IV. Weitere zum Erfüllungsproblem polynomial äquivalente kombinatorische Aufgaben

von Joachim von zur Gathen und Malte Sieveking

Wir geben zunächst nach (Karp 1972) neun vollständige Sprachen in NP an. Dann wird gezeigt, dass die zu den lösbaren rationalen, diophantischen und modularen Gleichungssystemen gehörigen Sprachen in P sind. Anschliessend werden rationale und diophantische Ungleichungssysteme untersucht, wobei die letzteren wiederum eine vollständige Sprache in NP ergeben. Im letzten Teil wird die Reduzibilität von ganzen Zahlen und von Polynomen behandelt.

Die Bezeichnungen sind die gleichen wie in III, wo auch die 0-1-Kodierungen der betrachteten Sprachen beschrieben sind.

1. DREIFAERBBARKEIT ist eine vollständige Sprache. Sie besteht aus allen Graphen (P,K) mit der Eigenschaft, dass es eine Abbildung $\phi\colon P \longrightarrow \{f_0,f_1,f_2\}$ gibt mit

$$(\forall p,q \in P)\ \{p,q\} \in K \Longrightarrow \phi(p) \neq \phi(q),$$

d.h. dass der Graph mit drei Farben f_0,f_1,f_2 färbbar ist.

Die Vollständigkeit beweisen wir mit folgender Transformation:

ERFUELLBARKEIT MIT HOECHSTENS DREI VARIABLEN PRO KLAUSEL $\leq_\pi$ DREIFAERBBARKEIT.

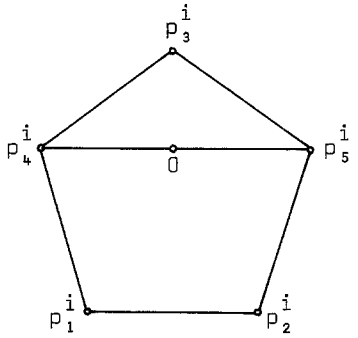
Seien $C_1,\ldots,C_m$ Disjunktionen von jeweils höchstens drei Elementen von $\{x_1,\ldots,x_n,\bar{x}_1,\ldots,\bar{x}_n\}$. Falls nötig, erreichen wir durch Wiederholung, dass in jedem C_i genau drei Zeichen vorkommen. Jedes C_i hat dann die Form $C_i = y_{i1} \vee y_{i2} \vee y_{i3}$, wobei y_{ik} ein x_j oder ein $\bar{x}_j$ ist.
Der Formel $C_1 \wedge \ldots \wedge C_m$ ordnen wir den Graphen $G = (P,K)$ zu mit

$$P = \{0,2\} \cup \{x_j \mid j \leq n\} \cup \{\bar{x}_j \mid j \leq n\} \cup \{p_k^i \mid i \leq m,\ k \leq 5\}$$

$$K = \{\{0,2\}\} \cup \{\{x_j,2\} \mid j \leq n\} \cup \{\{\bar{x}_j,2\} \mid j \leq n\}$$

$$\cup\ \{\{x_j,\bar{x}_j\} \mid j \leq n\} \cup \{\{y_{ik},p_k^i\} \mid i \leq m,\ k \leq 3\}$$

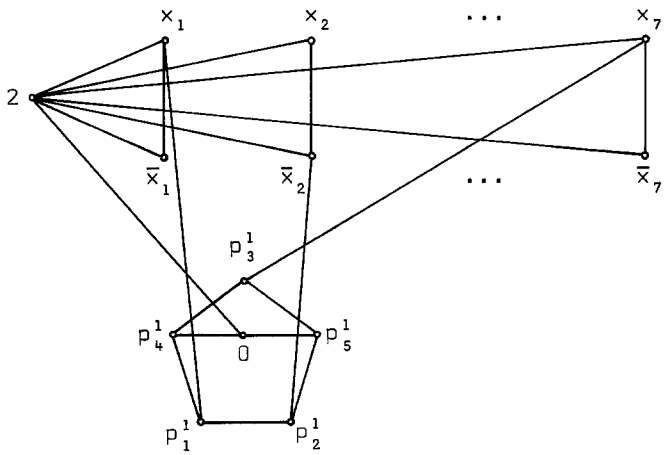
$\cup$ für alle $i \leq m$ folgende sieben Kanten:



Bemerke, dass 0 den gleichen Punkt für alle i bezeichnet.

(Dieser Graph wurde von E. Specker vorgeschlagen.)

<u>Beispiel</u> $C_1 = x_1 \vee \bar{x}_2 \vee x_7$, also $y_{11} = x_1$, $y_{12} = \bar{x}_2$, $y_{13} = x_7$.



Wir zeigen, dass $C_1 \wedge \ldots \wedge C_m$ erfüllbar ist genau dann, wenn G dreifärbbar ist.

Sei $C_1 \wedge \ldots \wedge C_m$ erfüllbar und $v: \{x_1,\ldots,x_n\} \longrightarrow \{0,1\}$ eine Belegung mit $v(C_1 \wedge \ldots \wedge C_m) = 1$. Für alle $i \leq m$ gilt dann $v(C_i) = 1$, d.h. für alle $i \leq m$ gibt es ein k_i mit $v(y_{ik_i}) = 1$.

Folgende Abbildung ϕ ist dann eine Färbung von G:

$$\phi(0) = f_0,$$

$$\phi(2) = f_2,$$

$$\phi(x_j) = f_{v(x_j)},$$

$$\phi(\bar{x}_j) = f_{v(\bar{x}_j)},$$

und die Punkte der Fünfecke $(p_1^i, p_2^i, p_3^i, p_4^i, p_5^i)$ färbt man der Reihe nach, für $k_i = 1$ im Gegenuhrzeigersinn, sonst im Uhrzeigersinn. Dabei beginnt man mit $\phi(p^i_{k_i}) = f_o$. Nachher sind jeweils höchstens zwei Farben ausgeschlossen, so dass stets eine freie Farbe gewählt werden kann.

Sei umgekehrt G mit drei Farben f_o, f_1, f_2 gefärbt, und etwa $\phi(0) = f_o$, $\phi(2) = f_2$. Für $j \leq n$ ist $\phi(x_j) = f_o$ und $\phi(\bar{x}_j) = f_1$ oder umgekehrt.

Wir definieren $v: \{x_1, \ldots, x_n\} \to \{0,1\}$ durch

$$x_j \to \begin{cases} 0 & \text{falls } \phi(x_j) = f_o \\ 1 & \text{falls } \phi(x_j) = f_1. \end{cases}$$

Wir zeigen, dass $v(C_1 \wedge \ldots \wedge C_m) = 1$ gilt:

Andernfalls gibt es ein $C_i = y_{i1} \vee y_{i2} \vee y_{i3}$ mit $v(C_i) = 0$, d.h. $v(y_{i1}) = v(y_{i2}) = v(y_{i3}) = 0$. Dann ist

$$\phi(y_{i1}) = \phi(y_{i2}) = \phi(y_{i3}) = f_o \text{ und o.B.d.A.}$$
$$\phi(p_1^i) = f_1,\ \phi(p_2^i) = f_2,$$
$$\text{also} \quad \phi(p_4^i) = f_2,\ \phi(p_5^i) = f_1.$$

p_3^i ist mit Punkten der Farben f_o, f_1, f_2 verbunden, was der Färbungseigenschaft widerspricht. Also gilt

$$v(C_1 \wedge \ldots \wedge C_m) = 1.$$

2. Die Sprache k-FAERBBARKEIT besteht aus allen Graphen G = (P,K) mit der Eigenschaft, dass es eine Abbildung $\phi: P \to \{f_1, \ldots, f_k\}$ gibt mit

$$(\forall p,q \in P)\ \{p,q\} \in K \Longrightarrow \phi(p) \neq \phi(q),$$

d.h. dass der Graph mit k Farben färbbar ist. k-FAERBBARKEIT ist vollständig für $k \geq 3$:

$$\text{DREIFAERBBARKEIT} \leq_\pi \text{k-FAERBBARKEIT}.$$

Einem Graphen G = (P,K) ordnen wir den Graphen G' = (P',K') zu mit

$$P' = P \cup \{1, \ldots, k-3\}$$

$$K' = K \cup \{\{i,j\} \mid i,j \leq k-3\} \cup \{\{p,j\} \mid p \in P, j \leq k-3\}.$$

Offensichtlich ist $G \in$ DREIFAERBBARKEIT, genau wenn $G' \in$ k-FAERBBARKEIT.

