Komplexitätstheorie und Polynomideale II

Studienstiftungsseminar St. Johann 1998
Arbeitsgruppe "Quo vadis, Komplexitätstheorie?"
Christian Bohr

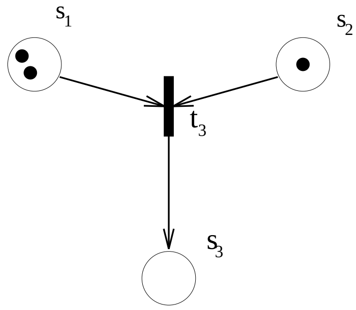
14. September 1998

Inhaltsverzeichnis

1 Endlich präsentierte Halbgruppen und Petrinetze

Ein **Petri-Netz** ist eine Art dynamisches System, bestehend aus einem gerichteten Graphen mit zwei Arten von Knoten: den sogenannten "Stellen" und den "Schaltern". Kanten dürfen nur von einer Stelle zu einem Schalter und umgekehrt laufen. Die Kanten können gewichtet sein. Zusätzlich ist jede Stelle mit einer natürlichen Zahl markiert. Man kann sich die Stellen als eine Art Vorratsbehälter vorstellen, deren Inhalt durch die jeweilige Zahl ("marking") quantifiziert wird.

Symbolisiert wird ein Petrinetz durch ein Diagramm, in dem die Stellen als Kreise und die Schalter als Striche symbolisiert werden. Ein Beispiel:

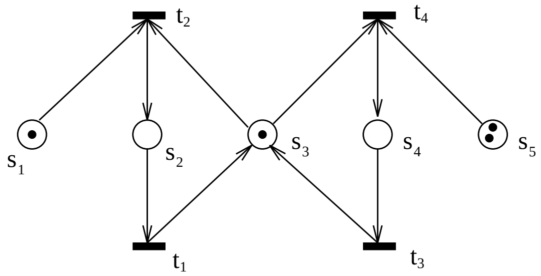


Beginnt das Petri-Netz zu laufen, so kann jeder Schalter feuern, wenn für jede einlaufende Kante der Ausgangspunkt (eine Stelle) mindestens ein Element enthält. In diesem Fall wird jeder dieser Stellen ein Element entzogen und jeder Stelle, die Endpunkt einer von dem betrachteten Schalter auslaufenden Kante ist, ein Element hinzugefügt. Dabei kann es passieren, daß von mehreren Schaltern nur einer feuern kann, weil diese Schalter mit der gleichen Stelle verbunden sind. Es gibt mehrere Methoden in diesem Fall zu entscheiden, welcher Schalter feuert, meist geschieht dies zufällig. Formal ist ein Petri-Netz wie folgt definiert:

Definition 1. *Ein Petri-Netz ist ein Quadrupel aus einer endlichen Menge S, den Stellen, einer endlichen Menge T, den Schaltern, einer Abbildung $F : S \times T \cup T \times S \to \mathbb{N}$, die die Kanten bewertet (d.h. Null ist, falls keine Kanten zwischen den beiden Knoten existiert) und einer Abbildung $m : S \to \mathbb{N}$. Ein Schalter $t \in T$ kann feuern, wenn für alle $s \in S$ $m(s) \geq F(s,t)$ gilt. Dabei produziert er den neuen Zustand m' mit $m'(s) = m(s) - F(s,t) + F(t,s)$ für alle $s \in S$, notiert als $m \xrightarrow{t} m'$.*

Ein Petri-Netz heißt reversibel, wenn es zu jedem $t \in T$ ein $t^{rev} \in T$ mit $F(s,t) = F(t^{rev}, s)$ und $F(t,s) = F(s, t^{rev})$ für alle $s \in S$ gibt. Natürlich kann man ein Petri-Netz durch Hinzufügen von Schaltern immer reversibel machen.

