IX. Ein Entscheidungsverfahren für die Theorie der reell-abgeschlossenen Körper

von H.R. Wüthrich

1. Einleitung

Tarski hat in (Tarski 1951) ein Entscheidungsverfahren für die elementare Theorie des Körpers der reellen Zahlen angegeben. Der zeitliche Aufwand dieses Verfahrens für eine Formel der Länge L ist ungefähr

$2^{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}$ L.

1973 gelang es Collins (siehe (Collins 1975)), ein Entscheidungsverfahren (sogar Quantorenelimination) anzugeben, welches mit Aufwand $2^{2^{cL}}$ auskommt. Etwas später hat (Monck 1974) ein wesentlich einfacheres Verfahren vom Aufwand $2^{2^{2^{cL}}}$ gefunden, das von (Solovay 1975) zu einem $2^{2^{cL}}$-Verfahren verbessert wurde. In dieser Arbeit wird eine modifizierte Version des Monck-Solovayschen Verfahrens dargestellt und zu einem Verfahren zur Quantorenelimination ergänzt.

Das Entscheidungsverfahren funktioniert grob gesagt so: Zu jeder Formel $\exists y\varphi\,(x_1,\ldots,x_r,y)$ und jedem r-Tupel $\langle b_1,\ldots,b_r\rangle$ von reellen algebraischen Zahlen wird eine endliche Menge S von reellen algebraischen Zahlen konstruiert, so dass $\exists y\varphi(b_1,\ldots,b_r,y)$ gilt, genau wenn $\varphi(b_1,\ldots,b_r,a)$ gilt für ein $a\in S$. Damit kann jeder geschlossenen Formel φ eine quantorenfreie Formel $\psi(x_1,\ldots,x_s)$ und eine Folge $\langle b_1,\ldots,b_s\rangle$ von reellen algebraischen Zahlen zugeordnet werden, so dass φ gilt genau wenn $\psi(b_1,\ldots,b_s)$ gilt. Das Entscheiden von Primformeln mit algebraischer Variablenbelegung schliesslich wird auf das Entscheiden von Primformeln mit rationaler Variablenbelegung zurückgeführt.

Sei $P\subset \mathbb{R}[x_1,\ldots,x_r]$ eine Menge von Polynomen. Mit $U(P)$ bezeichnen wir die Menge aller maximalen, zusammenhängenden Mengen $U\subset \mathbb{R}$, so dass alle Polynome aus P auf U konstantes Vorzeichen haben. In Paragraph 2 ordnen wir induktiv nach Formelaufbau jeder Formel $\varphi(x_1,\ldots,x_r)$ eine endliche Menge $\mathbb{P}_\varphi\subset \mathbb{Z}[x_1,\ldots,x_r]$ zu, so dass φ auf jeder Menge aus $U(\mathbb{P}_\varphi)$ konstanten Wahrheitswert hat, und gleichzeitig geben wir eine obere Schranke für die Grösse von $\mathbb{P}_\varphi$ in Abhängigkeit von der Länge von φ (Satz 2). Um diese Zuordnung für Formeln der Gestalt $\exists x_i\psi(x_1,\ldots,x_r)$ definieren zu können, führen wir zunächst gewisse Abbildungen

$$E_{x_i}: 2^{\mathbb{Z}[x_1,\ldots,x_r]} \longrightarrow 2^{\mathbb{Z}[x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_r]}.$$

ein, so dass für alle endlichen $\mathbb{P}\subset \mathbb{Z}[x_1,\ldots,x_r]$, alle $U\in U(\mathbb{P})$ und alle

$V \in U(E_{x_i} \mathbb{P})$ die Projektion von U auf die Koordinaten $x_1,\ldots,x_{i-1}$, $x_{i+1},\ldots,x_r$ entweder V umfasst oder leeren Durchschnitt mit V hat. Im Anschluss an die Konstruktion der Zuordnung $\varphi \longrightarrow \mathbb{P}_\varphi$ zeigen wir dann, dass für jede Formel $\varphi(x_1,\ldots,x_r,y)$, jedes reell algebraische r-Tupel $\langle b_1,\ldots,b_r\rangle$ und jedes Repräsentantensystem S der Partition $U(\{P(b_1,\ldots,b_r,y) \mid P \in \mathbb{P}_\varphi\})$ die Formel $\exists y \varphi(b_1,\ldots,b_r,y)$ äquivalent ist zur Disjunktion aller $\varphi(b_1,\ldots,b_r,a)$ mit $a \in S$.

In Paragraph 3 wird nun für jede Partition $U(\mathbb{P}(b_1,\ldots,b_r,y))$ ($\mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r,y]$ endlich) effektiv ein Repräsentantensystem konstruiert. Reell algebraische Zahlen werden dabei dargestellt durch Paare $\langle B,i\rangle$, $B \in \mathbb{Z}[x]$, $i \in \mathbb{N}$, wobei b als i-te reelle Wurzel von B interpretiert wird.

Da jede quantorenfreie Formel äquivalent ist einer booleschen Kombination von Formeln der Form $P(x_1,\ldots,x_r)>0$, $P(x_1,\ldots,x_r) \in \mathbb{Z}[x_1,\ldots,x_r]$, können wir uns beim Entscheiden der mit algebraischen Zahlen belegten Primformeln auf Formeln der Form $P(b_1,\ldots,b_r)>0$ beschränken. Dazu werden die b_k mit Hilfe der Sturmschen Ketten durch rationale Zahlen q_k so approximiert, dass $P(b_1,\ldots,b_r)>0$ genau, wenn $P(q_1,\ldots,q_r) \geq \varepsilon$, wobei ε sowie die notwendige Approximationsgenauigkeit in Abhängigkeit von P und den b_k angegeben werden.

In Paragraph 4 wird der Entscheidungsalgorithmus formuliert und gezeigt (Satz 7), dass eine universelle Konstante c existiert, so dass der Algorithmus jede abgeschlossene Formel der Länge L und Quantorentiefe Q in höchstens L^{c^Q} Schritten entscheidet. (Es werden immer Bit-Operationen gezählt).

In Paragraph 5 schliesslich wird ein Verfahren zur Quantorenelimination beschrieben. Dazu werden die Partitionen $U(\mathbb{P})$ in geeigneter Weise zu Partitionen $V(\mathbb{P})$ verfeinert, nämlich so, dass

1. zu gegebenem $\mathbb{P}$ ein algebraisches Repräsentantensystem von $V(\mathbb{P})$ konstruiert werden kann, und
2. zu gegebenem $\mathbb{P}$ und Repräsentantensystem von $V(\mathbb{P})$ für jeden Punkt $\underline{a}$ des Repräsentantensystems eine quantorenfreie Formel $\Phi_{\underline{a}}(P)$ konstruiert werden kann, die wahr ist genau auf der Zelle von $V(\mathbb{P})$, die $\underline{a}$ enthält.

2. Die einer Formel zugeordnete Partition des $\mathbb{R}^r$

Definition Für $\mathbb{P} \subset \mathbb{R}[x_1,\ldots,x_r]$ sei $U(\mathbb{P})$ die Menge aller maximaler zusammenhängender Mengen $U \subset \mathbb{R}^r$, so dass alle Polynome aus $\mathbb{P}$ auf U

konstantes Vorzeichen haben.

Um die Notation einfacher zu halten, haben wir die Abhängigkeit von U von der Zahl r in obiger Definition nicht zum Ausdruck gebracht. Wenn Missverständnisse nicht zu befürchten sind, werden wir auch im folgenden ähnliche Vereinfachungen der Notation verwenden.

Der Index x_i in den folgenden Definitionen bedeutet, dass alle Polynome als Polynome in x_i mit Koeffizienten in $\mathbb{Z}[x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_r]$ aufgefasst werden.

Definition

Für $i=1,\ldots,r$, für $\left.\begin{array}{l} P = \sum_{j=0}^{n} P_j\, x_i^j \\ Q = \sum_{j=0}^{m} Q_j\, x_i^j \end{array}\right\} \in \mathbb{Z}[x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_r][x_i]$

sei

$$M_{x_i}(P,Q,p,q,g) := \left(\begin{array}{cccccc} P_p & P_{p-1} & \cdots & P_o & & \\ & \ddots & & \ddots & & \\ & & \ddots & & \ddots & \\ & & & P_p & P_{p-1} & \cdots P_o \\ Q_q & Q_{q-1} & \cdots\cdots & Q_o & & \\ & \ddots & & \ddots & & \\ & & Q_q & Q_{q-1} & \cdots\cdots & Q_o \end{array}\right) \begin{array}{l} \} q-(g-1) \\ \} p-(g-1) \end{array}$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{p+q-(g-1)}$$

und

$$S_{x_i}(P,Q,p,q,g) := \det(MM^T)$$

wobei $M := M_{x_i}(P,Q,p,q,g)$.