Bemerkung ZWEIFAERBBARKEIT ist in P. Der folgende Algorithmus testet, ob ein Graph G = (P,K) zweifärbbar ist.

Man wählt $r \in P$, ordnet ihm die Farbe $\phi(r)=f_1$ zu und bestimmt schrittweise für die Punkte p, die mit einem bereits gefärbten Punkt q verbunden sind, $\phi(p)$ durch $\phi(p) \neq \phi(q)$. Wenn p mit Punkten verschiedener Farbe verbunden ist, so wird G verworfen. Falls nur noch Punkte ungefärbt sind, die mit keinem gefärbten Punkt verbunden sind, so beginnt man wieder wie oben mit einem beliebigen solchen Punkt r und der Farbe f_1. Dann ist G zweifärbbar, genau wenn dieses Verfahren niemals verwirft.

3. Die Sprache CLIQUENUEBERDECKUNG enthält alle Paare (G,n), wo $G = (P,K)$ ein Graph und $n \in \mathbb{N}$ ist, mit der Eigenschaft, dass es vollständige Untergraphen (= Cliquen) $G_1,\ldots,G_n$ von G gibt, deren Punktmengen P überdecken (die G_j dürfen auch leer sein). CLIQUENUEBERDECKUNG ist vollständig:

$$\text{DREIFAERBBARKEIT} \leq_\pi \text{CLIQUENUEBERDECKUNG}.$$

Einem Graphen $G = (P,K)$ ordnen wir den komplementären Graphen $G' = (P',K')$ mit $P' = P$ und $K' = \binom{P}{2} \setminus K$ und $n=3$ zu. Dann gilt

$G \in$ DREIFAERBBARKEIT

$\Longleftrightarrow$ $(\exists \phi\colon P \to \{1,2,3\})$ $(\forall \{p,q\} \in K)\ \phi(p) \neq \phi(q)$

$\Longleftrightarrow$ $\exists$Ueberdeckung $P_1 \cup P_2 \cup P_3$ von P, so dass für $i \in \{1,2,3\}$ je zwei Punkte von P_i in G nicht miteinander verbunden sind

$\Longleftrightarrow$ $\exists$Ueberdeckung $P_1 \cup P_2 \cup P_3$ von P mit $(\forall i \leq 3)$ $(\forall p,q \in P_i)$ $\{p,q\} \in K'$

$\Longleftrightarrow$ $(G',3) \in$ CLIQUENUEBERDECKUNG.

4. PARTITION besteht aus allen Paaren $(M,\{S_1,\ldots,S_r\})$, wobei M eine endliche Menge ist und die S_j Teilmengen von M sind, mit der Eigenschaft, dass es eine Teilfamilie $\{S_{i_1},\ldots,S_{i_\rho}\}$ von $\{S_1,\ldots,S_r\}$ gibt, deren Elemente paarweise disjunkt sind und deren Vereinigung M ist. Als Kodierung verwenden wir die Kodierung der $|M| \times r$-Inzidenzmatrix, d.h. der Matrix mit den Koeffizienten

$$a_{ij} = \begin{cases} 1 & m_i \in S_j \\ 0 & \text{sonst} \end{cases}$$

wobei $M = \{m_1,\ldots,m_{|M|}\}$.

PARTITION ist vollständig:

$$\text{DREIFAERBBARKEIT} \leq_\pi \text{PARTITION}.$$

Einem Graphen $G = (P,K)$ ordnen wir zu:

$$M = P \cup K\times\{1,2,3\}$$

und folgende Mengen S_j, indiziert durch $(P\times\{1,2,3\}) \cup (K\times\{1,2,3\})$:

$$S_{p,f} = \{p\} \cup \{(k,f) \mid p \in k\},$$

$$S_{k,f} = \{(k,f)\}.$$

Sei $(P,K) \in$ DREIFAERBBARKEIT, etwa mit $\phi: P \to \{1,2,3\}$ gefärbt. Dann bilden die Mengen

$$\{S_{p,\phi(p)} \mid p \in P\} \cup \{S_{k,f} \mid (\forall p \in k)\phi(p) \neq f\}$$

eine Ueberdeckung von M, und sie sind paarweise disjunkt. Also ist $(M,\{S_j\}) \in$ PARTITION. Sei umgekehrt $(M,\{S_j\}) \in$ PARTITION, etwa

$$M = \bigcup_{j\in J} S_j \text{ mit } J \subset (P\times\{1,2,3\}) \cup (K\times\{1,2,3\}).$$

Für jedes $p \in P$ gibt es genau ein $f \in \{1,2,3\}$ mit $(p,f) \in J$. Dann ist

$$\phi: P \to \{1,2,3\}$$

$$p \mapsto f$$

eine Färbung von (P,K), also $G \in$ DREIFAERBBARKEIT.

5. Die Sprache SCHNITTMENGE besteht aus allen Paaren $(N,\{U_1,\ldots,U_t\})$, wo N eine endliche Menge und $U_1,\ldots,U_t$ Teilmengen von N sind, mit der Eigenschaft, dass es eine Teilmenge U von N gibt mit $\forall_j |U_j \cap U| = 1$. Ihre Vollständigkeit zeigen wir durch eine polynomiale Transformation des "dualen" Problems:

$$\text{PARTITION} \leq_\pi \text{SCHNITTMENGE}.$$

Sei $\{S_1,\ldots,S_r\}$ eine Familie von Teilmengen von $M = \{u_1,\ldots,u_t\}$. Wir ordnen ihr zu eine Familie $U_1,\ldots,U_t$ von Teilmengen von $N = \{s_1,\ldots,s_r\}$ mit

$$s_j \in U_i \iff u_i \in S_j \text{ (transponierte } \in\text{-Matrix)}.$$

Dann gilt:

$$(M,\{S_1,\ldots,S_r\}) \in \text{PARTITION}$$
$$\Longleftrightarrow (\exists R \subset \{1,\ldots,r\})\ (\forall i \leq t)\ (\exists\,!\, j \in R)\ u_i \in S_j$$
$$\Longleftrightarrow (\exists R \subset \{1,\ldots,r\})\ (\forall i \leq t)\ (\exists\,!\, j \in R)\ s_j \in U_i$$
$$\Longleftrightarrow (N,\{U_1,\ldots,U_t\}) \in \text{SCHNITTMENGE}.$$

6. Die Sprache DREIDIMENSIONALES REPRAESENTANTENSYSTEM besteht aus allen Paaren von endlichen Mengen (T,U) mit $U \subset T^3$ und mit der Eigenschaft, dass es eine Teilmenge $W \subset U$ gibt, so dass die drei Projektionen $pr_i: T^3 \to T$ $(i \in \{1,2,3\})$ bijektiv von W nach T sind.
Lawler (siehe Karp 1972) hat mit der folgenden Transformation gezeigt, dass diese Sprache vollständig ist:

$$\text{PARTITION} \leq_\pi \text{DREIDIMENSIONALES REPRAESENTANTENSYSTEM}.$$

Dabei wird jedem $(M,\{S_1,\ldots,S_r\})$ das folgende (T,U) zugeordnet:

$$T = M \cup \{(x,j) \mid j \in \{1,\ldots,r\}, x \in S_j\}.$$

Sei $\pi: T \to T$ eine feste Permutation, so dass für alle $j \in \{1,\ldots,r\}$ und alle $\beta \in S_j \times \{j\}$

$$\{\pi^i(\beta) \mid i \geq 0\} = S_j \times \{j\}$$

ist (d.h. π ist Zyklus auf $S_j \times \{j\}$).