Petri-Netze kann man zur Beschreibung von “Nebenläufigkeiten” benutzen, d.h. mehrere Prozesse laufen unabängig voneinander ab, ohne sich gegenseitig zu stören, selbst wenn sie gemeinsame Betriebsmittel benutzen. In dem Petri-Netz



gibt es zwei "Prozesse", gegeben durch s_1, s_2, t_1 und t_2 bzw. s_4, s_5, t_3 und t_4. Jeder von ihnen kann nur arbeiten, wenn der jeweils andere nicht gerade aktiv ist. Z.B. könnten die beiden Prozesse für Vorgänge, die durch die Schalter t_2 und t_4 beschrieben werden, einen gemeinsamen Drucker benötigen und t_1 bzw. t_3 dessen Freigabe symbolisieren. Die Stelle s_3 bewirkt dann, daß ein Prozess den Drucker nur benutzen kann, wenn der jeweils andere ihn freigegeben hat. Im obigen Zustand können z.B. t_2 und t_4 feuern (=Drucken), aber das Feuern eines Schalters blockiert den jeweils anderen. Die Markierungen in s_1 und s_5 können als Druckjobs gedeutet werden, die nacheinander abgearbeitet werden.

Interessante Fragen im Zusammenhang mit Petrinetzen liegen auf der Hand:

- Seien zwei Zustände des Netzes gegeben. Gibt es eine endliche Folge von Zuständen, die den einen in den anderen überführt, so daß je ein Zustand aus dem vorherigen durch Feuern eines Schalters hervorgeht (das "Erreichbarkeitsproblem")?

- Ist die Zahl der Zustände, die von einem gewissen Anfangszustand erreichbar sind endlich?

Diese Fragen lassen sich in Fragen über Polynomideale zurückführen. Ein nützlicher Zwischenschritt dabei ist es, diese Fragen als Fragen über Halbgruppen zu formulieren:

Definition 2. *Eine Halbgruppe ist ein Paar $(G, \cdot)$ aus einer Menge G und einer Abbildung ("Verknüpfung") $\cdot : G \times G \to G, (a, b) \mapsto a \cdot b$ mit folgenden Eigenschaften:*

1. *Für alle $a, b, c \in G$ gilt $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*

2. *Es gibt ein Element $1 \in G$ mit $1 \cdot a = a \cdot 1 = 1$ für alle $a \in G$.*

Meistens schreibt man einfach ab statt $a \cdot b$. Die Halbgruppe heißt kommutativ, wenn für alle $a, b \in G$ $a \cdot b = b \cdot a$ gilt.

Das einfachste Beispiel ist $\mathbb{N}^n$ mit der Addition. Eine dazu isomorphe Halbgruppe heißt eine freie Halbgruppe von endlichem Rang. Diese Halbgruppen sehen wie folgt aus: Sei $S = \{s_1, \ldots s_n\}$ eine endliche Menge. Dann ist die Menge S^* der Wörter über S, also die Menge der endlichen Folgen von Elementen aus S eine Halbgruppe, die Multiplikation ist durch Hintereinanderschreiben gegeben. Erlaubt man "Umsortieren", so ist die Halbgruppe kommutativ. Benutzt man die Multiindexschreibweise, so ist der Isomorphismus $\mathbb{N}^n \cong S^*$ durch $\alpha \to s^\alpha = s_1^{\alpha_1} \cdot \cdots \cdot s_n^{\alpha_n}$ gegeben.

Aus freien Halbgruppen gewinnt man durch Äquivalenzklassenbildung die sogenannten endlich präsentierten Halbgruppen: Sei $\mathcal{P} \subset S^* \times S^*$ eine endliche Menge von Kongruenzen (l, s), notiert als $l \equiv s$. Die Relation

$$m \equiv m' \Leftrightarrow \text{es gibt ein } \tilde{m} \in S^* \text{ und } (l, r) \in \mathcal{P} \text{ mit } m' = \tilde{m}l, m = \tilde{m}r$$

erzeugt eine Äquivalenzrelation $\equiv_\mathcal{P}$ auf S^*, und $S^*/\equiv_\mathcal{P}$ ist wieder eine Halbgruppe. Eine Halbgruppe heißt endlich präsentiert, wenn sie zu einer solchen Halbgruppe isomorph ist.

Das System $\mathcal{P}$ von Kongruenzen heißt auch kommutatives semi-Thue-System über S und kommutatives Thue-System, wenn $(l, r) \in \mathcal{P} \Leftrightarrow (r, l) \in \mathcal{P}$ gilt.