Für $\mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r]$, sei

$$C_{x_i}\mathbb{P} := \{Q \in \mathbb{Z}[x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_r]: \exists\, P=\sum_{o}^{n} P_j x_i^j \in \mathbb{P},\ \exists\, j\ Q=P_j\}$$

und

$$E_{x_i}\mathbb{P} := C_{x_i}\mathbb{P} \cup \{S_{x_i}(P,Q,p,q,g): P,Q \in (\mathbb{P} \cup \tfrac{\partial}{\partial x_i}\mathbb{P}), p \le \deg_{x_i} P, q \le \deg_{x_i} Q, 1 \le g \le \min(p,q)\}$$

Definition Für $P = \sum a_{i_1\ldots i_r} x_1^{i_1}\ldots x_r^{i_r} \in \mathbb{Z}[x_1,\ldots,x_r]$ sei

$$\sigma(P) := \begin{cases} \max\limits_{i_1,..,i_r} \left\{ \sum\limits_{i=1}^{r} i_j, \ \#\text{Binärstellen von } a_{i_1..i_r} \right\} & \text{falls } P\neq 0 \\ 1 & \text{sonst} \end{cases}$$

und für $\mathbb{P}\subset \mathbb{Z}[x_1,\ldots,x_r]$ sei

$$\sigma(\mathbb{P}) := \max(\{\sigma(P): P\in\mathbb{P}\}\cup\{\#\,\mathbb{P}\})$$

Satz 1 Für alle i, $1\leq i\leq r$, hat E_{x_i} folgende Eigenschaften:

1. $\forall\, \mathbb{P}\subset \mathbb{Z}[x_1,\ldots,x_r]\ \forall\, U\in \mathcal{U}(\mathbb{P})\ \forall\, V\in \mathcal{U}\ (E_{x_i}\mathbb{P})$ gilt:

$$(\exists\,(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_r)\in V\ \exists\, x\in\mathbb{R}\ (a_1,\ldots,a_{i-1},x,a_{i+1},..,a_r)\in U)$$
$$\Longrightarrow (\forall\,(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_r)\in V\ \exists\, x\in\mathbb{R}\ (a_1,\ldots,a_{i-1},x,a_{i+1},\ldots,a_r)\in U)$$

2. Für eine (von r und $\sigma(\mathbb{P})$ unabhängige) Konstante c gilt für alle $\mathbb{P}\subset \mathbb{Z}[x_1,\ldots,x_r]$

$$\sigma(E_{x_i}\mathbb{P}) \leq [r\cdot\sigma(\mathbb{P})]^c$$

Beweis Wir beweisen den Satz oBdA für i=r, um die Notation einfach zu halten.

Beweis von 1.

Wir zeigen: (*)
- $\forall\, V\in \mathcal{U}(E_{x_r}\mathbb{P})$ gilt:
- es gibt stetige Funktionen $f_1,\ldots,f_t$, $f_i: V\longrightarrow\mathbb{R}$ mit
- a) $f_1<\ldots<f_t$ auf V
- b) $\forall\, P\in\mathbb{P}\ \forall\, a\in V\ \forall\, x\in\mathbb{R}\ (P(\underline{a},x)=0 \Longleftrightarrow \exists\, i\ x=f_i(\underline{a}))$.

Daraus folgt 1.:
Sind nämlich $U\in \mathcal{U}(\mathbb{P})$, $V\in \mathcal{U}(E_{x_r}\mathbb{P})$, $\underline{a}\in V$ und $x\in\mathbb{R}$ mit $(\underline{a},x)\in U$, so sei

$$U' := \begin{cases} \{(\underline{a}',x'): \underline{a}'\in V, f_i(\underline{a}')<x'<f_{i+1}(\underline{a}')\} & \text{falls } f_i(\underline{a})<x<f_{i+1}(\underline{a}) \\ \{(\underline{a}',f_i(\underline{a}')): \underline{a}'\in V\} & \text{falls } f_i(\underline{a}) = x \end{cases}$$

Es ist $(\underline{a},x)\in U'$ und U' ist zusammenhängend, somit $U'\subset U$.
Ferner folgt aus (*) und der Def. von U':

$$\forall \underline{a} \in V \ (\{\underline{a}\}\times\mathbb{R}) \cap U' \neq \phi,$$

also $$\forall \underline{a} \in V \ (\{\underline{a}\}\times\mathbb{R}) \cap U \neq \phi.$$

Für den Beweis von (*) sei $V \in \mathcal{U}(E_{x_r}\mathbb{P})$ beliebig, fest. Es gilt:

a) $\forall P \in \mathbb{P}$ $\deg P(\underline{a},x_r)$ = konst. auf V:

Dies folgt aus $C_{x_r}P \subset E_{x_r}P$.

b) $\forall P,Q \in \mathbb{P} \cup \frac{\partial}{\partial x_r}\mathbb{P}$ $\deg(P(\underline{a},x_r),Q(\underline{a},x_r))$ = konst. auf V:

Für ein bel. $\underline{a} \in \mathbb{C}^{r-1}$ mit $\deg P(\underline{a},x_r) =: p, \deg Q(\underline{a},x_r) =: q$ ist nämlich

$$\deg(P(\underline{a},x_r),Q(\underline{a},x_r)) \geq g \iff [S_{x_r}(P,Q,p,q,g)]|_{\underline{a}} = 0,$$ denn:

$[M_{x_r}(P(\underline{a},x_r),Q(\underline{a},x_r),p,q,g)]$ ist die Matrix des homogenen Gleichungssystems für die unbekannten Koeffizienten von $A,B \in \mathbb{C}[x_r]$, die sich durch Koeffizientenvergleich aus

$$\left.\begin{array}{c} A\cdot P(\underline{a},x_r) + BQ(\underline{a},x_r) = 0 \\ \deg A \leq q-g,\ \deg B \leq p-g \end{array}\right\} (**)$$

ergibt; es gilt somit

$$\begin{aligned} & \operatorname{Rang}(M_{x_r}(P(\underline{a},x_r),Q(\underline{a},x_r),p,q,g) \text{ nicht maximal} \\ \iff\ & (**) \text{ nicht-trivial lösbar} \\ \iff\ & \deg(P(\underline{a},x_r),Q(\underline{a},x_r)) \geq g. \end{aligned}$$

Für jede $\square$-Matrix M gilt aber

$$\operatorname{Rang}(M) \text{ nicht maximal} \iff \det(MM^T) = 0$$

(man erweitere M zu einer quadratischen Matrix $\tilde{M}$ durch Hinzufügen von paarweise orthonormierten Zeilen, die zu allen Zeilen von M orthogonal sind. Dann ist

$$\begin{aligned} & \operatorname{Rang}(M) \text{ nicht maximal} \\ \iff\ & \operatorname{Rang}(\tilde{M}) \text{ nicht maximal} \\ \iff\ & \det\tilde{M} = 0 \\ \iff\ & \det(\tilde{M}\tilde{M}^T) = 0 \\ \iff\ & \det(MM^T) = 0, \text{ da ja} \end{aligned}$$

$$\tilde{M}\tilde{M}^T = \left(\begin{array}{c:c} MM^T & \\ & 0 \\ \hdashline 0 & I \end{array}\right),$$

und es ist

$$\begin{aligned} & \det(M_{x_r}(P(\underline{a},x_r),Q(\underline{a},x_r),p,q,g)\cdot M^T_{x_r}(P(\underline{a},x_r),Q(\underline{a},x_r),p,q,g)) \\ &= [\det(M_{x_r}(P,Q,p,q,g)\cdot M^T_{x_r}(P,Q,p,q,g))]|_{\underline{a}} = [S_{x_r}(P,Q,p,q,g)]|_{\underline{a}}. \end{aligned}$$

b) folgt also aus $S_{x_r}(P,Q,p,q,g) \in E_{x_r}\mathbb{P}$.

c) $\forall P \in \mathbb{P}$ gilt: Die Anzahl der verschiedenen reellen Wurzeln von $P(\underline{a},x_r)$ ist konstant auf V:
Seien nämlich $P \in \mathbb{P}$ und $\underline{a} \in V$ beliebig und seien $\alpha_1,\ldots,\alpha_n \in \mathbb{C}$ die verschiedenen komplexen Wurzeln von $P(\underline{a},x_r)$, mit Vielfachheiten $e_1,\ldots,e_k$. Bezeichnet ferner für positives ε

$$\gamma_\varepsilon(\alpha_i) := \{z \in \mathbb{C}: |z-\alpha_i| < \varepsilon\}$$

und für beliebige $Q \in \mathbb{R}[x]$

$N_{\gamma_\varepsilon(\alpha_i)}(Q)$:= Anzahl Wurzeln von Q in $\gamma_\varepsilon(\alpha_i)$ (Vielfachheiten mitgezählt),

so gilt wegen a)

$$\forall \varepsilon>0\ (\gamma_\varepsilon(\alpha_i) \cap \gamma_\varepsilon(\alpha_j)=\phi (i\neq j) \Longrightarrow \text{es gibt eine Umgebung } U(\underline{a}) \text{ in V mit } \forall \underline{b} \in U(\underline{a})\ \forall i\ N_{\gamma_\varepsilon(\alpha_i)}(P(\underline{b},x_r) = e_i). \qquad (***)$$

Unter Benützung von b) lässt sich diese Aussage verschärfen zu

$\forall \varepsilon>0 (\gamma_\varepsilon(\alpha_i) \cap \gamma_\varepsilon(\alpha_j)=\phi (i\neq j)$ und $\forall j\ \gamma_\varepsilon(\alpha_j)$ enthält keine Wurzel $\neq \alpha_j$ von $\frac{d}{dx_r}P(\underline{a},x_r) \Longrightarrow$ es gibt eine Umgebung $U(\underline{a})$ $\forall \underline{b} \in U(\underline{a})$ $\forall j$ $\gamma_\varepsilon(\alpha_j)$ enthält <u>genau eine</u> Wurzel von $P(\underline{b},x_r)$):

Wählt man hier nämlich die gemäss (***) existierende Umgebung $U(\underline{a})$, so gilt für diese sicher

$$\forall \underline{b} \in U(\underline{a})\ \forall i\ N_{\gamma_\varepsilon(\alpha_i)}((P(\underline{b},x_r),\tfrac{d}{dx_r}P(\underline{b},x_r))) \leq N_{\gamma_\varepsilon(\alpha_i)}((P(\underline{a},x_r),\tfrac{d}{dx_r}P(\underline{a},x_r))).$$

Wegen b) muss aber sogar für jedes $\underline{b} \in U(\underline{a})$ und jedes i Gleichheit gelten, weil

$$\sum_{i=1}^{k} N_{\gamma_\varepsilon(\alpha_i)}((P(\underline{b},x_r),\tfrac{d}{dx_r}P(\underline{b},x_r))) = \deg(P(\underline{b},x_r),\tfrac{d}{dx_r}P(\underline{b},x_r)) = \text{konstant auf V.}$$

Sind jetzt etwa $\alpha_1,\ldots,\alpha_t$ die verschiedenen <u>reellen</u> Wurzeln von $P(\underline{a},x_r)$, so existiert nach dem eben Gesagten für hinreichend kleine $\varepsilon>0$ eine Umgebung $U(\underline{a})$, so dass für jedes $\underline{b} \in U(\underline{a})$, jedes $\gamma_\varepsilon(\alpha_i)$ genau eine Wurzel von $P(\underline{b},x_r)$ enthält, und keine reelle Wurzel von $P(\underline{b},x_r)$ ausserhalb $\bigcup_i \gamma_\varepsilon(\alpha_i)$ liegt. Die Wurzel in $\gamma_\varepsilon(\alpha_i)$ ist zudem reell, da auch die konjugiert Komplexe in $\gamma_\varepsilon(\alpha_i)$ liegt (i=1,...,t).
Die Menge

$$T := \{\underline{a} \in V: P(\underline{a},x_r) \text{ hat genau t versch. reelle Wurzeln}\}$$

ist also sowohl offen in V als auch abgeschlossen in V und nicht leer, also gleich V.
Damit ist c) bewiesen.