$$U = \{(x,(x,j),(x,j)) \mid j \in \{1,\ldots,r\}, x \in S_j\}$$
$$\cup\ \{(\alpha,\beta,\pi(\beta)) \mid \alpha \in T \setminus M, \beta \in T\}.$$

Wenn $R \subset \{1,\ldots,r\}$ eine Partition von M definiert, so sei $T' = \bigcup_{j \in R} (S_j \times \{j\})$. Da $|T'| = |M|$ ist, gibt es eine Bijektion

$$\varphi : T \setminus M \to T \setminus T'.$$

Dann ist

$$W = \{(x,(x,j),(x,j)) \mid (x,j) \in T'\} \cup \{(\alpha,\varphi(\alpha),\pi(\varphi(\alpha))) \mid \alpha \in T \setminus M\}$$

ein dreidimensionales Repräsentantensystem.
(pr_3 ist bijektiv, da $\pi: T \setminus T' \to T \setminus T'$ bijektiv ist).

Sei umgekehrt W ein dreidimensionales Repräsentantensystem und $R = \{j \mid (\exists x \in M)\ (x,(x,j),(x,j)) \in W\}$. Wegen $pr_1(W) = T$ ist $\bigcup_{j \in R} S_j = M$.
Sei $j \in R$ und etwa $(x,(x,j),(x,j)) \in W$. Sei ferner $(y,j) = \pi^{-1}(x,j)$. Es gibt kein $\alpha \in T \setminus M$ mit

$$(\alpha,(y,j),\pi(y,j)) \in W,$$

also ist

$$(y,(y,j),(y,j)) \in W.$$

Da π^{-1} ein Zyklus auf $S_j \times \{j\}$ ist, folgt

$$(\forall z \in S_j)\ (z,(z,j),(z,j)) \in W.$$

Wenn also $i,j \in R$ und $x \in S_i \cap S_j$ ist, so ist $(x,(x,i),(x,i)) \in W$ und $(x,(x,j),(x,j)) \in W$, also $i=j$, und folglich definiert R eine Partition von M.

7. Die Sprache RUCKSACK besteht aus allen Folgen $(a_1,\ldots,a_r,b)$ von natürlichen Zahlen mit der Eigenschaft, dass es ein $R \subset \{1,\ldots,r\}$ gibt mit $\sum_{j \in R} a_j = b$ (man möchte den Rucksack b mit einem Teil des Proviants $a_1,\ldots,a_r$ genau ausfüllen). Diese Sprache ist vollständig:

$$\text{PARTITION} \leq_\pi \text{RUCKSACK}.$$

Seien $S_1,\ldots,S_r$ Teilmengen von $M = \{u_1,\ldots,u_t\}$. Wir setzen

$$d=r+1,\ \varepsilon_{ji} = \begin{cases} 1 & \text{falls } u_i \in S_j \\ 0 & \text{sonst} \end{cases}$$

$$a_j = \sum_{i=1}^{t} \varepsilon_{ji} d^{i-1},\ b = \frac{d^t-1}{d-1}.$$

Dann gilt:

$$(M,\{S_1,\ldots,S_r\}) \in \text{PARTITION}$$

$$\Longleftrightarrow (\exists R \subset \{1,\ldots,r\})\ (\forall i \leq t)\ (\exists!\ j \in R)\ u_i \in S_j$$

$$\Longleftrightarrow (\exists R \subset \{1,\ldots,r\}) \sum_{i=1}^{t} \Big(\sum_{j \in R} \varepsilon_{ji}\Big) d^{i-1} = 1+\ldots+d^{t-1} = b$$

(da $(\forall i)\ \sum_{j \in R} \varepsilon_{ji} \leq \sum_{j \leq r} \varepsilon_{ji} \leq r < d$ und die d-adische Darstellung eindeutig ist)

$$\Longleftrightarrow (\exists R \subset \{1,\ldots,r\}) \sum_{j \in R} a_j = \sum_{j \in R} \Big(\sum_{i=1}^{t} \varepsilon_{ji} d^{i-1}\Big) = b$$

$$\Longleftrightarrow (a_1,\ldots,a_r,b) \in \text{RUCKSACK}.$$

8. Das multiplikative Analogon zu RUCKSACK ist FAKTORZERLEGUNG, das aus allen Folgen $(a_1,\ldots,a_r,b)$ von natürlichen Zahlen besteht, die die Eigenschaft haben, dass es eine Teilfolge $(a_{i_1},\ldots,a_{i_\rho})$ von $(a_1,\ldots,a_r)$ gibt mit $\prod_1^\rho a_{i_k} = b$. FAKTORZERLEGUNG ist vollständig:

PARTITION $\leq_\pi$ FAKTORZERLEGUNG.

Seien $S_1,\ldots,S_r$ Teilmengen von $M = \{u_1,\ldots,u_t\}$. Wir konstruieren paarweise teilerfremde Zahlen $p_1,\ldots,p_t$, z.B. die ersten t Primzahlen. Man überlegt sich leicht, dass dies in einer Zeit geht, die polynomial in t ist. Wir setzen

$$a_i = \prod_{\{j \mid u_j \in S_i\}} p_j \quad \text{für } i = 1,\ldots,t,$$

$$b = \prod_{1}^{t} p_j.$$

Dann gilt:

$$\begin{aligned}
&(M,\{S_1,\ldots,S_r\}) \in \text{PARTITION} \\
\Longleftrightarrow\ &(\exists R \subset \{1,\ldots,r\})\ (\forall j \leq t)\ (\exists\, !\, i \in R)\ u_j \in S_i \\
\Longleftrightarrow\ &(\exists R \subset \{1,\ldots,r\})\ (\forall j \leq t)\ (\exists\, !\, i \in R)\ p_j \mid a_i \\
\Longleftrightarrow\ &(\exists R \subset \{1,\ldots,r\})\ \prod_{1}^{t} p_j = \prod_{i \in R} a_i \\
\Longleftrightarrow\ &(a_1,\ldots,a_r,b) \in \text{FAKTORZERLEGUNG}.
\end{aligned}$$

9. Die Sprache HALBIEREN besteht aus allen Folgen $(c_1,\ldots,c_s)$ von ganzen Zahlen, die die Eigenschaft haben, dass es ein $S \subset \{1,\ldots,s\}$ gibt mit $\sum_{i \in S} c_i = \sum_{i \notin S} c_i$.

HALBIEREN ist vollständig:

RUCKSACK $\leq_\pi$ HALBIEREN.