Es zeigt sich nun, daß reversible Petri-Netze und kommutative Thue-Systeme im wesentlichen das gleiche sind. Hier soll der Weg von einem Petri-Netz zu einem Thue-System am obigen Beispiel beschrieben werden:

Zunächst muß man durch Hinzufügen eines Schalters t^{rev} das Netz reversibel machen. Das "Alphabet" S ist einfach die Menge der Stellen des Petri-Netzes, also hier $\{s_1, s_2, s_3\}$. Ein Zustand $m : S \to \mathbb{N}$ wird zu einem Wort $s^{m(s)} = \Pi_i s_i^{m(s_i)}$. Die Relationen müssen nun so gewählt werden, daß zwei Wörter genau dann äquivalent sind, wenn die zugehörigen Zustände ineinander übergeführt werden können. In diesem Fall gibt es nur einen Schalter, und dieser macht aus einem Wort s^α das Wort s^β mit $\beta = \alpha + (-1, -1, 2)$. Bringt man die negativen Exponenten (die ja in einer Halbgruppe keinen Sinn machen) auf die andere Seite, so erhält man

$$s^\alpha s_1 s_2 \xrightarrow{t_1} s^\alpha s_3^2.$$

Die richtige Relation ist also $s_1 s_2 \equiv s_3^2$. Der Schalter t^{rev} erzeugt natürlich auch eine Relation, diese ist gerade $s_3^2 \equiv s_1 s_2$. Diese beiden Relationen bilden also ein kommutatives Thue-System über S. Die dadurch definierte Äquivalenzrelation hat die Eigenschaft, daß eine Äquivalenzklasse genau der Menge aller Zustände entspricht, die durch Feuern des Schalters ineinander überführt werden können.

Allgemein erzeugt jeder Schalter t eine Kongruenz $(l, r) \in \mathcal{P}$ mit $l = \Pi_i s_i^{F(s_i,t)}$, $r = \Pi_i s_i^{F(t,s_i)}$. Damit ist auch klar, wie man zu einem kommutativen Thue-System $\mathcal{P}$ über S ein Petri-Netz erhält. Insgesamt hat man also eine 1-1-Korrespondenz

$$\text{reversible Petri-Netze} \Leftrightarrow \text{kommutative Thue-Systeme.}$$

Nun lassen sich die oben aufgeworfenen Fragen über Petri-Netze als Fragen über Präsentationen von Halbgruppen formulieren: Sei $(S, \mathcal{P})$ die Präsentation einer Halbgruppe (d.h. ein kommutatives Thue-System). Dann sind zu den obigen Problemen äquivalent:

- Seien $m, m' \in S^*$. Gilt $m \equiv_{\mathcal{P}} m'$?
- Sei $m \in S^*$. Ist die Klasse $[m]$ endlich?

Im nächsten Abschnitt sollen diese Fragen als Fragen über Ideale in Polynomringen formuliert und Aussagen über ihre Komplexität gemacht werden.

2 Der Zusammenhang mit Polynomidealen und Resultate über die Komplexität

Der Einfachkeit halber soll die Umformulierung der Halbgruppen-Probleme in Problemstellungen über Polynomideale nur für das erste der beiden Probleme, das Äquivalenzproblem, durchgeführt werden. Sei also S eine endliche Menge und $\mathcal{P}$ ein kommutatives Thue-System über S. Wir benutzen die Elemente $s_1, \ldots, s|n$ von S als Unbekannte und betrachten den Polynomring $\mathbb{Q}[s_1, \ldots, s_n] = \mathbb{Q}[s]$. Damit kann man jedes Wort in S^* als Monom in $\mathbb{Q}[s]$ interpretieren. Die Kongruenzen $(l, r) \in \mathcal{P}$ definieren nun jeweils ein Polynom $l - r$ in $\mathbb{Q}[s]$ und somit definiert $\mathcal{P} = (l_i, r_i)_{i \in I}$ ein Ideal $I = (l_1 - r_1, \ldots, l_w - r_w)$ in $\mathbb{Q}[s]$. Man sieht nun leicht daß für $m, m' \in S^*$ gilt

$$m \equiv_{\mathcal{P}} m' \Leftrightarrow m' - m \in I,$$

d.h. das Problem, zu entscheiden, ob zwei Wörter bzgl. $\mathcal{P}$ äquivalent sind, ist darauf zurückgeführt, zu entscheiden, ob ein gewisses Polynom in einem Ideal liegt. In der englischen Literatur wird diese Problem mit PIMP (polynomial ideal membership problem) abgekürzt. Wie komplex ist nun dieses Problem? Bereits aus dem Jahre 1926 stammt eine fundamentale Abschätzung.