Wir definieren nun für $P \in \mathbb{P}$ und $1 \leq i \leq \#$ reelle Wurzeln von P auf V

$$f_{P,i} : V \longrightarrow \mathbb{R}$$
$$\underline{b} \longmapsto \text{i-te reelle Wurzel von } P(\underline{b}, x_r).$$

Die $f_{P,i}$ sind auf V wohldefiniert und stetig, nach dem eben Gesagten.

d) Gilt für $Q, P \in \mathbb{P}$, $i, j \in \mathbb{N}$ und ein $\underline{b} \in V$

$$f_{Q,i}(\underline{b}) = f_{P,j}(\underline{b})$$

dann gilt dies für alle $\underline{b} \in V$:

Der Beweis dieser Behauptung verläuft analog dem Beweis von c), wenn man dort $\frac{d}{dx_r} P(\underline{b}, x_r)$ durch $Q(\underline{b}, x_r)$ ersetzt.

Somit ist (*) und damit 1. des Satzes bewiesen.

Beweis von 2.

Sei $\mathbb{P} \subset \mathbb{Z}[x_1, \ldots, x_r]$, $\sigma(\mathbb{P}) =: n$, $r \geq 2$.

α) $\#(E_{x_r} \mathbb{P}) \leq \# C_{x_r} P + \# \{S_{x_r}(P,Q,p,q,g) : 1 \leq p, \gamma \leq n,\ 1 \leq g \leq \min\{p,q\},$
$P, Q \in \mathbb{P} \cup \frac{\partial}{\partial x_r} \mathbb{P}\}$

$$\leq (n+1)^2 + 4n^5 \leq r^2(n^2+n^5) \leq (r \cdot n)^5$$

β) Sei $R \in E_{x_r} \mathbb{P}$.

Falls $R \in C_{x_r} \mathbb{P}$, dann $\sigma(R) \leq n$.

Sei jetzt $R = S_{x_r}(P,Q,p,q,g)$ für $P, Q \in \mathbb{P} \cup \frac{\partial}{\partial x_r} \mathbb{P}$, $1 \leq p, q \leq n$, $1 \leq g \leq \min\{p,q\}$

$S_{x_r}(P,Q,p,q,g) = \det(M_{x_r}(P,Q,p,q,g) \cdot M^T_{x_r}(P,Q,p,q,g))$

Es ist leicht nachzurechnen:

(i) $P_1, \ldots, P_m \in \mathbb{Z}[x_1, \ldots, x_r]$ & $\sigma(P_i) \leq n$ $(i=1,..,m) \Rightarrow \sigma(\sum_1^m P_i) \leq n + \log m$

(ii) P_i wie (i) $\Longrightarrow \sigma(\prod_1^m P_i) \leq m \cdot n(r+1)$

($\prod_1^m P_i$ ist eine Summe von $(n+1)^{rm}$ Produkten von Monomen der P_i)

(iii) Ist M eine Matrix der Ordnung m mit Elementen $P_i \in \mathbb{Z}[x_1, \ldots, x_{r-1}]$, $\sigma(P_i) \leq n$, dann $\sigma(\det M) \leq m(rn+m)$

(iv) Ist M eine $m \times t$-Matrix mit Elementen $P_i \in \mathbb{Z}[x_r, \ldots, x_{r-1}]$, $\sigma(P_i) \leq n$, dann ist $M M^T$ eine $m \times m$-Matrix mit Elementen $Q_i \in \mathbb{Z}[x_1, \ldots, x_{r-1}]$, $\sigma(Q_i) \leq 2nr + \lg t$

(v) $M_{x_r}(P,Q,p,q,g)$ ist eine $m \times t$-Matrix mit Elementen $P_i \in \mathbb{Z}[x_1, \ldots, x_{r-1}]$ mit $m, t, \sigma(P_i) \leq 2n$. Daraus folgt

$$\sigma(S_{x_r}(P,Q,p,q,g)) \leq (nr)^6.$$

Damit ist Satz 1 vollständig bewiesen.

In der Theorie der reell abgeschlossenen Körper ist jede Primformel äquivalent einer Formel,in der nur Primformeln vom Typ $P>o$ ($P \in \mathbb{Z}[x_1,\ldots,x_r]$) vorkommen. Für das Folgende werde deshalb vorausgesetzt, dass jede Primformel von diesem Typ sei. Um die Darstellung zu vereinfachen, jedoch o.B.d.A., wollen wir auch voraussetzen, dass in jeder Formel nur die logischen Operationen $\vee$ und $\neg$, und nur $\exists$ -Quantoren vorkommen.
Die Schreibweise $\Psi(x_1,\ldots,x_r)$ soll besagen, dass $\{x_1,\ldots,x_r\}$ die Menge der freien Variablen in Ψ umfasse.
Wir werden ferner die Schreibweise $\varphi = \Psi \vee \Phi$, $\varphi = \neg\Psi$ etc. benützen um auszudrücken, dass φ eine Formel vom Typ $\Psi \vee \Phi$, $\neg\Psi$ etc. sei.

Definition Jeder Formel $\varphi(x_1,\ldots,x_r)$ ordnen wir eine Menge $\mathbb{P}_{\varphi(x_1,\ldots,x_r)} \subset \mathbb{Z}[x_1,\ldots,x_r]$ zu wie folgt:

a) $\mathbb{P}_{P(x_1,\ldots,x_r)>o} := \{P(x_1,\ldots,x_r)\}$

b) $\mathbb{P}_{(\Phi\vee\Psi)(x_1,\ldots,x_r)} := \mathbb{P}_{\Phi(x_1,\ldots,x_r)} \cup \mathbb{P}_{\Psi(x_1,\ldots,x_r)}$

c) $\mathbb{P}_{\neg\Psi(x_1,\ldots,x_r)} := \mathbb{P}_{\Psi(x_1,\ldots,x_r)}$

d) $\mathbb{P}_{\exists y\,\Psi(x_1,\ldots,x_{r,y})} := E_y\mathbb{P}_{\Psi(x_1,\ldots,x_{r,y})}$

Definition Für eine Formel $\varphi(x_1,\ldots,x_r)$ und $(a_1,\ldots,a_r) \in \mathbb{R}^r$ sei

$$\hat{\varphi}(a_1,\ldots,a_r) := \begin{cases} 1 \text{ falls } \varphi(a_1,\ldots,a_r) \text{ gilt in } \mathbb{R} \\ 0 \text{ sonst.} \end{cases}$$

Satz 2 (1) Für jede Formel $\varphi(x_1,\ldots,x_r)$, für jedes $V \in \mathfrak{U}(\mathbb{P}_{\varphi(x_1,\ldots,x_r)})$ gilt

$$\hat{\varphi}(x_1,\ldots,x_r) = \text{konstant auf } V.$$

(2) Es gibt eine Konstante c, so dass für jede Formel $\varphi(x_1,\ldots,x_r)$ mit Länge $\ell > r$ und Quantorentiefe q gilt

$$\sigma(\mathbb{P}_{\varphi(x_1,\ldots,x_r)}) \leq \ell^{c^q}.$$

Beweis Durch Induktion nach der Länge von $\varphi(x_1,\ldots,x_r)$.

(1) Wir führen nur den Fall $\varphi(x_1,\ldots,x_r) = \exists y\Psi(x_1,\ldots,x_r,y)$ aus:

$\mathbb{P}_{\varphi(x_1,\ldots,x_r)} = E_y\, \mathbb{P}_{\Psi(x_1,\ldots,x_r,y)}$ (Def. von $\mathbb{P}_\varphi$)

Der Satz gelte für $\Psi(x_1,\ldots,x_r,y)$.

Sei $V \in U(\mathbb{P}_{\varphi(x_1,\ldots,x_r)})$, $\underline{a} \in V$ mit $\hat{\varphi}(\underline{a}) = 1$.

$\Longrightarrow$ es existiert $b \in \mathbb{R}, \hat{\Psi}(\underline{a},b) = 1$

Sei $U \in U(\mathbb{P}_{\Psi(x_1,\ldots,x_r,y)})$ mit $(\underline{a},b) \in U$

$\Longrightarrow$ für alle $\underline{a}' \in V$ existiert b' mit $(\underline{a}',b') \in U$
Satz 1

$\Longrightarrow$ für alle $\underline{a}' \in V$ existiert b' mit $\hat{\Psi}(\underline{a}',b') = 1$
I.V.

$\Longrightarrow$ für alle $\underline{a}' \in V$ $\hat{\varphi}(\underline{a}') = 1$.

(2) Auch hier ist $\varphi(x_1,\ldots,x_r) = \exists y\, \Psi(x_1,\ldots,x_r,y)$ der einzige nicht-triviale Fall.

Es existiere c sodass für jede Formel $\varphi(x_1,..,x_r)=(\exists y)\Psi(x_1,..,y_r,y)$ der Länge ℓ und Quantorentiefe q $\sigma(\mathbb{P}_{\Psi(x_1,\ldots,x_r,y)}) \leq \ell^{c^{q-1}}$.