Einer Folge $(a_1,\ldots,a_r,b)$ ordnen wir zu:

$$s = r+2$$

$$c_i = a_i \text{ für } i=1,\ldots,r$$

$$c_{r+1} = b+1$$

$$c_{r+2} = \Big(\sum_{i=1}^{r} a_i\Big) + 1 - b$$

Dann gilt:

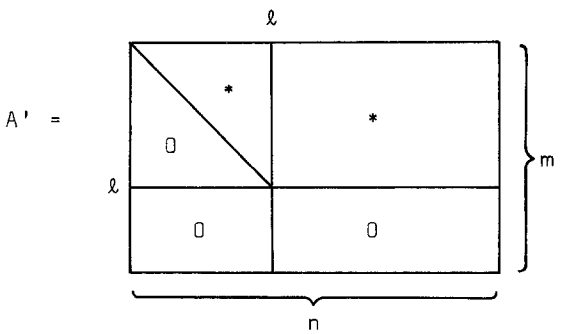
$$\begin{aligned}
&(a_1,\ldots,a_r,b) \in \text{RUCKSACK} \\
\Longleftrightarrow\ &(\exists R \subset \{1,\ldots,r\}) \sum_{i \in R} a_i = b \\
\Longleftrightarrow\ &(\exists R \subset \{1,\ldots,r\}) \sum_{i \in R} a_i + c_{r+2} = \sum_{i \notin R} a_i + c_{r+1}
\end{aligned}$$

$$\Longleftrightarrow \quad (c_1,\ldots,c_{r+2}) \in \text{HALBIEREN}$$

(da $\sum_{i=1}^{r} c_i < c_{r+1} + c_{r+2}$ ist, kommen in einer Halbierung c_{r+1} und c_{r+2} nicht auf der gleichen Seite vor).

10. In diesem und den nächsten beiden Abschnitten betrachten wir lineare Gleichungssysteme in $\mathbb{Q}$, in $\mathbb{Z}$ und in $\mathbb{Z}/q\mathbb{Z}$ für ein $q \in \mathbb{Z}$. Wir wollen die Lösbarkeit solcher Systeme entscheiden und gegebenenfalls Lösungen berechnen.
In $\mathbb{Q}$ verwendet man gewöhnlich die Gauss-Elimination, in $\mathbb{Z}$ die auf die Elementarteilertheorie führende Elimination mit Hilfe des euklidschen Algorithmus. Systeme von linearen Kongruenzen kann man durch Einführen von Schlupfvariablen auf lineare diophantische Gleichungssysteme zurückführen.
Die Anzahl arithmetischer Operationen dieser Algorithmen ist polynomial in der Inputlänge. Dagegen ist nicht von vornherein klar, ob die bei den Berechnungen auftretenden Zahlen klein genug sind. Dass dies für eine modifizierte Gauss-Elimination doch der Fall ist, hat (Edmonds 1967) gezeigt. Diese Schlussweise lässt sich nicht ohne weiteres auf den diophantischen Fall übertragen. Wir gehen deshalb nach einem Vorschlag von V. Strassen so vor, dass wir das lineare diophantische System durch ein äquivalentes Kongruenzsystem ersetzen und auf dieses die Elementarteilermethode anwenden. Hier kann man das Koeffizientenwachstum unter Kontrolle halten, indem man nach jedem Rechenschritt reduziert.

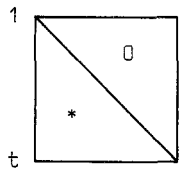
Satz Es gibt eine polynomial beschränkte TM, welche für jedes Paar (A,b) aus einer ganzzahligen m×n-Matrix A und einem ganzzahligen m-Vektor b ein ebensolches Paar (A',b') und eine Permutation π der Koordinaten in $\mathbb{Q}^n$ berechnet, so dass



die Diagonalelemente bis zur ℓ-ten Zeile $\neq 0$ sind und für alle $x \in \mathbb{Q}^n$ gilt:

$$Ax = b \iff A'(\pi x) = b'.$$

Für späteren Gebrauch (12.) bemerken wir, dass ausserdem gilt: Wenn A links oben ein t×t-Kästchen mit Dreiecksform



und lauter Elementen $\neq 0$ in der Diagonale hat, so auch A' (d.h. A' hat ein t×t-Kästchen in Diagonalform).

Korollar 1 Es gibt eine polynomial beschränkte TM, die für jedes Paar (A,b) aus einer ganzzahligen m×n-Matrix A und einem ganzzahligen m-Vektor b

(i) entscheidet, ob ein $x \in \mathbb{Q}^n$ mit $Ax = b$ existiert, und, falls die Entscheidung positiv ausfällt, ein solches x konstruiert,

(ii) eine Basis über $\mathbb{Q}$ aus ganzzahligen Vektoren des Nullraumes $\{x \in \mathbb{Q}^n \mid Ax=0\}$ berechnet.

Beweis Nach obigem Satz kann angenommen werden, dass A die dort für A' angegebene Form hat. Dann gilt:

$$((\exists x \in \mathbb{Q}^n)\ Ax=b) \iff ((\forall j, \ell+1 \leq j \leq m)\ b_j = 0)$$

Falls es eine Lösung von $Ax = b$ gibt, erhält man eine solche vermöge

$$x_r = \begin{cases} 0 & (\ell+1 \leq r \leq n) \\ (a_{rr})^{-1} \left(b_r - \sum_{j=r+1}^{n} a_{rj} x_j \right) & (1 \leq r \leq \ell) \end{cases}$$

Eine Basis $x^{(1)}, \ldots, x^{(n-\ell)}$ des Nullraumes von A erhält man mit

$$x_r^{(i)} = \begin{cases} \prod_{j \leq \ell} a_{jj} & \text{falls } r = \ell+i \\ 0 & \text{falls } r \neq \ell+i \text{ und } \ell+1 \leq r \leq n \\ -\frac{1}{a_{rr}} \cdot \sum_{r+1 \leq j \leq n} a_{rj}\, x_j^{(i)} & \text{falls } 1 \leq r \leq \ell \end{cases}$$

Man prüft leicht nach, dass $\sum_{r+1\leq j\leq n} a_{rj}x_j^{(i)}$ stets ganzzahliges Vielfaches von $\prod_{i\leq j\leq r} a_{jj}$ ist, also $x^{(1)},\ldots,x^{(n-\ell)}$ ganzzahlige Koordinaten haben.

Die Sprache LINEARE RATIONALE GLEICHUNGEN besteht aus allen Paaren (A,b) aus einer ganzzahligen m×n-Matrix A und einem ganzzahligen m-Vektor b mit der Eigenschaft, dass ein $x\in\mathbb{Q}^n$ existiert mit Ax = b (eigentlich sollte diese Sprache LOESBARE LINEARE RATIONALE GLEICHUNGS-SYSTEME heissen, aber hier und in den folgenden Abschnitten verwenden wir die obige kürzere Bezeichnungsweise).

Korollar 2 LINEARE RATIONALE GLEICHUNGEN ist in P.

Beweis des Satzes Der folgende Gauss-Algorithmus berechnet rekursiv eine Folge $A^{(o)}, A^{(1)},\ldots,A^{(\ell)}$ von m×(n+1)-Matrizen aus rationalen Zahlen sowie eine Folge $\pi^{(o)},\pi^{(1)},\ldots,\pi^{(\ell)}$ von Permutationen der Koordinaten in $\mathbb{Q}^n$. Zunächst ist

$$a_{ij}^{(o)} = \begin{cases} a_{ij} & (1\leq j\leq n) \\ b_i & (j=n+1) \end{cases}$$

$$\pi^{(o)} = id$$

$A^{(k)}$ und $\pi^{(k)}$ erhält man, indem man

(1) in $A^{(k-1)}$ die r-te und k-te Zeile und die s-te und k-te Spalte vertauscht, wobei (r,s) das lexikographisch kleinste Paar mit $a_{rs}^{(k-1)} \neq 0$, $k\leq r,s$ und $s\leq n$ ist (falls kein solches existiert, ist $\ell=k-1$)

(2) sodann für jedes $i\geq k+1$ dasjenige Vielfache der k-ten Zeile zu der i-ten addiert, für welches eine Null an der Stelle (i,k) entsteht

(3) $\pi^{(k)} = (ks)\circ\pi^{(k-1)}$

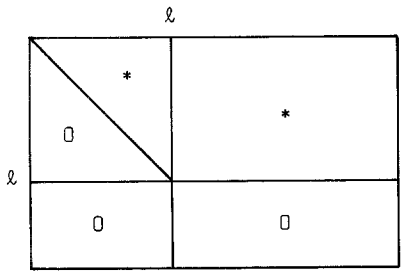
Dann gilt

$$(\forall x\in\mathbb{Q}^n)\ (\sum_{1\leq j\leq n} a_{ij}^{(k-1)}(\pi^{(k-1)}(x))_j = a_{i,n+1}^{(k-1)} \quad (1\leq i\leq m)$$

$$\Longleftrightarrow \sum_{1\leq j\leq n} a_{ij}^{(k)}(\pi^{(k)}(x))_j = a_{i,n+1}^{(k)} \quad (1\leq i\leq m))$$

und ausserdem

$$(A^{(\ell)})_{1\le i\le m,\ 1\le j\le n} =$$



Wir multiplizieren noch die Zeilen von $A^{(\ell)}$ mit einer geeigneten ganzen Zahl, derart, dass alle Einträge ganzzahlig werden. So erhalten wir das gesuchte Paar (A',b'). Die zusätzliche Behauptung über das Dreieckskästchen ist klar.

