*

$$p^e \in \langle p_1, \ldots, p_w \rangle.$$

3. Petrinetze und VAS



Markierung: Anzahl von Marken auf den Stellen

Feuern einer Transition: Markierungsänderung

Erreichbarkeitsmenge: Menge der erreichbaren Markierungen

Reversible PNs entsprechen endlich dargestellten kommutativen Halbgruppen:

Symbole: s_1, s_2, s_3

Kongruenzen:	Polynome:
$s_1 \equiv s_2 s_3$	$p_1 = s_2 s_3 - s_1$
$s_2 \equiv s_2 s_3$	$p_2 = s_2 s_3 - s_2$
$s_2 s_3^2 \equiv s_1$	$p_3 = s_1 - s_2 s_3^2$

Standard- (Gröbner-) Basen

Zulässige Termordnung:

(i) $x_{\pi(1)} \succ x_{\pi(2)} \succ \ldots \succ x_{\pi(n)} \succ 1$

(ii) Seien m, m_1, m_2 Monome mit $m_1 \prec m_2$. Dann

$$mm_1 \prec mm_2 \, .$$

Beispiele:

1. lex: $x_1^2 \succ x_1 x_2^3 x_3^5$
2. grevlex: $x_2^3 \succ x_1$ und $x_1 x_2 x_3 \succ x_1 x_3^2$

Definition: Seien I ein Ideal in $\mathbb{Q}[x] = \mathbb{Q}[x_1, \ldots, x_n]$ und $\prec$ eine zulässige Termordnung. Eine Menge $\{g_1, \ldots, g_r\}$ von Polynomen aus $\mathbb{Q}[x]$ heißt Standard- oder Gröbnerbasis von I (bzgl. $\prec$), wenn gilt:

1. $\{g_1, \ldots, g_r\}$ ist Basis von I;
2. $\{LT(g_1), \ldots, LT(g_r)\}$ ist eine Basis des Leading Term Ideals von I, also des kleinsten Ideals, das die führenden Terme aller $f \in I$ enthält.

Beispiel

Betrachte die Basis

$$\{x^5 + y^4 + z^3 - 1, x^3 + y^2 + z^2 - 1\}$$

mit der invers lex Termordnung.

Es ergibt sich folgende Gröbnerbasis:

Ändert man die Basis leicht:

$$\{x^5 + y^4 + z^3 - 1, x^3 + y^3 + z^2 - 1\}$$

so ergibt sich:

Etwas Literatur

— Entscheidbarkeit: Hilbert [1890], G. Hermann [1926]

für Ringe: Seidenberg [1974], Richman [1974]

— Doppelt exponentielle Gradschranke für Koeffizienten aus $\mathbb{Q}$: Hermann [1926], Mayr/Meyer [1982]

— Exp. Gradschranke für spezielle p: Brownawell[1987], Heintz et al.[1988], Berenstein/Yger [1988]

— Exponentielle obere Platzschranke für endlich dargestellte kommutative Halbgruppen (fpcs): Mayr/Meyer [1982]

— Exponentielle untere Platzschranke, für fpcs's: Mayr/Meyer [1982]

— Exponentielle obere Platzschranke für das allgemeine Wortproblem, mit Koeffizienten in $\mathbb{Q}$: Mayr [1988]

— Doppelt exponentielle obere Gradschranke für Gröbnerbasen: Dubé [1990]

Die Komplexität des WP für kommut. Halbgruppen

Theorem: *Sei* $d = \max\{\deg(p_i)\}$. *Falls*

$$p \in \langle p_1, \ldots, p_w \rangle,$$

dann gibt es $g_1, \ldots, g_w$, *so daß*

$$\text{(i)} \quad p = \sum_{i=1}^{w} g_i p_i;$$

$$\text{(ii)} \quad \deg(g_i) \leq \deg(p) + (wd)^{2^n}.$$

Siehe Hermann [1926], Mayr/Meyer [1982]. Daraus folgt:

Korollar: *Das (uniforme) Wortproblem für endlich dargestellte kommutative Halbgruppen kann mit exponentiellem Platzbedarf (in der Größe der Eingabe) gelöst werden.*

Siehe Mayr/Meyer [1982].