Gemäss Satz 1(2) existiert $\bar{c}$ so dass

$$\sigma(E_y\mathbb{P}_{\Psi(x_1,\ldots,x_r,y)}) \leq [(r+1)\cdot\sigma(\mathbb{P}_{\Psi(x_1,\ldots,x_r,y)}]^{\bar{c}}$$

also

$$\sigma(\mathbb{P}_\varphi) = \sigma(E_y\mathbb{P}_\Psi) \leq [(r+1)\cdot\ell^{c^{q-1}}]^{\bar{c}} \leq \ell^{\bar{c}(c^{q-1}+1)} \leq \ell^{c^q},$$

falls etwa $c \geq 2\bar{c}$.

Definition Für $\mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r,y]$ und $\underline{a}=(a_1,\ldots,a_r) \in \mathbb{R}^r$ sei

$\mathbb{P}(\underline{a},y) := \{P(a_1,\ldots,a_r,y): P \in \mathbb{P}\} \subset \mathbb{R}[y]$.

Korollar zu Satz 2

Sei $\varphi(x_1,\ldots,x_r,y)$ eine Formel und $\underline{a}=(a_1,\ldots,a_r) \in \mathbb{R}^r$ beliebig und sei $\mathbb{P} := \mathbb{P}_{\varphi(x_1,\ldots,x_r,y)}$. Dann gilt für alle $V \in U(\mathbb{P}(\underline{a},y))$

$$\hat{\varphi}(\underline{a},b) = \text{konst. für alle } b \in V.$$

Beweis Nach Definition von V gilt für alle $P \in \mathbb{P}_{\varphi(x_1,\ldots,x_r,y)}$:

$$\operatorname{sg} P(\underline{a},b) = \text{konst. für alle } b \in V .$$

Da V zusammenhängend, gibt es ein $W \in U(\mathbb{P}_{\varphi(x_1,\ldots,x_r,y)})$ mit $\{\underline{a}\}\times V \subset W$.

Da $\hat{\varphi}$ = konst. auf W gemäss Satz 2, folgt die Behauptung.

Wenn wir sagen, eine Punktmenge S sei ein Repräsentantensystem (R.S.) einer Partition $\mathfrak{U}$, so verstehen wir darunter: $\forall U \in \mathfrak{U}\ U \cap S \neq \phi$. Diese Durchschnitte brauchen nicht einpunktig zu sein.

Satz 3 Sei $\varphi(x_1,\ldots,x_r)$ eine Formel, $\underline{a} = (a_1,\ldots,a_r) \in \mathbb{R}^r$. Dann gilt

a) falls $\varphi = P>o$: $\hat{\varphi}(\underline{a}) = \begin{cases} 1 \text{ falls } P(\underline{a})>o \\ 0 \text{ sonst} \end{cases}$

b) falls $\varphi = \Psi \vee \Phi$: $\hat{\varphi}(\underline{a}) = \max\{\hat{\Psi}(\underline{a}),\hat{\Phi}(\underline{a})\}$

c) falls $\varphi = \neg\Psi$: $\hat{\varphi}(\underline{a}) = 1-\hat{\Psi}(\underline{a})$

d) falls $\varphi = (\exists y)\Psi(x_1,\ldots,x_r,y)$, so sei $\mathbb{P}(x_1,\ldots,x_r,y) := \mathbb{P}_{\Psi(x_1,..,x_r,y)}$ und S ein Repräsentantensystem von $\mathfrak{U}(\mathbb{P}(\underline{a},y))$.
Dann $\hat{\varphi}(\underline{a}) = \max\limits_{b\in S}\{\hat{\Psi}(\underline{a},b)\}$

Beweis Die Fälle a), b), c) sind trivial. Im Fall d) gilt

$\hat{\varphi}(\underline{a}) = 1$

$\Longleftrightarrow$ es existiert $b \in \mathbb{R}$ mit $\hat{\Psi}(\underline{a},b) = 1$

$\Longleftrightarrow$ es existiert $b \in S$ mit $\hat{\Psi}(\underline{a},b) = 1$ (Korollar zu Satz 2)

$\Longleftrightarrow \max\limits_{b\in S}\{\hat{\Psi}(\underline{a},b)\} = 1$

Satz 3 liefert in offensichtlicher Weise ein Entscheidungsverfahren, induktiv nach Formelaufbau. Damit dieses effektiv sei, müssen wir noch angeben, wie die Fälle a) und d) effektiv behandelt werden.

3. Effektive Berechnung eines R.S. von $\mathfrak{U}(\mathbb{P}(\underline{a},y))$ und von $sgP(\underline{a})$ für algebraisches $\underline{a}$.

Eine reelle algebraische Zahl stellen wir dar durch ein Paar (B,i), wo $B \in \mathbb{Z}[x]$, $i \in \mathbb{N}$. a ist dann die i-te reelle Wurzel von B (jede Wurzel einfach gezählt).
Wir zeigen zuerst, wie in dieser Darstellung ein Repräsentantensystem von $\mathfrak{U}(\mathbb{P}(\underline{a},y))$ berechnet wird, nachher, wie $P(\underline{a})>o$ entschieden wird.

Definition Für $\mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r,y]$, $\mathbb{A} \subset \mathbb{R}^r$ sei

$$I(\mathbb{P},\mathbb{A}) := \{b \in \mathbb{R}: \exists P \in \mathbb{P}\ \exists \underline{a} \in \mathbb{A}\ P(\underline{a},b)=o \ \&\ P(\underline{a},y)\neq o\}.$$

Definition Für $\mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r,y]$ sei

$$\tilde{\mathbb{P}} := \{y, P, P\pm Q, \frac{\partial}{\partial y}P, P\pm 1: P,Q \in \mathbb{P}\}$$

Lemma 3.1 $\forall\, \underline{a} \in \mathbb{R}^r \; \forall\, \mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r,y]$ ist $I(\tilde{\mathbb{P}},\{\underline{a}\})$ ein R.S. für $U(\mathbb{P}(\underline{a},y))$.

Beweis Sei $\underline{a} \in \mathbb{R}^r$, $V \in U(\mathbb{P}(\underline{a},y))$.
Zu zeigen: $V \cap I(\tilde{\mathbb{P}},\{\underline{a}\}) \neq \phi$.
Falls $V = \{b\}$ für ein $b \in \mathbb{R}$, dann $b \in I(\mathbb{P},\{\underline{a}\}) \subset I(\tilde{\mathbb{P}},\{\underline{a}\})$.
Andernfalls $V = (b,c)$ für $b,c \in \mathbb{R} \cup \{\pm\infty\}$, $b<c$.

α) $b,c \in \mathbb{R}$.
Dann existiert $P,Q \in \mathbb{P}$ mit $P(\underline{a},b) = Q(\underline{a},c) = o$.
Die Behauptung folgt dann
falls $P = Q$: wegen $\frac{\partial}{\partial y} P \in \tilde{\mathbb{P}}$
falls $P \neq Q$: wegen $P \pm Q \in \tilde{\mathbb{P}}$.

β) $b \in \mathbb{R}$ und $c = \infty$ oder $b = -\infty$ und $c \in \mathbb{R}$,
wie α), mit $P \pm 1$ statt $P \pm Q$

γ) $b = -\infty$, $c = +\infty$.
Hier gilt die Behauptung, weil $o \in I(\tilde{\mathbb{P}},\{\underline{a}\})$.

Lemma 3.2 Sei $\mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r,y]$, $\mathbb{B} \subset \mathbb{Z}[x_1]$, $\mathbb{A} \subset \mathbb{R}^{r-1}$.
Dann

$$I(\mathbb{P},I(\mathbb{B})\times\mathbb{A}) \subset \mathbb{Z}(E_{x_1}(\mathbb{B}\cup\mathbb{P}),\mathbb{A})$$

Beweis Es genügt, den Fall $\mathbb{A} = \{\underline{a}\}$, $\underline{a} = (a_2,\ldots,a_r) \in \mathbb{R}^{r-1}$ zu beweisen.
Wir zeigen: $\forall \underline{a} \in \mathbb{R}(a \notin I(E_{x_1}(\mathbb{B}\cup\mathbb{P}),\{\underline{a}\}) \Longrightarrow a \notin I(\mathbb{P},I(\mathbb{B})\times\{\underline{a}\}))$.
Sei $a,b \in \mathbb{R}$, $a \notin I(E_{x_1}(\mathbb{B}\cup\mathbb{P}),\{\underline{a}\})$ und $P \in \mathbb{P}$, $o \neq B \in \mathbb{B}$ mit $P(b,\underline{a},a)=o$, $B(b)=o$.
Zu zeigen: $P(b,\underline{a},y) = o$.
Sei $V \in U(E_{x_1}(\mathbb{B}\cup\mathbb{P}))$ mit $(\underline{a},a) \in V$ und $U \in U(\mathbb{B}\cup\mathbb{P})$ mit $(b,\underline{a},a) \in U$.
Dann
(i) $\forall a'((\underline{a},a') \in V \Longrightarrow \exists\, b'(b',\underline{a},a') \in U$ ((Satz 1)
(ii) $U = \{b\}\times U'$ für ein gewisses $U' \subset \mathbb{R}^r$
(denn $B=o$ auf $U \Longrightarrow \#\{b_1 : \exists\, b_2,\ldots,b_{r+1}(b_r,\ldots,b_{r+1}) \in U\} < \infty$ und U zusammenhängend.)
Wegen $P=o$ auf U folgt aus (i) und (ii):

$$\forall a'((\underline{a},a') \in V \Longrightarrow (b,\underline{a},a') \in U \Longrightarrow P(b,\underline{a},a')=o)$$

Daraus folgt $P(b,\underline{a},y) = o$, denn
$a \notin I(E_{x_1}(\mathbb{B}\cup\mathbb{P}),\underline{a}) \Longrightarrow \forall\, Q \in E_{x_1}(\mathbb{B}\cup\mathbb{P})(Q(\underline{a},y) = o \vee Q(\underline{a},a) \neq o)$

$\Longrightarrow$ es gibt ein Intervall $W \subset \mathbb{R}$, so dass $a \in W$ und
$(\forall a' \in W\ \forall Q \in E_{x_1}(\mathbb{B} \cup \mathbb{P})\ \operatorname{sg} Q(\underline{a},a') = \operatorname{sg} Q(\underline{a},a))$

$\Longrightarrow \{a\} \times W \subset V \Longrightarrow \#\{a' : (\underline{a},a') \in V\} = \infty$.