Im Folgenden zeigen wir, dass es $\tilde{a}_{ij}^{(k)}$, $\tilde{a}^{(k)} \in \mathbb{Z}$ gibt mit

$$a_{ij}^{(k)} = \tilde{a}_{ij}^{(k)} / \tilde{a}^{(k)},$$

derart dass wir die Länge der Binärdarstellungen der $\tilde{a}_{ij}^{(k)}$, $\tilde{a}^{(k)}$ geeignet abschätzen können, d.h. durch ein Polynom in der Länge der Darstellung von (A,b). Wenn wir die auftretenden rationalen Zahlen stets in gekürzter Form schreiben, ist damit gezeigt, dass die Längen der im Algorithmus vorkommenden Zahlen beschränkt sind, und dass also der Algorithmus in polynomialer Zeit ausführbar ist.
Wir können o.B.d.A. annehmen, dass in (1) stets (r,s) = (k,k) ist. Dann gilt

$$a_{ij}^{(k)} = \frac{1}{a_{kk}^{(k-1)}} \begin{vmatrix} a_{kk}^{(k-1)} & a_{kj}^{(k-1)} \\ a_{ik}^{(k-1)} & a_{ij}^{(k-1)} \end{vmatrix} \qquad (i,j \ge k+1)$$

Wir definieren nach (Edmonds 1967) $\tilde{a}_{ij}^{(k)}$ rekursiv durch folgende Gleichungen:

$$\tilde{a}_{ij}^{(o)} = a_{ij}^{(o)}$$

$$\tilde{a}_{ij}^{(k)} = \frac{1}{\tilde{a}_{k-1,k-1}^{(k-2)}} \begin{vmatrix} \tilde{a}_{kk}^{(k-1)} & \tilde{a}_{kj}^{(k-1)} \\ \tilde{a}_{ik}^{(k-1)} & \tilde{a}_{ij}^{(k-1)} \end{vmatrix} \qquad (i,j \ge k+1)$$

Man sieht mit Induktion nach k, dass

$$a_{ij}^{(k)} = \tilde{a}_{ij}^{(k)} (\tilde{a}_{kk}^{(k-1)})^{-1} \qquad (i,j \ge k+1)$$

Es gilt folgende Beziehung nach (Edmonds 1967), siehe auch (Bareiss 1968):

$$\tilde{a}_{ij}^{(k)} = \begin{vmatrix} a_{11}^{(o)} & a_{12}^{(o)} & \cdots & a_{1k}^{(o)} & a_{1j}^{(o)} \\ a_{21}^{(o)} & a_{22}^{(o)} & \cdots & a_{2k}^{(o)} & a_{2j}^{(o)} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{k1}^{(o)} & a_{k2}^{(o)} & \cdots & a_{kk}^{(o)} & a_{kj}^{(o)} \\ a_{i1}^{(o)} & a_{i2}^{(o)} & \cdots & a_{ik}^{(o)} & a_{ij}^{(o)} \end{vmatrix} \quad (i,j \geq k+1)$$

denn hieraus folgt

$$|\tilde{a}_{ij}^{(k)}| \leq n! \ (\max_{i,j}\{|a_{ij}^{(o)}|\})^n.$$

Diese Abschätzung gilt auch, wenn nicht $i,j \geq k+1$ ist.
Die binäre Länge von $\tilde{a}_{ij}^{(k)}$ ist also

$$\leq n(\log n + \max_{i,j}\{\log |a_{ij}^{(o)}|\}).$$

Damit ist der Satz bewiesen.

11. Satz Es gibt eine polynomial beschränkte TM, welche für jedes Tripel (A,b,q) aus einer ganzzahligen m×n-Matrix A, einem ganzzahligen m-Vektor b und einem $q \in \mathbb{N}$

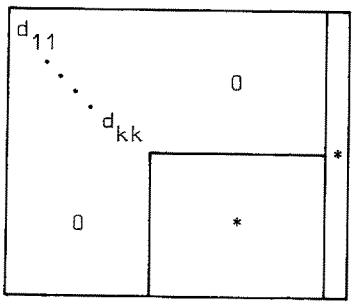
(i) entscheidet, ob ein $x \in \mathbb{Z}^n$ mit $Ax \equiv b \bmod q$ existiert, und, falls die Entscheidung positiv ausfällt, ein solches x berechnet,

(ii) eine Basis über $\mathbb{Z}$ von $\{x \in \mathbb{Z}^n \mid Ax \equiv 0 \bmod q\}$ berechnet.

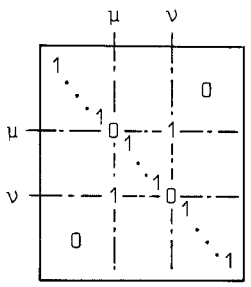
Die Sprache LINEARE KONGRUENZEN besteht aus allen Tripeln (A,b,q) aus einer ganzzahligen m×n-Matrix A, einem ganzzahligen m-Vektor b und einem $q \in \mathbb{N}$ mit der Eigenschaft, dass es ein $x \in \mathbb{Z}^n$ gibt mit $Ax \equiv b \bmod q$

Korollar LINEARE KONGRUENZEN ist in P.

Beweis des Satzes Eine m×(n+1)-Matrix D der Form



mit $d_{11},\ldots,d_{kk} \neq 0$ heisse k-Diagonalmatrix. Mit $S(\mu,\nu)$ bezeichnen wir die n×n-Matrix



Wenn man aus einer m×n-Matrix A durch Vertauschen der μ-ten und ν-ten Spalte eine Matrix A' erhält, so ist $A \cdot S(\mu,\nu) = A'$.

Sei D eine m×(n+1)-Matrix mit $d_{kk} \not\equiv 0$ modq, die (k-1)-Diagonalmatrix, aber nicht k-Diagonalmatrix ist. Dann bezeichnen wir mit (*) die folgende Operation, die wieder eine m×(n+1)-Matrix D' liefert mit $d'_{kk} \not\equiv 0$ modq und so, dass D' eine (k-1)-Diagonalmatrix ist.

(*): Falls es ein j gibt mit $k+1 \leq j \leq n$ und $d_{kj} \neq 0$, so sei s die kleinste solche Zahl, und sei $\alpha = d_{ks}/d_{kk}$. Subtrahiere das $\lfloor \alpha \rfloor$-fache der k-ten Spalte von der s-ten Spalte und reduziere alle Zahlen modq. Wenn $\lfloor \alpha \rfloor \neq \alpha$ ist, so vertausche die k-te und s-te Spalte.

