Seminar
Entscheidungsverfahren für Logische Theorien

Thema: Quantorenelimination

Stefanie Lück
e-Mail: slueck@uni-koblenz.de

01.03.2005

Universität Koblenz
Wintersemester 2004/2005
Dr. Peter Baumgartner

Inhaltsverzeichnis

Kapitel 1

Einführung und Grundlagen

1.1 Was ist Quantorenelimination und wozu dient sie?

Die Quantorenelimination ist ein Verfahren der mathematischen Logik, mit dem Formeln vereinfacht werden. Anwendungsgebiete sind zum Beispiel Beweisverfahren für geometrische Sätze oder die Vereinfachung der Überprüfung, ob eine entscheidbare Theorie **T** erfüllbar ist. Hier zeigt man, dass jede in **T** enthaltene Formel, die Quantoren enthält, sich in eine quantorenfreie Formel umwandeln lässt, die in **T** äquivalent ist. Die Gültigkeit dieser quantorenfreien Formel in **T** ist dann besonders einfach entscheidbar.

Quantorenelimination spielt auch in automatischen Beweisen und der Computeralgebra eine wichtige Rolle, da sie hilft, das Entscheidungsproblem für die zugrunde liegende Theorie zu vereinfachen oder sogar ganz zu lösen.

Ob es eine Methode zur Eliminierung von Quantoren gibt, hängt von der Sprache ab, in der die Formeln definiert wurden. Es ist häufig erforderlich, Formeln umzuschreiben, zum Beispiel in Pränexform, bevor ein Quantoreneliminierungsalgorithmus auf sie angewendet werden kann. Danach wird ein Quantor nach dem anderen von innen nach außen eliminiert.

1.2 Grundlagen

Um das Verfahren der Quantorenelimination in einer Theorie **T** verstehen zu können, werden zunächst einige Grundbegriffe erklärt. Danach folgt eine kurze Einführung in die Zahlentheorie.

1.2.1 Grundbegriffe

Eine Struktur ist ein Paar $\Re = (U_\Re, I_\Re)$ und es gilt:

- $U_\Re$ ist eine beliebige Menge $\neq \emptyset$ (die Grundmenge bzw. das Universum)
- $I_\Re$ ist eine Abbildung, die:
  - jedem k-stelligen Prädikatsymbol P (das im Definitionsbereich von $I_\Re$ liegt) ein k-stelliges Prädikat über $U_\Re$ zuordnet

  - jedem k-stelligen Funktionssymbol f (im Definitionsbereich von $I_\Re$) eine k-stellige Funktion auf $U_\Re$ zuordnet
  - jeder Variablen x (wenn $I_\Re$ auf x definiert ist) ein Element der Grundmenge $U_\Re$ zuordnet

- der Definitionsbereich von $I_\Re$ ist eine Teilmenge von $\{P_i^k, f_i^k, x_i | i = 1, 2, \ldots$ und $k = 0, 1, 2, \ldots\}$
- der Wertebereich von $I_\Re$ ist eine Teilmenge aller Prädikate und Funktionen auf $U_\Re$, sowie der Elemente von $U_\Re$

Eine Struktur heißt *passend* zu einer Formel, wenn sie für alle in der Formel vorkommenden Prädikatsymbole, Funktionssymbole und freien Variablen definiert ist. Eine Formel F *gilt* in einer Struktur $\Re$, falls $\Re$ zu F passt und $\Re$ F wahr macht. Man sagt dann auch, dass $\Re$ *Modell* für F ist und schreibt $\Re \models F$. F ist *allgemeingültig*, wenn jede zu F passende Struktur ein Modell für F ist. In diesem Fall schreibt man $\models F$. F ist *erfüllbar*, wenn es mindestens ein Modell für F gibt.

Eine *Theorie* $\mathbf{T}$ ist eine Formelmenge, die gegen Folgerbarkeit abgeschlossen ist, das heisst $\mathbf{T}$ ist eine Theorie, wenn für alle $F_i \in \mathbf{T}$ mit $(i = 1, \ldots, n)$ und alle Formeln G gilt: Wenn G aus $\{F_1, \ldots, F_n\}$ folgt, dann ist $G \in \mathbf{T}$. Alle gültigen Formeln sind in $\mathbf{T}$ enthalten. Ein Satz ist eine Formel, die Element dieser Theorie $\mathbf{T}$ ist.

$\mathbf{T}$ kann also wie folgt definiert werden: Gegeben ist eine Struktur $\Re$. Die Theorie zu dieser Struktur ist die Menge aller Formeln, die in $\Re$ gültig sind. Es gilt also: $\mathbf{T} = \mathrm{Th}\,\Re = \{F \,|\, \Re \models F\}$. Für jede Formel F gilt entweder $F \in \mathbf{T}$ oder $\neg F \in \mathbf{T}$, das heisst $\mathbf{T}$ ist immer vollständig.