Definition Für $\mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r,y]$ und $B_1,\ldots,B_r \in \mathbb{Z}[x]$ sei $RS(\mathbb{P},B_1,\ldots,B_r) \in \mathbb{Z}[y]$ definiert durch:

$$\mathbb{B}_1 := \tilde{\mathbb{P}},$$
$$\mathbb{B}_{i+1} := E_{x_i}(\mathbb{B}_i \cup \{B_i\}) \quad (i=1,\ldots,r),$$
$$RS(\mathbb{P},B_1,\ldots,B_r) := \prod_{A \in \mathbb{B}_{r+1}} A .$$

Satz 4 Seien $\mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r,y]$, $B_1,\ldots,B_r \in \mathbb{Z}[x]$ und sei $B := RS(\mathbb{P},B_1,\ldots,B_r)$.

Dann (1) $\forall \underline{a} \in I(B_1)\times\ldots\times I(B_r)$ ist $I(B)$ ein R.S. für $U(\mathbb{P}(\underline{a},y))$.

(2) $\sigma(B) \leq [\sigma(\mathbb{P}) \cdot \max_{1\leq i\leq r}\{\sigma(B_i)\}]^{k^{r+1}}$ für eine gewisse universelle Konstante k.

Beweis (1) Aus Lemma 3.2 folgt durch Induktion nach i $(i=1,\ldots,r)$

$$I(\mathbb{B}_i, I(B_i)\times\ldots\times I(B_r)) \subset I(\mathbb{B}_{i+1}, I(B_{i+1})\times\ldots\times I(B_r)),$$

also

$$I(\tilde{\mathbb{P}}, I(B_1)\times\ldots\times I(B_r)) \subset I(B).$$

Gemäss Lemma 3.1 steht links von $\subset$, für alle $\underline{a} \in I(B_1)\times\ldots\times I(B_r)$, ein R.S. von $U(\mathbb{P}(\underline{a},y))$, also auch rechts.

(2) Sei $m := \sigma(\mathbb{P})$, $n := \max_{1\leq i\leq r}(\sigma(B_i))$, und o.B.d.A. $m \geq 2$.

Es existieren k_1, k_2 mit

$$\sigma(\mathbb{B}_1) \leq m^{k_1} \qquad \text{(Def. von } \tilde{\mathbb{P}})$$
$$\sigma(\mathbb{B}_{i+1}) \leq (r\cdot\sigma(\mathbb{B}_i)\cdot n)^{k_2} \quad (i=1,\ldots,r) \qquad \text{Satz 1,(2)}$$

Durch Induktion nach i folgt für $k := \max\{k_1,k_2\}$

$$\sigma(\mathbb{B}_i) \leq (r\cdot n)^{\sum_{t=1}^{i-1} k^t} \cdot m^{k^i} \quad (i=1,\ldots,r+1)$$

Daraus folgt (ii), da $\sigma(B) \leq [\sigma(\mathbb{B}_{r+1})]^2$.

Die folgende Prozedur berechnet $RS(\mathbb{P},B_1,\ldots,B_r)$. Auf die Berechnung von E_{x_i} wir später eingegangen (Lemma 4.2).

<u>procedure</u> REPRESENT $(\mathbb{P},B_1,\ldots,B_r)$;

Input: $\mathbb{P}\subset \mathbb{Z}[x_1,\ldots,x_r,y]$
$B_1,\ldots,B_r \in \mathbb{Z}[x]$, $B_i \neq o$ $(i=1,\ldots,r)$

Output: $RS(\mathbb{P},B_1,\ldots,B_r)$

<u>begin</u> $\mathbb{B}_1 := \tilde{\mathbb{P}}$;
<u>if</u> r=o <u>then</u> <u>goto</u> exit;
<u>for</u> i=1,...,r <u>do</u>
$\mathbb{B}_{i+1} := E_{x_i}(\mathbb{B}_i \cup \{B_i\})$;
Comment $\mathbb{B}_i \subset \mathbb{Z}[x_i,\ldots,x_r,y]$ $(i=1,\ldots,r)$
$\mathbb{B}_{r+1} \subset \mathbb{Z}[y]$;

exit: $B := \prod_{A\in \mathbb{B}_{r+1}} A$;

<u>end</u>;

Wir kommen nun zur Berechnung von sg $P(\underline{a})$ für algebraisches $\underline{a}$.

<u>Definition</u> Für $a\in\mathbb{R}$ sei

$$\sigma(a) := \begin{cases} \min\{\sigma(P): P\in\mathbb{Z}[x],\ P\neq o,\ P(a)=o\} & \text{falls existiert} \\ \infty & \text{sonst} \end{cases}$$

<u>Bemerkung</u> Für ein $a\in\mathbb{Z}$, aufgefasst als ein $P\in\mathbb{Z}[x_1,\ldots,x_r]$, ist $\sigma(a) = \sigma(P)$.

Für algebraische Zahlen $a_1,\ldots,a_r$ entscheiden wir $P(a_1,\ldots,a_r)>o$, indem wir die a_i durch rationale q_i approximieren und für ein geeignetes ε $P(q_1,\ldots,q_r)\geq\varepsilon$ entscheiden.
Der folgende Satz gibt ein solches ε und die erforderliche Approximationsgüte in Abhängigkeit von $\sigma(P)$, $\sigma(a_i)$ an. Die Voraussetzungen sind dabei unseren Bedürfnissen angepasst.

<u>Satz 5</u> Zu jedem $k_o\in\mathbb{R}^+$ existieren $k_1,k_2\in\mathbb{R}^+$, so dass gilt:
$\forall r,L\in\mathbb{N}$ $\forall P\in\mathbb{Z}[x_1,\ldots,x_r]$ mit $\sigma(P)\leq L$, $\forall(a_1,\ldots,a_r)\in\mathbb{R}^r$ mit $\sigma(a_i)\leq L^{k_o^r}$ $(i=1,\ldots,r)$ $\forall(q_1,\ldots,q_r)\in\mathbb{R}^r$

$$(|a_i-q_i|<2^{-L^{k_2^r}}(i=1,..,r) \Longrightarrow (o<P(a_1,...,a_r) \Longleftrightarrow 2^{-L^{k_1^r}} \leq P(q_1,...,q_r))).$$

k_1 und k_2 können in Abhängigkeit von k_o effektiv angegeben werden.

Beweis Es genügt zu zeigen:

(i) Zu jedem k_o gibt es ein k_1, so dass $\forall r$, $L\in\mathbb{N}$, $\forall P\in \mathbf{Z}[x_1,...,x_r]$, $\forall (a_1,...,a_r)\in \mathbb{R}^r$ unter den Voraussetzungen des Satzes

$$P(a_1,...,a_r) = o \quad \text{oder} \quad |P(a_1,...,a_r)| \geq 2\cdot 2^{-L^{k_1^r}}$$

(ii) Zu jedem k_o, k_1 gibt es ein k_2, so dass $\forall r$, $L\in\mathbb{N}$, $\forall P\in \mathbf{Z}[x_1,...,x_r]$, $\forall(a_1,...,a_r)\in \mathbb{R}^r$ unter den Voraussetzungen des Satzes

$$\forall(q_1,..,q_r)\in \mathbb{R}^r\ (|a_i-q_i|<2^{-L^{k_2^r}},i=1,..,r \Longrightarrow |P(a_1,..,a_r)-P(q_1,..,q_r)|< 2^{-L^{k_1^r}})$$

Daraus folgt der Satz: Ist k_o vorgegeben und dazu k_1 gemäss (i), k_2 gemäss (ii), so gilt mit $\varepsilon_j := 2^{-L^{k_j^r}}$ $(j=1,2)$, für $|a_i-q_i|<\varepsilon_2$:

$$P(a_1,...,a_r)>o \underset{(i)}{\Longrightarrow} P(a_1,...,a_r)\geq 2\varepsilon_1 \underset{(ii)}{\Longrightarrow} P(q_1,...,q_r) \geq \varepsilon_1$$

und

$$P(q_1,...,q_r) \geq \varepsilon_1 \underset{(ii)}{\Longrightarrow} P(a_1,...,a_r) > o$$

Beweis von (i) Ein bekannter Satz der Funktionentheorie besagt:

Ist $B = c_n x^n+...+c_o \in \mathbb{C}[x]$, $c_n\neq o$ und $B(a)=o$, dann

$$|a| \leq 2\cdot \max_k \sqrt[k]{|\frac{c_{n-k}}{c_n}|}.$$

Für $B\in \mathbf{Z}[x]$ folgt daraus

$$B(a) = o \Longrightarrow |a| \leq 2^{\sigma(B)+1},$$

somit

$$|a| \leq 2^{\sigma(a)+1} \qquad (*)$$

Mit $C(x) := x^n\cdot B(\frac{1}{x})$ gilt ferner für $a\neq o$: $C(\frac{1}{a})=o \Longleftrightarrow B(a)=o$, also $\sigma(a)=\sigma(\frac{1}{a})$.

$(*)$ auf $\frac{1}{a}$ angewandt ergibt:

$$a\neq o \Longrightarrow 2^{-(\sigma(a)+1)} \leq |a|$$

Für den Beweis von (i) genügt es deshalb, ein k_1 anzugeben mit $\sigma(P(a_1,...,a_r)) \leq L^{k_1^r}-2$

Zu diesem Zwecke seien $B_1,...,B_r\in \mathbf{Z}[x]$ mit

$$\left.\begin{array}{l}\sigma(B_i) \leq L^{k_o^r} \\ B_i(a_i) = o\end{array}\right\} \; i=1,\ldots,r$$

und

$$\mathbb{P} := \{y-P(x_1,\ldots,x_r)\} \subset \mathbb{Z}[x_1,\ldots,x_r,y].$$

Gemäss Satz 4 gilt dann für $B(y) := RS(\mathbb{P},B_1,\ldots,B_r) \in \mathbb{Z}[y]$: $I(B(y))$ ist ein R.S. für $U(\mathbb{P}(a_1,\ldots,a_r,y))$, somit

$$B(P(a_1,\ldots,a_r)) = 0.$$

Deshalb ist $\sigma(P(a_1,\ldots,a_r)) \leq \sigma(B(y))$, woraus die Existenz von k_1 mit Satz 4, (2) folgt.