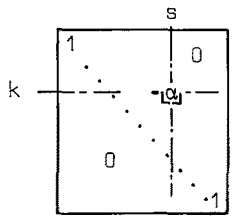
Falls es kein solches j gibt, so sei r die kleinste Zahl $\geq k+1$ mit $d_{rk} \neq 0$, und sei $\beta = d_{rk}/d_{kk}$. Subtrahiere das $\lfloor \beta \rfloor$-fache der k-ten Zeile von der r-ten Zeile und reduziere alle Zahlen modq. Wenn $\lfloor \beta \rfloor \neq \beta$ ist, so vertausche die k-te und r-te Zeile.

Der folgende Algorithmus berechnet zu (A,b) Folgen $A^{(o)},\ldots,A^{(\ell)}$ sowie $T^{(o)},\ldots,T^{(\ell)}$, wobei für $0 \leq k \leq \ell$ $A^{(k)}$ eine k-Diagonalmatrix und $T^{(k)}$ eine n×n-Matrix mit Determinante 1 ist (alle zu betrachtenden Matrizen haben ganzzahlige Koeffizienten).

Indem man in der m×(n+1)-Matrix (A,b) alle Elemente modq reduziert, erhält man $A^{(o)}$, und $T^{(o)} = I_n$.

Seien $A^{(k-1)}$ und $T^{(k-1)}$ bereits berechnet. Falls es kein (i,j) mit $a_{ij}^{(k-1)} \neq 0$, $k \leq i \leq m$, $k \leq j \leq n$ gibt, so ist $\ell = k-1$. Andernfalls sei (u,v) das lexikographisch kleinste solche Paar, und $\tilde{A}$ entstehe aus $A^{(k-1)}$ durch Vertauschen der k-ten und u-ten Zeile sowie der k-ten und v-ten Spalte. Die Operation (*) wird, beginnend mit $\tilde{A}$, so oft hintereinander ausgeführt, bis eine k-Diagonalmatrix entsteht. $A^{(k)}$ ist diese Matrix. $T^{(k)}$

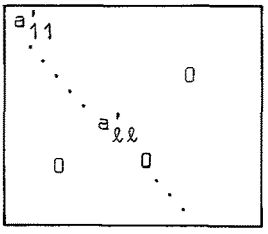
wird erhalten, indem man $T^{(k-1)}$ nacheinander von rechts multipliziert mit S(k,v), sowie für jede Anwendung des ersten Falles von (*) mit



und ausserdem mit S(k,s), falls $\alpha_j \neq \alpha$ ist ($T^{(k)}$ wird nicht modq reduziert).

Wie man leicht sieht, ist nach O(m+n) Anwendungen von (*) das Element an der Stelle (k,k) um mindestens die Hälfte verringert. Hieraus folgt, dass (*) nur polynomial oft angewandt werden muss. Ebenso sieht man, dass für alle k die Länge der Binärdarstellung von $T^{(k)}$ polynomial in der Inputlänge ist.

Wir bezeichnen mit A' die m×n-Untermatrix $(a_{ij}^{(\ell)})_{1\leq j\leq n}$ von $A^{(\ell)}$, und mit b' die (n+1)-te Spalte von $A^{(\ell)}$. Dann ist A' eine Diagonalmatrix der Form



mit $a'_{11},\ldots,a'_{\ell\ell} \not\equiv 0$ modq, und es gilt

$$(\forall x\in \mathbb{Z}^n)\ (AT^{(\ell)}x \equiv b \text{ modq} \iff A'x \equiv b' \text{modq})$$

$$\text{und } (AT^{(\ell)}x \equiv 0 \text{ modq} \iff A'x \equiv 0 \text{ modq}).$$

Hieraus folgt

$$((\exists x\in \mathbb{Z}^n)Ax \equiv b \text{ modq}) \iff ((\forall i, 1\leq i\leq m)\, ggT(a'_{ii},q) \mid b'_i).$$

Falls diese Bedingung erfüllt ist, so berechne mit Hilfe des euklidschen Algorithmus $y_1,\ldots,y_\ell$ mit $y_i a'_{ii} \equiv ggT(a'_{ii},q) \text{modq}$. Sei

$$z_i = y_i b'_i / ggT(a'_{ii},q) \quad (1\leq i\leq \ell)$$

$$x = T^{(\ell)}(z_1,\ldots,z_\ell,0,\ldots,0)^t$$

Dann ist

$$Ax \equiv b \bmod q.$$

Wenn $e_1,\ldots,e_n \in \mathbb{Z}^n$ die Einheitsvektoren sind, so ist

$$\{T^{(\ell)}(q/ggT(a'_{11},q)\cdot e_1),\ldots,T^{(\ell)}(q/ggT(a'_{\ell\ell},q)\cdot e_\ell),T^{(\ell)}e_{\ell+1},\ldots,T^{(\ell)}e_n\}$$

eine Basis über $\mathbb{Z}$ von

$$\{x\in \mathbb{Z}^n \mid Ax \equiv 0 \bmod q\}.$$

12. Satz Es gibt eine polynomial beschränkte TM, die für jedes Paar (A,b) aus einer ganzzahligen m×n-Matrix A und einem ganzzahligen m-Vektor b

(i) entscheidet, ob ein $x\in \mathbb{Z}^n$ mit $Ax = b$ existiert, und, falls die Entscheidung positiv ausfällt, ein solches x berechnet,

(ii) eine Basis von $\{x\in \mathbb{Z}^n \mid Ax=0\}$ berechnet.

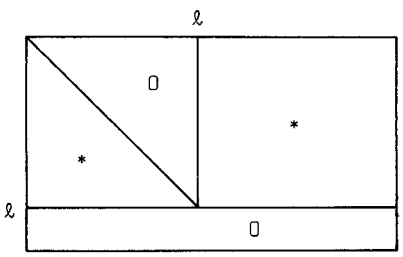
Die Sprache LINEARE DIOPHANTISCHE GLEICHUNGEN besteht aus allen Paaren (A,b), A,b wie oben, mit der Eigenschaft, dass es ein $x\in \mathbb{Z}^n$ gibt mit $Ax = b$.

Korollar LINEARE DIOPHANTISCHE GLEICHUNGEN ist in P.

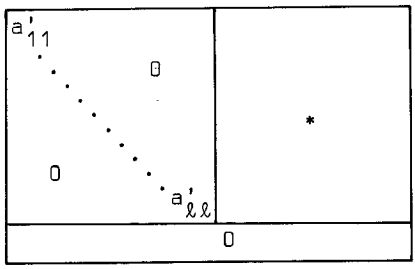
Beweis des Satzes Nach dem Satz aus 10. können wir annehmen, dass A die dort für A' beschriebene Form hat. Für $k = 1,\ldots,\lfloor\frac{\ell}{2}\rfloor$ wird nun vertauscht:

1. die k-te Zeile mit der $(\ell-k+1)$-ten Zeile
2. die k-te Spalte mit der $(\ell-k+1)$-ten Spalte

Die so entstehende Matrix hat die Form



und wir können auf sie wiederum den Satz von 10. anwenden. So erhalten wir eine Matrix

$A' =$ 

mit $a'_{11},\ldots,a'_{\ell\ell} \neq 0$ sowie einen Vektor b', und es genügt, für (A',b') die Behauptung zu beweisen.