Satz 1. *(G. Hermann) Sei $I = (g_1, \ldots, g_w) \subset \mathbb{Q}[x]$ ein Ideal, d der maximale Totalgrad der g_i sowie $f \in I$. Dann gibt es Polynome $p_1, \ldots, p_s \in \mathbb{Q}[x]$ mit $f = \sum_i p_i g_i$ und $deg(p_i) \leq deg(f) + (wd)^{2^n}$.*

Daraus kann man - unter Benutzung von Algorithmen für Parallelrechnermodelle und der "Parallel Computation Thesis" - folgendes Resultat über PIMP ableiten:

Satz 2. *[1] PIMP ist mit einer Turing-Maschine lösbar, deren Arbeitsbandlänge exponentiell von der Länge der Eingabe abhängt.*

Dieses Komplexitätsresultat für PIMP impliziert sofort die entsprechende Aussagen für das Äquivalenzproblem bei Halbgruppenpräsentationen und das Erreichbarkeitsproblem bei Petri-Netzen. Mit dem gleichen Aufwand kann man übrigens auch Darstellungen $f = \sum_i p_i g_i$ berechnen bzw. bei Petri-Netzen eine Folge von Zuständen angeben, die zwei Markierungen ineinander überführt, falls das überhaupt möglich ist.

Die nächste Frage ist natürlich, ob es nicht sogar bessere Algorithmen gibt. Die Antwort darauf gibt der nächste Satz:

Satz 3. *[2] Das Äquivalenzproblem für endlich präsentierte kommutative Halbgruppen ist in EXPSPACE.*

Da dieses Problem auf PIMP reduzierbar ist, folgt sofort, daß auch $PIMP$ in $EXPSPACE$ liegt. Insbesondere gibt es also Instanzen des Problems, die von keiner Turing-Maschine mit weniger als exponentieller Arbeitsbandgrösse gelöst werden können. Bewiesen wird dieser Satz dadurch, daß man ein Verfahren zur Reduktion auf eine Klasse angibt, deren Vollständigkeit bekannt ist, hier wird die Klasse der doppelt exponentiell beschränkten und terminierenden 3-Registermaschinen benutzt.

3 Weitere Komplexitätsresultate für Polynomideale

3.1 Berechnung von Gröbnerbasen

In diesem Abschnitt soll ein Komplexitätsergebnis für das Problem der Berechnung von (reduzierten) Gröbnerbasen vorgestellt werden. Zunächst hat man eine Abschätzung über den maximalen Grad der Polynome in einer Gröbnerbasis:

Satz 4. *[4] Sei $I = (g_1, \ldots, g_w) \subset \mathbb{Q}[x]$ ein Ideal , d der maximale Totalgrad der g_i und sei eine zulässige Termordnung gegeben. Dann besteht die reduzierte Gröbnerbasis für I aus Polynomen der Ordnung $\leq 2(\frac{d^2}{2} + d)^{2^{n-1}}$.*

Ähnliche Abschätzungen existieren für den Grad der Normalform eines Polynoms bzgl. der reduzierten Gröbnerbasis eines Ideals. Damit kann man - wieder auf dem Umweg über Aufwandsabschätzungen für parallelisierte Algorithmen - den folgenden Satz beweisen:

Satz 5. *[1] Um die reduzierte Gröbnerbasis eines Ideals (mit gegebenen Erzeugern) mit einer Turing-Maschine zu berechnen genügt ein Arbeitsband, dessen Länge exponentiell von der Länge der Eingabe abhängt.*

3.2 Der Nullstellensatz

Der Nullstellensatz von Hilbert sagt aus, daß für ein Polynom f genau dann an allen gemeinsamen komplexen Nullstellen von endlich vielen Polynomen $g_1, \ldots, g_w$ verschwindet, wenn eine Potenz von f in dem von den g_i erzeugten Ideal liegt. Ein Spezialfall davon ist folgende Aussage: Seien $g_1, \ldots, g_w$ Polynome mit Koeffizienten in $\mathbb{C}$. Das Gleichungssystem

$$\begin{aligned} g_1(x_1, \ldots, x_n) &= 0 \\ g_2(x_1, \ldots, x_n) &= 0 \\ &\cdot \\ &\cdot \\ &\cdot \\ g_w(x_1, \ldots, x_n) &= 0 \end{aligned}$$

besitzt genau dann eine Lösung, wenn $1 \notin (g_1, \ldots, g_w)$ gilt. Sind die g_i rational und haben keine gemeinsame Lösung in $\mathbb{C}^n$, dann gilt auch $1 \in (g_1, \ldots, g_w) \subset \mathbb{Q}[x]$. Glücklicherweise sind diese speziellen Instanzen von PIMP wesentlich weniger komplex als das allgemeine Problem. Wieder über eine Gradabschätzung ([5]) beweist man