Beweis von (ii) Dies ist im wesentlichen der Beweis der gleichmässigen Stetigkeit von $P(x_1,\ldots,x_r) \in \mathbb{Z}[x_1,\ldots,x_r]$, $\sigma(P(x_1,\ldots,x_1)) \leq L$, auf dem Bereich $\{(a_1,\ldots,a_r) \in \mathbb{R}^r: -2\cdot 2^{L^{k_o^r}} \leq a_i \leq +2\cdot 2^{L^{k_o^r}}, 1 \leq i \leq r\}$, wie man mit Hilfe von (*) aus (i) erkennt.

Durch Ausführen der Beweise erkennt man auch die Gültigkeit der letzten Behauptung des Satzes.

Satz 6 Man kann einen Algorithmus angeben, der folgendes leistet:
Input :- $B \in \mathbb{Z}[x]$ mit $\sigma(B) =: n$ und den verschiedenen reellen Wurzeln

$a_1,\ldots,a_w$

- $s \in \mathbb{N}$

Output: $r_1,\ldots,r_w \in \mathbb{Z}$ mit

(1) $\left|a_i - \frac{r_i}{2^s}\right| \leq 2^{-s}$

(2) $|r_i| \leq 2^{n+1+s}+1$

Es gibt Konstante c_1,c_2, so dass der Algorithmus weniger als $c_1(ns)^{c_2}$ Schritte benötigt.

Beweis Siehe (Heindel 1971), speziell Korollar 7.1

4. Formulierung des Algorithmus und Zeitabschätzung

Sätze 1-6 liefern einen effektiven Algorithmus für die Entscheidung abgeschlossener Formeln. Für dessen Formulierung wollen wir die Existenz folgender Unteralgorithmen (Funktionsprozeduren) voraussetzten, z.T.

ohne sie explizite zu formulieren. Statt dessen wird jeweils auf die entsprechenden Sätze verwiesen.

1. PARTITION : Input: $\varphi(x_1,\ldots,x_r)$, eine Formel
Output: $\mathbb{P}_{\varphi(x_1,\ldots,x_r)} \subset \mathbb{Z}[x_1,\ldots,x_r]$
$\Big\}\ r\geq 1$
(Def. von $\mathbb{P}_\varphi$, Lemma 4.2)

2. REPRESENT : Input: $\mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r,y]$
$B_1,\ldots,B_r \in \mathbb{Z}[x]$
$\Big\}\ r\geq 0$
Output: $RS(\mathbb{P},B_1,\ldots,B_r) \in \mathbb{Z}[y]$
(Satz 4)

3. PRIMETRUTH: Input: $P \in \mathbb{Z}[x_1,\ldots,x_r]$
$B_1,\ldots,B_r \in \mathbb{Z}[x]$.
$i_1,\ldots,i_r \in \mathbb{N}$
Output: 1 falls $P(a_1,..,a_r)>0$
0 sonst
$\Big\}$ wobei a_k die i_k-te reelle Wurzel von B_k ist. $(1\leq k\leq r)$
Um die Notation nicht zu belasten, wird angenommen, es sei dafür gesorgt, dass diese Prozedur Länge und Quantorentiefe der Inputformel des Hauptalgorithmus kenne.
(Satz 5, Satz 6, Lemma 4.1)

4. NROOTS : Input: $B \in \mathbb{Z}[x]$
Output: $n \in \mathbb{N}$, die Anzahl der verschiedenen reellen Wurzeln von B
(Satz 6)

Wir formulieren jetzt die rekursive Prozedur TRUTH mit

Input : $\varphi(x_1,\ldots,x_r)$, eine Formel
$B_1,\ldots,B_r \in \mathbb{Z}[x]$
$i_1,\ldots,i_r \in \mathbb{N}$
$\Big\}\ r\geq 0$

Output: $\hat{\varphi} := \hat{\varphi}(a_1,\ldots,a_r)$ wo a_k = i_k-te reelle Wurzel von B_k.

Im Fall r=o ist TRUTH der gesuchte Entscheidungsalgorithmus.

Zur Abkürzung setzen wir

$(\underline{x})$ für $(x_1,\ldots,x_r)$
$(\underline{B})$ für $(B_1,\ldots,B_r)$
$(\underline{i})$ für $(i_1,\ldots,i_r)$.

```
PROCEDURE  TRUTH (φ(x̲), (B̲), (i̲));
begin If φ(x̲) = P(x̲)>o then φ̂ := PRIMETRUTH (P(x̲),(B̲),(i̲)) else
      if φ(x̲) = Ψ(x̲) ∨ Φ(x̲) then φ̂ := max(TRUTH(Ψ(x̲),(B̲),(i̲)),
                                          TRUTH(Φ(x̲),(B̲),(i̲))) else
      if φ(x̲) = ¬ Ψ(x̲) then φ̂ := 1-TRUTH(Ψ(x̲),(B̲),(i̲)) else
      begin comment φ(x̲) = ∃ x_{r+1} Ψ(x̲,x_{r+1});
            ℙ := PARTITION(Ψ(x̲,x_{r+1}));
        B_{r+1} := REPRESENT(ℙ,(B̲));
            n := NROOTS(B_{r+1});
            φ̂ := max  (TRUTH(Ψ(x̲,x_{r+1}),(B̲,B_{r+1}),(i̲,i_{r+1})));
                 1≤i_{r+1}≤n
      end;
end;
```

(Da ein einziger Aufruf von PARTITION auch die zu sämtlichen Teilformeln gehörigen Partitionen berechnet, würde ein einmaliger Aufruf dieses Unteralgorithmus genügen und selbstverständlich zu einer besseren Zeitschranke für den Hauptalgorithmus führen. Diese Verbesserung würde aber lediglich in den Konstanten zum Ausdruck kommen. Die obige "kompaktere" Darstellung des Algorithmus wurde deshalb vorgezogen.)

Die Richtigkeit des Algorithmus folgt unmittelbar aus Satz 3.

Für die Anwendung von Satz 5 auf PRIMETRUTH beweisen wir das folgende Lemma, das auch für die Abschätzung des Aufwandes wichtig ist.

Lemma 4.1 Es gibt eine Konstante k_o, so dass folgendes gilt: Wird TRUTH mit einer abgeschlossenen Formel Γ der Länge L und Quantorentiefe Q aufgerufen, dann gilt für jeden rekursiven Aufruf

$$\text{TRUTH}(\varphi(x_1,\ldots,x_r),\ B_1,\ldots,B_r,\ i_1,\ldots,i_r)$$

$$(1)\quad r \le Q$$

$$(2)\quad \sigma(B_j) \le L^{k_o^Q} \qquad j=1,\ldots,r\ .$$

Beweis Für den Beweis der (von k_o unabhängigen) Behauptung (1) zeigt man durch Induktion nach r:

$$r + q \le Q\ ,$$

wobei q die Quantorentiefe von $\varphi(x_1,\ldots,x_r)$ ist.

Für den Beweis von Behauptung (2) zeigt man durch Induktion nach r die Existenz einer Konstanten k, so dass bei geeigneter Numerierung der B_j

$$\sigma(B_j) \leq Q^{\sum_{\rho=1}^{j=1}(2k)^\rho \cdot L^{2^j \cdot k^{Q+j-1}}} \qquad (1 \leq j \leq r) \qquad (*)$$

für jeden rekursiven Aufruf TRUTH($\varphi(x_1,\ldots,x_1),B_1,\ldots,B_r,i_1,\ldots,i_r$). Im Induktionsschritt zeigt man durch Induktion nach j, unter der Voraussetzung (*), dass für die $\mathbb{B}_j$ in der Prozedur REPRESENT($\mathbb{P}_{\Psi(x_1,\ldots,x_{r+1})},B_1,\ldots,B_r$) gilt:

$$\sigma(\mathbb{B}_j) \leq Q^{\frac{1}{2}\sum_{\rho=1}^{j=1}(2k)^\rho \cdot L^{2^{j-1} \cdot k^{Q+j-1}}} \qquad (j=1,\ldots,r+1) \qquad (**)$$

unter Benützung von Satz 1 (2).

Für den Induktionsanfang in (**) benützt man Satz 2 (2) und beachtet, dass für eine geeignete Konstante $\tilde{k}$

$$\sigma(\tilde{\mathbb{P}}) \leq [\sigma(\mathbb{P})]^{\tilde{k}}.$$

Die Behauptung für B_{r+1} folgt wegen

$$\sigma(\prod_{A \in \mathbb{B}_{r+1}} A) \leq [\sigma(\mathbb{B}_{r+1})]^2$$

und $r \leq Q$.

Aus dem Lemma folgt, dass für alle im Verlaufe des Algorithmus auftretenden Polynome die Voraussetzungen in Satz 5 für r := Q erfüllt sind.

In der Prozedur PARTITION müssen bei der Berechnung von $E_y\mathbb{P}(x_1,\ldots,x_r,y)$ Determinanten mit Elementen aus $\mathbb{Z}[x_1,\ldots,x_r]$ berechnet werden. Dazu:

Lemma 4.2 Es gibt eine Konstante c, so dass für alle m,n die Determinante einer m×m-Matrix mit Elementen $P \in \mathbb{Z}[x_1,\ldots,x_r]$, $\sigma(P) \leq n$, in höchstens $[c(r+1)\cdot n \cdot m^2]^{2(r+1)}$ Schritten berechnet werden kann.

Beweis In (Bareiss 1968) wird ein Determinanten-Algorithmus für Matrizen mit Elementen aus einem Ring A angegeben und gezeigt, dass alle während der Berechnung auftretenden Elemente Unterdeterminanten der gegebenen Matrix sind. Für den Fall $A = \mathbb{Z}[x_1,\ldots,x_r]$ lässt sich die obige Zeitschranke leicht nachweisen, wenn man noch die Bemerkungen unter β) des Beweises von Satz 1, (2), beachtet.