Sei $q = \prod_{1\leq i\leq \ell} a'_{ii}$, $q_i = q/a'_{ii}$. Wir multiplizieren für $1\leq i\leq \ell$ die i-te Zeile von (A',b') mit q_i. Sei (A'',b'') das so erhaltene Paar, $\tilde{A}$ die rechte obere $\ell\times(n-\ell)$-Teilmatrix $(a''_{ij})_{\substack{1\leq i\leq \ell \\ \ell+1\leq j\leq n}}$, $\tilde{b} = (b''_1,\ldots,b''_\ell)^t$ und $p: \mathbb{Z}^n \to \mathbb{Z}^{n-\ell}$ die Projektion auf die letzten $n-\ell$ Koordinaten. Dann ist $a''_{ii} = q (1\leq i\leq \ell)$, und für alle $x\in \mathbb{Z}^n$ gilt

(*)
$$A'x = b' \iff A''x = b'' \iff$$
$$(\tilde{A}p(x) \equiv \tilde{b} \bmod q \;\&\; (\forall i, \ell+1\leq i\leq m)\; b'_i = 0)$$

Nach dem Satz von 11. gibt es eine polynomial beschränkte TM, die entscheidet, ob ein $x\in \mathbb{Z}^{n-\ell}$ existiert mit $\tilde{A}x \equiv \tilde{b} \bmod q$, gegebenenfalls ein solches x konstruiert und ausserdem eine Basis B von $\{x\in \mathbb{Z}^{n-\ell} \mid \tilde{A}x \equiv 0 \bmod q\}$ berechnet. Mit Hilfe von (*) kann man dann entscheiden, ob es ein $\bar{x}\in \mathbb{Z}^n$ mit $A'\bar{x} = b'$ gibt. Falls die Entscheidung positiv ausfällt, sei $\tilde{A}x \equiv \tilde{b} \bmod q$, $\bar{x} = (x_1,\ldots,x_n)^t$ mit

$$x_i = \frac{1}{q}(b_i - (\tilde{A}x)_i) \quad (1\leq i\leq \ell).$$

Dann ist $A'\bar{x} = b'$. Damit ist (i) gezeigt.

Für $y = (y_{\ell+1},\ldots,y_n)^t \in B$ sei $\bar{y} = (y_1,\ldots,y_n)^t$ mit

$$(y_1,\ldots,y_\ell)^t = -\frac{1}{q}\tilde{A}y .$$

Dann ist $\{\bar{y}: y\in B\}$ eine Basis über $\mathbb{Z}$ von $\{x\in \mathbb{Z}^n \mid A'x=0\}$. Damit ist auch (ii) bewiesen.

13. Satz Seien $A_1,\dots,A_m$ Linearformen auf $\mathbb{Q}^n$ und $b_1,\dots,b_m \in \mathbb{Q}$. Dann gilt

$$\{x\in\mathbb{Q}^n \mid A_i x \geq b_i \ (1\leq i\leq m)\} = \emptyset \iff$$

$$\{y\in\mathbb{Q}^m \mid \sum_{i=1}^m y_i A_i = 0,\ \sum_{i=1}^m y_i b_i = 1,\ y_i \geq 0 \text{ für } 1\leq i\leq m\} \neq \emptyset.$$

Beweis Die Behauptung "$\Longleftarrow$" ist klar. Wir beweisen "$\Longrightarrow$" durch Induktion nach n. Der Fall n = 0 ist klar. Sei $n>0$, $x = (x_1,\dots,x_n)$ mit

$$(S) \qquad A_i x = a_{i1}x_1 + \dots + a_{in}x_n \geq b_i \quad (1\leq i\leq m).$$

Wir setzen

$$A_i' x = a_{i1}x_1 + \dots + a_{in-1}x_{n-1}.$$

Dann ist

$$\frac{1}{a_{in}} A_i' x - \frac{b_i}{a_{in}} \geq -x_n \quad \text{falls } a_{in} > 0$$

$$-x_n \geq \frac{1}{a_{jn}} A_j' x - \frac{b_j}{a_{jn}} \quad \text{falls } a_{jn} < 0$$

Aus (S) folgt also

$$A_k' x \geq b_k \qquad (1\leq k\leq m \text{ mit } a_{kn} = 0)$$

$$(S') \qquad \frac{1}{a_{in}} A_i' x - \frac{1}{a_{jn}} A_j' x \geq \frac{b_i}{a_{in}} - \frac{b_j}{a_{jn}} \quad (1\leq i,j\leq m \text{ mit } a_{in} > 0,\ a_{jn} < 0)$$

Ist umgekehrt (S') für ein $x' = (x_1,\dots,x_{n-1})$ erfüllt, so gilt

$$\alpha = \min\{\frac{1}{a_{in}}(A_i' x' - b_i) \mid a_{in} > 0\} \geq$$

$$\beta = \max\{\frac{1}{a_{jn}}(A_j' x' - b_j) \mid a_{jn} < 0\}.$$

Für jedes x_n mit $\alpha \geq x_n \geq \beta$ ist dann $(x_1,\dots,x_n)$ eine Lösung von (S). Folglich ist (S) lösbar, genau wenn (S') es ist.

Sei der Satz nun schon für n-1 bewiesen und (S) nicht lösbar. Dann gibt es $\alpha_{ij}\geq 0$, $\alpha_k \geq 0$ so dass $\alpha_{ij} = 0$ falls nicht $a_{in}>0$ und $a_{jn}<0$, und $\alpha_k = 0$ falls nicht $a_{kn} = 0$, und

$$\sum_{i,j} \alpha_{ij} \left(\frac{1}{a_{in}} A'_i + \frac{-1}{a_{jn}} A'_j \right) + \sum_k \alpha_k A'_k = 0$$

$$\sum_{i,j} \alpha_{ij} \left(\frac{b_i}{a_{in}} - \frac{b_j}{a_{jn}} \right) + \sum_k \alpha_k b_k = 1.$$

Setzt man

$$y_i = \frac{1}{a_{in}} \left(\sum_{1 \le j \le m} \alpha_{ij} \right) \quad \text{falls } a_{in} > 0$$

$$y_j = \frac{-1}{a_{jn}} \left(\sum_{1 \le i \le m} \alpha_{ij} \right) \quad \text{falls } a_{jn} < 0$$

$$y_k = \alpha_k \quad \text{falls } a_{kn} = 0$$

so gilt $\sum y_i A_i = 0$, $\sum y_i b_i = 1$, $(\forall i)\ y_i \ge 0$.

Die Sprache LINEARE RATIONALE UNGLEICHUNGEN besteht aus allen Paaren (A,b) aus einer ganzzahligen m×n-Matrix A und einem ganzzahligen m-Vektor b mit der Eigenschaft, dass es $x \in \mathbb{Q}^n$ gibt mit $Ax \ge b$.

Korollar LINEARE RATIONALE UNGLEICHUNGEN ebenso wie ihr Komplement ist in NP.

Beweis Der Leser überzeugt sich, dass es eine polynomial beschränkte NT gibt, welche für $I \subset \{1,\ldots,m\}$ ein x_I mit $A_i x_I = b_i$ $(i \in I)$ konstruiert, falls es ein solches gibt (Korollar 1 von 10.) und genau dann akzeptiert, wenn für alle i mit $1 \le i \le m$ $A_i x_I \ge b_i$. Falls das System lösbar ist, gibt es ein I mit $\{x \mid A_i x = b_i \ (\forall i \in I)\} \subset \{x \mid Ax \ge b\}$ (Tschernikow 1971, I.1). Also akzeptiert eine solche Maschine gerade LINEARE RATIONALE UNGLEICHUNGEN. Folglich ist diese Sprache in NP, und nach dem vorangegangenen Satz ebenfalls ihr Komplement.

14. Die Sprache LINEARE DIOPHANTISCHE UNGLEICHUNGEN besteht aus allen Paaren (A,b) von einer ganzzahligen m×n-Matrix A und einem ganzzahligen m-Vektor b mit der Eigenschaft, dass es einen ganzzahligen Vektor x mit $Ax \ge b$ gibt.

Der folgende Satz (von zur Gathen, Sieveking, 197?) zeigt, dass diese Sprache in NP ist.