Satz 6. *[1] Sei $I = (g_1, \ldots, g_w) \subset \mathbb{Q}[x]$ ein Ideal, $f \in \mathbb{Q}[x]$ ein Polynom. Die Frage, ob $f^e \in (g_1, \ldots, g_w)$ für ein $e \in \mathbb{N}$ gilt, kann von einer Turing-Maschine entschieden werden, deren Arbeitsbandlänge polynomial von der Länge der Eingabe abhängt.*

Für Spezialfälle von PIMP ist also die Komplexität wesentlich geringer als im allgemeinen Fall. Ein anderer "schöner" Fall tritt schließlich auf, wenn die Erzeuger g_i alle homogen sind, dann hat man wieder Gradabschätzungen für die p_i in $f = \sum_i p_i g_i$ und diese zeigen, daß in diesem Fall PIMP wieder mit in der Eingabe polynomialer Länge des Arbeitsbandes gelöst werden kann.

4 Ein Beispiel

Das Petri-Netz aus dem zweiten Beispiel definiert folgende Halbgruppenpräsentation: Die Menge der Erzeuger ist $\{s_1, \ldots, s_5\}$ und die Relationen sind

$$\begin{aligned} s_2 &\equiv s_3 \\ s_1 s_3 &\equiv s_2 \\ s_4 &\equiv s_3 \\ s_5 s_3 &\equiv s_4. \end{aligned}$$

Eine mögliche Startsituation ist $m = (2, 0, 1, 0, 1)$, d.h. beide Prozesse haben noch Druckjobs und s_3 ist besetzt. Als Polynom in $\mathbb{Q}[s]$ entspricht das dem Monom $s_1^2 s_3 s_5$. Der erwünschte Endzustand ist $m_1 = (0, 0, 1, 0, 0)$. Ein mögliches Problem könnte der Zustand $m_2 = (1, 0, 0, 0, 0)$ sein, in dem kein Drucker mehr drucken kann, obwohl noch Druckaufträge vorhanden sind ("Deadlock"). Um zu klären, welcher der beiden Endzustände von m_0 ausgehend möglich ist muß man also berechnen, welches der Polynome $f = s_3 - s_1^2 s_3 s_5$ bzw. $g = s_1 - s_1^2 s_3 s_5$ in dem Ideal

$$I = (s_2 - s_3, s_1 s_3 - s_2, s_4 - s_3, s_5 s_3 - s_4) \subset \mathbb{Q}[s]$$

liegt. Das entsprechende Singular-Programm lautet:

```
ring r = 0,(s1,s2,s3,s4),dp;
ideal I = s2-s3,s1*s3-s2,s4_s3,s5*s3-s4;
poly m0 = s1*s1*s3*s5;
poly m1 = s3;
poly m2 = s1;
ideal J = groebner(I);
poly f = m1 - m0;
reduce (f,J);
poly g = m2 - m0;
reduce (g,J);
```

Dieses Netz lässt sich auch mit einem in Java geschriebenen Programm simulieren, das sich unter http://www.ee.uwa.edu.au/ ˜ braunl/pns findet. Das Algebra-Programm Singular wird unter http://www.mathematik.uni-kl.de/˜zca/Singular/distribution.html angeboten.

Literatur

[1] Some Complexity Results for Polynomial Ideals, E.W. Mayr, Journal of Complexity 13, 1997, 303-325

[2] E.W. Mayr, A. Meyer, The complexity of the word problem for commutative semigroups and polynomial ideals, Adv. Math. 46(3), 1982, 305-329

[3] E.W. Mayr, On Polynomial Ideals, their Complexity and Applications, Technical Report TUM-I9520, 1995 (http://www14.informatik.tu-muenchen.de:80/berichte/1995/tum-i9520.html)

[4] T.W. Dube, The structure of polynomial ideals and Gröbner bases, SIAM J. Comput. 19, 1990, 750-773

[5] W.D. Brownawell, Bounds for the degrees in the Nullstellensatz, Ann. of Math. 126, 1987, 577-591