Satz 7 Es gibt eine Konstante k, so dass Algorithmus TRUTH für das Entscheiden jeder abgeschlossenen Formel Γ der Länge L und Quantorentiefe Q L^{k^Q} Schritte benötigt.

Beweis Sei $T_1(L,Q,\ell,q)$ der Zeitbedarf für einen Aufruf $TRUTH(\varphi(x_1,\ldots,x_r),B_1,\ldots,B_r,i_1,\ldots,i_r)$, der im Verlaufe der Berechnung von TRUTH(Γ) vorkommt, wenn L und Q resp. ℓ und q Länge und Quantorentiefe von Γ resp. φ sind.
Wir zeigen, dass für gewisse Konstante c_1, c_2

$$T_1(L,Q,\ell,q) \leq \ell \cdot L^{c_1^Q + q c_2^Q} \qquad (*)$$

Daraus folgt der Satz, indem man etwa

$$k := 1 + c_2 + c_3^2$$

und $\ell=L$, $q=Q$ setzt.
Wir beweisen (*) für festes L und Q durch Induktion nach ℓ.

Sei $TRUTH(\varphi(x_1,\ldots,x_r),B_1,\ldots,B_r,i_1,\ldots,i_r)$ ein Aufruf, der im Verlaufe der Berechnung von TRUTH(Γ) vorkomme, L,Q,ℓ,q wie oben, und (*) sei bewiesen für Aufrufe mit Formeln der Länge $<\ell$.

a) $\varphi(x_1,\ldots,x_r) = P(x_1,\ldots,x_r) > o$

Gemäss Lemma 4.1 gibt es ein k_o mit $\sigma(B_j) \leq L^{k_o^Q}$ $(j=1,\ldots,r)$.
Für jede reelle Wurzel a eines B_j gilt daher

$$|a| \leq 2 \cdot 2^{k_o^Q} \qquad (**)$$

(siehe Beweis von (i), Satz 5)

Gemäss Satz 5 muss PRIMETRUTH für gewisse k_1, k_2 $P(q_1,\ldots,q_r)\text{-}2^{-L^{k_1^Q}}$ berechnen, wobei q_j eine rationale Approximation mit Genauigkeit $2^{-L^{k_2^Q}}$ der i_j-ten reellen Wurzel von B_j $(j=1,\ldots,r)$ ist.
Wegen Satz 6 und $r \leq Q$ (Lemma 4.1) existiert c_3, so dass die Berechnung der q_j höchstens $L^{c_3^Q}$ Schritte benötigt.
Dasselbe gilt für die Berechnung von $P(q_1,\ldots,q_r)\text{-}2^{-L^{k_1^Q}}$, wie man leicht nachrechnet unter Berücksichtigung von $\sigma(P) \leq L$ und der Tatsache, dass für ein k_3 die Länge von Zähler und Nenner der q_j stets durch $L^{k_3^Q}$ beschränkt sind (Satz 6).

Für den Nachweis von (*) wähle man nun c_1 so, dass $L^{c_1^Q}$ den gesamten Aufwand von PRIMETRUTH beschränkt.

b) $\varphi(x_1,\ldots,x_r) = \Psi(x_1,\ldots,x_r) \vee \Phi(x_1,\ldots,x_r)$

Sind ℓ_1 resp. ℓ_2 die Längen von Ψ resp. Φ, so folgt aus der Induktionsvoraussetzung direkt

$$\begin{aligned} T_1(L,Q,\ell,q) &\leq T_1(L,Q,\ell_1,q) + T_2(L,Q,\ell_2,q) \\ &\leq \ell_1 L^{c_1^Q + q c_2^Q} + \ell_2 L^{c_1^Q + q c_2^Q} \\ &\leq \ell \cdot L^{c_1^Q + q c_2^Q} \end{aligned}$$

c) $\varphi(x_1,\ldots,x_r) = \neg\, \Psi(x_1,\ldots,x_r)$

Analog Fall b)

d) $\varphi(x_1,\ldots,x_r) = \exists\, x_{r+1}\ \Psi(x_1,\ldots,x_{r+1})$

Sei $T_2(L,Q,\ell,q)$ der gesamte Aufwand für die Berechnung von

$$\begin{aligned} \mathbb{P} &:= \text{PARTITION}(\Psi(x_1,\ldots,x_{r+1})) \\ B_{r+1} &:= \text{REPRESENT}(\mathbb{P},B_1,\ldots,B_r) \\ n &:= \text{NROOTS}(B_{r+1}) \ . \end{aligned}$$

Falls gezeigt ist, dass c_4 existiert mit $T_2(L,Q,\ell,q) \leq L^{c_4^Q}$, so sind wir fertig. Da gemäss Lemma 4.1 $n \leq \sigma(B_{r+1}) \leq L^{k_o^Q}$ liefert nämlich die Induktionsvoraussetzung für den Fall d) ein c_2, sodass

$$\begin{aligned} T_1(L,Q,\ell,q) &\leq T_2(L,Q,\ell,q) + n \cdot T_1(L,Q,\ell-1,q-1) \\ &\leq L^{c_4^Q} + L^{k_o^Q} \cdot (\ell-1) \cdot L^{c_1^Q + (q-1)c_2^Q} \\ &\leq \ell \cdot L^{c_1^Q + (k_o+c_4)^Q + (q-1)c_2^Q} \end{aligned}$$

woraus die Behauptung folgt, wenn nur $c_2 \geq k_o + c_4$.

Für die Existenz von c_4 hat man PARTITION, REPRESENT und NROOTS zu untersuchen:

Die Prozedur PARTITION arbeitet rekursiv gemäss Def. von $\mathbb{P}_\varphi$.

Mit Hilfe von Lemma 4.2 kann man für deren Zeitbedarf $T_3(L,Q,\ell,q)$ durch Induktion nach ℓ zeigen, dass c_5 existiert mit

$$T_3(L,Q,\ell,q) \leq \ell+q\cdot\ell^{c_5^Q};$$

also gibt es ein c_6 mit

$$T_3(L,Q,\ell,q) \leq L^{c_6^Q},$$

denn $q\leq\ell\leq L$.

Der Aufwand von REPRESENT und NROOTS liegt ebenfalls unter der geforderten Schranke. Im ersten Fall folgt dies mit Hilfe der Sätze 2 und 3 sowie Lemma 4.1, im zweiten Fall mit Satz 6 (der ja auch die Anzahl der Wurzeln liefert) und Lemma 4.1.

Damit ist Satz 7 vollständig bewiesen.

5. Quantorenelimination

Definition Für $\mathbb{P}\subset\mathbb{Z}[x_1,\ldots,x_r]$, $1\leq k\leq r$, sei

$$D_{x_k}\mathbb{P} := \{\frac{\partial^i}{\partial x_k^i}P : P\in\mathbb{P}, 0\leq i\leq \deg_{x_k}P\}$$

Definition Für $\mathbb{P}\subset\mathbb{Z}[x_1,\ldots,x_r]$ definieren wir induktiv nach r

$$\mathbb{V}(\mathbb{P}) := \begin{cases} \{(W\times\mathbb{R})\cap U: W\in\mathbb{V}(E_{x_r}D_{x_r}\mathbb{P}), U\in\mathbb{U}(D_{x_r}\mathbb{P}), (W\times\mathbb{R})\cap U\neq\phi\} & \text{falls } r\geq 2 \\ \mathbb{U}(D_{x_1}\mathbb{P}) & \text{falls } r=1 \end{cases}$$

Definition Sind $\mathbb{U},\mathbb{V}$ Partitionen des $\mathbb{R}^r$, dann

$$\mathbb{V}\geqslant\mathbb{U} : \Longleftrightarrow \forall\, V\in\mathbb{V}\ \exists\, U\in\mathbb{U}\ V\subset U$$

Lemma 5.1 $\mathbb{V}(\mathbb{P})$ ist eine Partition des $\mathbb{R}^r$ und $\mathbb{V}(\mathbb{P})\geqslant\mathbb{U}(D_{x_r}\mathbb{P})\geqslant\mathbb{U}(\mathbb{P})$

Beweis 1. $\mathbb{V}(\mathbb{P})$ ist Partition:
Induktion nach r
gemäss Induktionsvoraussetzung ist $\mathbb{V}(\mathbb{P})$ dann Durchschnitt von 2 Partitionen, also selber Partition.

2. $\mathbb{V}(\mathbb{P})\geqslant\mathbb{U}(D_{x_r}\mathbb{P})\geqslant\mathbb{U}(\mathbb{P})$: trivial.

Wegen $\mathbb{V}(\mathbb{P})\geqslant\mathbb{U}(D_{x_r}\mathbb{P})$ hat jedes $P\in D_{x_r}\mathbb{P}$ auf jedem $V\in\mathbb{V}(\mathbb{P})$ konstantes Vorzeichen.

Die Abbildung

$$\Sigma : \mathbb{V}(\mathbb{P}) \longrightarrow \{-1,0,+1\}^{D_{x_r}\mathbb{P}}$$
$$V \longmapsto (P \mapsto \text{sg } P \text{ auf } V)$$

ist deshalb wohldefiniert.

Für $V \in \mathbb{V}(\mathbb{P})$ sei

$$\mathbb{Z}_V(\mathbb{P}) := \{V' \in \mathbb{V}(\mathbb{P}) : \text{proj}_{x_1,\ldots,x_{r-1}}(V') = \text{proj}_{x_1,\ldots,x_{r-1}}(V)\}$$

Aus der Definition von $\mathbb{V}(\mathbb{P})$ folgt:

$$\forall\, V \in \mathbb{V}(\mathbb{P})\ \exists\, W \in \mathbb{V}(E_{x_r} D_{x_r} \mathbb{P})(\bigcup \mathbb{Z}_V(\mathbb{P}) = W \times \mathbb{R}).$$

Lemma 5.2 $\forall\, \mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r]$ $\forall\, V \in \mathbb{V}(\mathbb{P})$ gilt:

$\Sigma \restriction \mathbb{Z}_V(\mathbb{P})$ ist injektiv.