Satz Seien A eine mxn-Matrix und b ein m-Vektor über $\mathbb{Z}$,
$L = \{x \in \mathbb{Q}^n \mid Ax \geq b\}$, $c = \max_{\substack{1\leq i\leq m \\ 1\leq j\leq n}} \{|a_{ij}|, |b_i|\}$,
$r = (n+1)n^{n(n+1)/2}c^{n^2}$, $K = \{x \in \mathbb{Q}^n \mid |x_j| \leq r \text{ für } 1\leq j\leq n\}$. Dann gilt

$$L \cap \mathbb{Z}^n \neq \emptyset \iff L \cap \mathbb{Z}^n \cap K \neq \emptyset.$$

Korollar LINEARE DIOPHANTISCHE UNGLEICHUNGEN ist in NP und vollständig.

Beweis Es gibt eine polynomial beschränkte NT, die zu (A,b) r wie im Satz berechnet und genau dann akzeptiert, wenn für ein $x \in \mathbb{Z}^n \cap K$ $Ax \geq b$ ist. Also ist diese Sprache in NP.

Die Vollständigkeit folgt aus der polynomialen Transformation

$$\text{RUCKSACK} \leq_\pi \text{LINEARE DIOPHANTISCHE UNGLEICHUNGEN},$$

die jedem $(a_1,\ldots,a_r,b)$ das Ungleichungssystem

$$\begin{aligned}
a_1x_1 + \ldots + a_rx_r &\geq b \\
-a_1x_1 - \ldots - a_rx_r &\geq -b \\
x_1 &\geq 0 \\
-x_1 &\geq -1 \\
&\vdots \\
x_r &\geq 0 \\
-x_r &\geq -1
\end{aligned}$$

zuordnet.

15. Das Komplement der Sprache PRIMZAHLEN ist offensichtlich in NP. Im Folgenden zeigen wir nach (Pratt 197?), dass auch PRIMZAHLEN in NP ist.

Eine Folge $M_1, M_2, \ldots, M_r$ von Mengen heisst zulässig, wenn $M_1 = \{2\}$ und zu jedem i$(2\leq i\leq r)$ Zahlen k,p sowie $e_1,\ldots,e_\ell \in \mathbb{N}$ und $q_1,\ldots,q_\ell \in M_{i-1}$ existieren mit $k\leq p$, $M_i = M_{i-1} \cup \{p\}$ und

(i) $$p - 1 = \prod_{j=1}^{\ell} q_j^{e_j}$$

(ii) $$k^{p-1} \equiv 1 \bmod p$$

(iii) $$(\forall j, 1\leq j\leq \ell)\ k^{(p-1)/q_j} \not\equiv 1 \bmod p$$

Eine Zahl p ist bekanntlich genau dann prim, wenn eine Zahl k existiert, welche modulo p die Ordnung p-1 hat, d.h. für welche

$$k^{p-1} \equiv 1 \bmod p \quad \text{und}$$

$$k^{(p-1)/q} \not\equiv 1 \bmod p \quad \text{für jeden Primteiler } q \text{ von } p-1.$$

Daher folgt mit Induktion nach r, dass jedes Glied einer zulässigen Folge nur aus Primzahlen besteht. Sind $M_1,\ldots,M_r$ und $N_1,\ldots,N_s$ zulässige Folgen, so auch $M_1,\ldots,M_r, M_r \cup N_2,\ldots,M_r \cup N_s$.

Für jeden Test (i), (ii), (iii) benötigt man $O(\log^2 p)$ Multiplikationen modulo p. Also gibt es eine polynomial beschränkte NT, die eine Zahl p genau dann akzeptiert, wenn es eine zulässige Folge $M_1,\ldots,M_r$ gibt mit

$$p \in M_r$$

$$r \leq \lceil \log p \rceil .$$

(Für $p \neq 3,7$ genügt $r \leq \log p$.)

Mit Induktion zeigt man leicht, dass diese NT genau PRIMZAHLEN akzeptiert.

16. Die Sprache PRIMFAKTORZERLEGUNG besteht aus allen Paaren (n,k) von natürlichen Zahlen mit der Eigenschaft, dass es einen Teiler d von n mit $1<d\leq k$ gibt.

Es ist klar, dass diese Sprache in NP ist. Ihr Komplement ist ebenfalls in NP, denn es gibt eine NT, die (n,k) genau dann akzeptiert, wenn es eine zulässige Folge $M_1,\ldots,M_r$ und $p_1,\ldots,p_s \in M_r$, $e_1,\ldots,e_s \in \mathbb{N}$ gibt mit

$$\prod_{1\leq i\leq s} p_i^{e_i} = n$$

$$r \leq \lceil \log n \rceil$$

$$(\forall i, 1\leq i\leq s) \quad k < p_i \text{ und } e_i \leq \log n.$$

17. REDUZIBILITAET VON POLYNOMEN besteht aus allen $f \in \mathbf{Z}[x]$ mit der Eigenschaft, dass es $g,h \in \mathbf{Z}[x]$ gibt mit $g \cdot h = f$ und deg g, deg h>0. Wir kodieren $f = a_n x^n + \ldots + a_0$ als $(n,a_n,\ldots,a_0)$. Diese Sprache ist in NP, denn nach (Mignotte 1974) ist $f = a_n x^n + \ldots + a_0$ reduzibel, genau

wenn es $g = b_m x^m + \ldots + b_0 \in \mathbb{Z}[x]$ gibt mit

$$g \text{ teilt } f$$

$$m \leq \frac{n}{2}$$

$$(\forall i, 1 \leq i \leq m) \; |b_i| \leq \binom{m}{i} \left(\sum_{1 \leq j \leq n} a_j^2 \right)^{1/2}.$$

Offene Probleme

1. Indem man z.B. einer Klausel

$$x_i \vee \bar{x}_j \vee \bar{x}_k$$

die Gleichungen

$$(x_i - 1)(x_j + 1)(x_k + 1) = 0$$

$$x_i^2 = x_j^2 = x_k^2 = 1$$

zuordnet, zeigt man:

ERFUELLBARKEIT MIT HOECHSTENS 3 VARIABLEN PRO KLAUSEL $\leq_\pi$ POLYNOMIALE KOMPLEXE GLEICHUNGEN

Diese Sprache besteht aus allen ganzzahligen Koeffizientenschemata von Systemen von Polynomen, die eine gemeinsame Nullstelle über $\mathbb{C}$ haben. Es ist nicht bekannt, ob diese Sprache in NP ist. Analoges gilt für POLYNOMIALE REELLE GLEICHUNGEN.

2. Falls es eine vollständige Sprache in NP gibt, deren Komplement in NP ist, so ist NP abgeschlossen gegen Komplementbildung. Da dieses nicht zu erwarten ist, kann man eine positive Antwort erhoffen auf die Fragen:

Ist LINEARE RATIONALE UNGLEICHUNGEN (13.) in P?

Ist PRIMZAHLEN (15.) oder PRIMFAKTORZERLEGUNG (16.) in P?

3. Ist IRREDUZIBILITAET VON POLYNOMEN in NP?

Literatur

Bareiss, E.H., Sylvester's Identity and Multistep Integer-Preserving Gaussian Elimination, Math. Comp. 22, 103 (1968) 565-578.

Edmonds, J., Systems of Distinct Representatives and Linear Algebra, Journal of Research of the National Bureau of Standards, 71B, 4 (1967) 241-245.

von zur Gathen, J. und Sieveking, M., A Bound on Solutions of Linear Integer Programs, zur Veröffentlichung eingereicht.

Karp, R.M., Reducibility among Combinatorial Problems, Complexity of Computer Computations, Plenum Press, New York, 1972.

Mignotte, M., An Inequality about Factors of Polynomials, Math. Comp. 28, 128 (1974) 1153-1157.

Pratt, V.R., Every Prime has a Succinct Certificate, erscheint demnächst.

Tschernikow, S.N., Lineare Ungleichungen, VEB Deutscher Verlag der Wissenschaften, Berlin, 1971.