. . . und die ”schlechte” Nachricht:

Theorem: *Jedes Problem, das zu seiner Lösung exponentiellen Platzes bedarf, kann auf ein (etwa) gleich großes Wortproblem für (endlich dargestellte) kommutative Halbgruppen reduziert werden.*

Siehe Mayr/Meyer [1982].

Daraus folgt sofort:

Korollar: *Das (uniforme) Wortproblem für endlich dargestellte kommutative Halbgruppen hat im* worst case *exponentiellen Platzbedarf.*

Folgerungen

Aus der exponentiellen unteren Platzschranke für das Wortproblem für kommutative Halbgruppen folgt sofort eine ebensolche untere Schranke für das (uniforme) Wortproblem für Polynomideale, da das erste ein Spezialfall des letzteren ist:

Betrachte u, v und die l_i und r_i als Monome. Dann gilt:

$$u \equiv v \ (\Gamma) \Longleftrightarrow u - v \in \langle r_1 - l_1, \ldots, r_w - l_w \rangle$$

Ebenso folgt eine exponentielle untere Platzschranke für das Erreichbarkeitsproblem bei reversiblen Petrinetzen und damit bei Petrinetzen bzw. Vektoradditionssystemen.

Eine untere Schranke für Gröbnerbasen

Aus der exponentiellen unteren Platzschranke für das Wortproblem für kommutative Halbgruppen folgt auch, daß es Polynomideale gibt, für die jede *Gröbnerbasis* (Standardbasis) mindestens $2^{2^{cn}}$ Elemente sowie Elemente vom Grad $\geq 2^{2^{cn}}$ enthalten muß (hierbei ist n die Größe des Problems und $c > 0$ eine geeignete Konstante).

Obere Schranke für das WP bei Polynomidealen

Aufgrund von Hermann's Gradschranke läßt sich die Lösbarkeit von

$$p = \sum_{i=1}^{w} g_i p_i$$

(wo die Unbekannten g_i Polynome sind) auf die Lösbarkeit eines linearen Gleichungssystem mit den Koeffizienten der Monome, deren Grad unterhalb Hermann's Schranke liegt, als Unbekannten reduzieren. Die Dimension dieses Gleichungssystems ist

$$2^{2^{cn}},$$

(n und c wie oben). Es ist möglich, die Lösbarkeit dieses linearen Gleichungssystems zu bestimmen, ohne es je explizit hinzuschreiben. Eine geschickte Implementierung benötigt lediglich Platz, der exponentiell in n ist.

Ebenso ergibt sich:

Theorem: *Ist* $p = \sum_{i=1}^{w} g_i p_i$*, so lassen sich geeignete Polynome* g_i *in exponentiellem Platz berechnen (Um die Ausgabe hinzuschreiben, wird im allgemeinen wesentlich mehr Platz benötigt).*

Sowie:

Theorem: *Sind die Voraussetzungen für Hilbert's Nullstellensatz erfüllt, so läßt sich ein geeigneter Exponent* e *in exponentiellem Platz berechnen.*

Spezialfälle für Polynomideale

Aus von Brownawell [1986] und anderen gegebenen Gradschranken folgt, daß das Wortproblem für Polynomideale in den beiden Spezialfällen

1. 0-dimensional, und
2. homogen,

mit polynomiellem Platzbedarf gelöst werden kann.

Durch eine Reduktion vom LBA-Problem erhalten wir das

Theorem: *Das Wortproblem für Polynomideale mit homogenen Erzeugenden ist PSPACE-vollständig.*

Zusammenfassung, offene Probleme

Es besteht ein enger Zusammenhang zwischen der Komplexität von Problemen für kommutative Halbgruppen, Petrinetze und Polynomideale. Dadurch ergeben sich zum Teil überraschende Anwendungen für in einzelnen Teilgebieten erzielte Ergebnisse.

Offene Probleme:

1. Welche Eigenschaften von Idealen machen PIMP einfacher?
2. Betrachte Polynomringe über den ganzen Zahlen!
3. Bestimme die Komplexität des Erreichbarkeitsproblems für Petrinetze ($\equiv$ Koeffizienten in $\mathbb{N}$ oder $\mathbb{Q}^+$)!