Beweis

a) $r>1$

Seien $\mathbb{P}$, $V \in \mathbb{V}(\mathbb{P})$ vorgegeben und seien
$V_i \in \mathbb{Z}_V(\mathbb{P})$, $V_i = (W \times \mathbb{R}) \cap U_i$, $W \in \mathbb{V}(E_{x_r} D_{x_r} \mathbb{P})$, $U_i \in \mathbb{U}(D_{x_r}\mathbb{P})$ $(i=1,2)$,
mit $\Sigma(V_1) = \Sigma(V_2)$.

Sei $(\underline{a}, b_1) \in V_1$ beliebig gewählt. $(\underline{a} \in W, b_1 \in \mathbb{R})$ Dann existiert $b_2 \in \mathbb{R}$, so dass $(\underline{a}, b_2) \in V_2$ (denn $(W \times \mathbb{R}) \cap V_2 \neq \phi$, somit $(\{\underline{a}'\} \times \mathbb{R}) \cap V_2 \neq \phi$ für alle $\underline{a}' \in W$).
Ist etwa $b_1 \leq b_2$, so genügt es, zu zeigen:

$$\forall\, P \in D_{x_r}\mathbb{P}\ \forall\, t \in [b_1, b_2]\ \text{sg } P(\underline{a}, t) = \text{sg } P(\underline{a}, b_2),$$

(denn daraus folgt $\{\underline{a}\} \times [b_1, b_2] \subset V_2$ und insbesondere $(\underline{a}, b_1) \in V_2$, also $V_1 = V_2$).

Hierzu genügt es, für $P \in \mathbb{R}[x]$ und $b_1 \leq b_2 \in \mathbb{R}$ zu zeigen:

$$\forall i\left(\text{sg}\left[\frac{d^i}{dx^i}P\right]_{x=b_1} = \text{sg}\left[\frac{d^i}{dx^i}P\right]_{x=b_2}\right) \Longrightarrow \forall i\left(\text{sg}\frac{d^i}{dx^i}P = \text{const. auf } [b_1, b_2]\right)$$

und dies geschieht leicht durch Induktion nach dem Grad von P.

b) $r=1$

Dieser Fall ist in offensichtlicher Weise im Beweis von Fall a) enthalten.

Definition Für $\mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r]$ werde jedem $\underline{a} \in \mathbb{R}^r$ eine quantorenfreie Formel $\Phi_{\underline{a}}(\mathbb{P})$ in den freien Variablen $x_1,\ldots,x_r$ zugeordnet wie folgt:

$r>1$: $\Phi_{(a_1,..,a_r)}(\mathbb{P}) := \Phi_{(a_1,..,a_{r-1})}(E_{x_r} D_{x_r} \mathbb{P}) \wedge \bigwedge_{P \in D_{x_r}\mathbb{P}} (sgP = sgP(a_1,..,a_r))$

$r=1$: $\Phi_a(\mathbb{P}) := \bigwedge_{P \in D_{x_1}\mathbb{P}} sgP = sgP(a)$

$(sgP=sgP(a_1,...,a_1)$ ist dabei eine Abkürzung für

$$\begin{cases} P > o & \text{falls } P(a_1,...,a_r) > o \\ P = o & \text{falls } P(a_1,...,a_r) = o \\ P < o & \text{falls } P(a_1,...,a_r) < o) \end{cases}$$

Korollar zu Lemma 5.2 Mit den obigen Bezeichnungen gilt:

Ist $\underline{a} \in V \in \mathbb{V}(\mathbb{P})$, dann ist $\Phi_{\underline{a}}(\mathbb{P})$ wahr genau auf V.

Beweis Durch Induktion nach r folgt die Behauptung sofort aus dem Lemma.

Definition Für $\mathbb{P} \subset \mathbb{Z}[x_1,...,x_r]$ sei $\nu_i(\mathbb{P}) \in \mathbb{Z}[x]$ $(i=1,...,r)$ definiert durch

$$\nu_i(\mathbb{P}) := \begin{cases} \nu_i(E_{x_r} D_{x_r} \mathbb{P}) & (i=1,...,r-1) \\ RS(D_{x_r}\mathbb{P}, \nu_1(\mathbb{P}),...,\nu_{r-1}(\mathbb{P})) & (i=r) \end{cases}$$

Lemma 5.3 $\forall \mathbb{P} \subset \mathbb{Z}[x_1,...,x_r]$ gilt:

$I(\nu_1(\mathbb{P})) \times ... \times I(\nu_r(\mathbb{P}))$ ist ein R.S. für $\mathbb{V}(\mathbb{P})$

Beweis Induktion nach r, mit Satz 4.

Satz 8 Sei $\varphi(x_1,...,x_r)$ eine Formel mit Länge L, Quantorentiefe Q und r freien Variablen und sei $\Psi(x_1,...,x_r)$ definiert durch

$$\Psi(x_1,...,x_r) := \bigvee_{\underline{a} \in M} \Phi_{\underline{a}}(x_1,...,x_r)$$

wobei $M := \{\underline{a} \in I(\nu_1(\mathbb{P}_\varphi)) \times ... \times I(\nu_r(\mathbb{P}_\varphi)) : \hat{\varphi}(\underline{a}) = 1\}$.

Dann gilt (1) $\varphi(x_1,...,x_r) \equiv \Psi(x_1,...,x_r)$

(2) Es gibt eine universelle Konstante c, so dass Ψ mit Aufwand $\leq L^{c^{Q+r}}$ berechnet werden kann.

Beweis Der Beweis von (1) folgt aus den Lemmas 5.1 und 5.3 und dem Korollar zu Lemma 5.2. Auf den Beweis von (2) wird hier verzichtet.

Die auszuführenden Ueberlegungen und Rechnungen sind völlig analog denen in Satz 7.

Im folgenden werden Algorithmen für die oben beschriebene Quantorenelimination (ELIM), die Berechnung der $\Phi_{\underline{a}}(\mathbb{P})$ (PHI) sowie der $\nu_i(\mathbb{P})$ (RSV) angedeutet.

PROCEDURE ELIM($\varphi(x_1,\ldots,x_r)$);

Input: $\varphi(x_1,\ldots,x_r)$, eine Formel

Output: $\Psi(x_1,\ldots,x_r)$, quantorenfrei, $\varphi(x_1,\ldots,x_r) \equiv \Psi(x_1,\ldots,x_r)$

```
begin  if r=0 then begin if TRUTH(φ)=1  then Ψ := (0=0)
                                        else Ψ := (0>0);
                     goto exit;
                   end
       P := PARTITION(φ(x_1,...,x_r);
       (B_1,...,B_r) := RSV(P);
       Ψ := "empty formula";
       for j := 1,...,r do
          n_j := NROOTS(B_j);
       for i_1 := 1,...,n_1 do  ┐
           . . . . . .          │
           . . . . . .          ├ *)
       for i_r := 1,...,n_r do  ┘
           if TRUTH(φ,B_1,...,B_r,i_1,...,i_r) = 1 then
                                  Ψ := Ψ ∨ PHI(P,B_1,...,B_r,i_1,...,i_r);
end
```

*) Der Uebersichtlichkeit halber wurde diese Schreibweise einer vom jeweiligen r unabhängigen vorgezogen.

PROCEDURE RSV(P);

Input: $\mathbb{P} \subset \mathbb{Z}[x_1,\ldots,x_r]$, endlich, $r \geq 1$

Output: $(B_1,\ldots,B_r) \in (\mathbb{Z}[x])^r$, $B_i = \nu_i(\mathbb{P})$ $(i=1,\ldots,r)$

```
begin  if r>1 then (B_1,...,B_{r-1}) := RSV(E_{x_r} D_{x_r} P);
       B_r := REPRESENT(D_{x_r} P,B_1,...,B_{r-1});
end
```

PROCEDURE PHI($\mathbb{P}, B_1, \ldots, B_r, i_1, \ldots, i_r$);

Input: $\mathbb{P} \subset \mathbb{Z}[x_1, \ldots, x_r]$ endlich
$B_1, \ldots, B_r \in \mathbb{Z}[x]$
$i_1, \ldots, i_r \in \mathbb{N}$

Output: $\Phi := \Phi_{(a_1,\ldots,a_r)}(\mathbb{P})$ gemäss Definition von $\Phi_{\underline{a}}(\mathbb{P})$,
wobei a_j = i_j-te reelle Wurzel von B_j $(j=1,\ldots,r)$

```
begin for "P ∈ D_{x_r}ℙ" do
      if PRIMETRUTH(P,B_1,...,B_r,i_1,...,i_r) = 1 then π_p := P>o else
      if PRIMETRUTH(-P,B_1,...,B_r,i_1,...,i_r) = 1 then π_p := P<o else
      π_p := P=o;
      if r>1 then
      Φ := PHI(E_{x_r}D_{x_r}ℙ,B_1,...,B_{r-1},i_1,...,i_{r-1}) ∧ ⋀_{P∈D_{x_r}ℙ} π_p
      else
      Φ := ⋀_{P∈D_{x_1}ℙ} π_p;
end
```

Literatur

Bareiss, E.H., Sylvester's Identity and Multistep Integer Preserving Gaussian Elimination, Math. Comp. 22 (1968) 565-566.

Collins, G.E., Quantifier elimination for real closed fields by cylindrical algebraic decomposition, Lecture Notes in Computer Science No. 33, pp. 134-183, Springer, 1975.

Heindel, L.E., Integer Arithmetic Algorithms for Polynomial Real Zero Determination, J. ACM 18 (1971) 533-548.

Monck, L., An Elementary-Recursive Decision Procedure for Th($\mathbb{R}$,+,·), Univ. of Calif., Berkeley, Dept. of Math., preprint.

Solovay, R., Brieflicher Hinweis 1975.

Tarski, A., A Decision Method for Elementary Algebra and Geometry, University of California Press, Berkeley, 1951.