1.2.2 Einführung in die Zahlentheorie

Im Folgenden wird die Sprache der Zahlentheorie betrachtet. Das ist eine prädikatenlogische Sprache mit Gleichheit und den folgenden Parametern:

- $\forall$, was so viel bedeuten soll wie "für alle natürlichen Zahlen"
- $\mathbf{0}$, einer Konstanten
- $\mathbf{S}$, einem einstelligen Funktionssymbol für die Nachfolgerfunktion mit:

$$\mathbf{S} : \mathbb{N} \to \mathbb{N} \qquad \text{und} \qquad \mathbf{S}(n) = n + 1 \qquad \forall\, n \in \mathbb{N}$$

  Für jede natürliche Zahl k gibt es einen Term $\mathbf{S}^k\mathbf{0}$, der für sie steht.

$$\begin{aligned} \mathbf{S}^0\mathbf{0} &= \mathbf{0} \\ \mathbf{S}^1\mathbf{0} &= \mathbf{S0} = 1 \\ \mathbf{S}^2\mathbf{0} &= \mathbf{SS0} = 2 \\ &\vdots \end{aligned}$$

- $<$, einem zweistelligen Prädikatsymbol für die Ordnungsrelation in $\mathbb{N}$

- $+$, $\cdot$ und $\mathbf{E}$, zweistelligen Funktionssymbolen für die Operationen "Addition", "Multiplikation" und "Exponentialfunktion"

$\Re$ soll die Struktur für diese Sprache sein, also $\Re = (\mathbb{N}, 0, S, <, +, \cdot, E)$. Es gilt $|\Re| = \mathbb{N}$ und $\mathbf{0} = 0$. Man kann nun verschiedene "Untersprachen" dieser Sprache bilden, indem man bestimmte Funktions- oder Prädikatsymbole einfach weglässt. Im Folgenden wird nur $\Re_S = (\mathbb{N}, 0, S)$ betrachtet.

1.3 Natürliche Zahlen mit Nachfolgern

In der betrachteten Sprache $\Re_S = (\mathbb{N}, 0, S)$ der natürlichen Zahlen mit Nachfolgern ist es immer noch möglich, jedes Element von $\mathbb{N}$ zu benennen. Als Parameter haben wir hier nur noch $\forall, \mathbf{0}$ und S.

A_S sei die Menge, die aus den folgenden Sätzen S1 bis S4 besteht. Diese Sätze gehören alle zu $\operatorname{Th}\Re_S$, sind also in $\Re_S$ wahr.

S1: $\forall x\, \mathbf{S}x \not\approx \mathbf{0}$ ($\mathbf{0}$ hat keinen Vorgänger)

S2: $\forall x \forall y(\mathbf{S}x \approx \mathbf{S}y \to x \approx y)$ (die Nachfolgerfunktion ist injektiv)

S3: $\forall y(y \not\approx \mathbf{0} \to \exists x\ y \approx \mathbf{S}x)$ (alle Zahlen ungleich $\mathbf{0}$ sind der Nachfolger einer anderen Zahl)

S4:

$$\left.\begin{array}{rcl} \forall x\, \mathbf{S}x & \not\approx & x \\ \forall x\, \mathbf{SS}x & \not\approx & x \\ & \vdots & \\ \forall x\, \mathbf{S}^n x & \not\approx & x \end{array}\right\} \text{(es entstehen keine Loops durch die Nachfolgerfunktion)}$$

$\Re_S$ ist also ein Modell für A_S ($\Re_S \models A_S$).
Es gilt außerdem $Cn\, A_S \subseteq \operatorname{Th}\Re_S$, wobei $Cn\, A_S$ die *Konsequenz* von A_S ist. Dies ist die Menge aller Sätze G, für die A_S Modell ist, oder anders gesagt, die Menge aller Sätze G, die aus A_S folgen ($Cn\, A_S = \{G | A_S \models G\}$)

Um zu beweisen, dass sogar $Cn\, A_S = \operatorname{Th}\Re_S$ gilt, werden zunächst beliebige Modelle für A_S betrachtet. Eine Struktur $\mathfrak{A} = (|\,\mathfrak{A}\,|, \mathbf{0}^{\mathfrak{A}}, \mathbf{S}^{\mathfrak{A}})$ wird so konstruiert, dass $\mathfrak{A}$ A_S wahr macht.

Zuerst lässt sich feststellen, dass $\mathbf{S}^{\mathfrak{A}}$ wegen S2 eine injektive Abbildung sein muss. Nach den Axiomen S1 und S3 muss $\mathbf{S}^{\mathfrak{A}}$ außerdem eine Abbildung von $|\,\mathfrak{A}\,|$ nach $|\,\mathfrak{A}\,| - \{\mathbf{0}^{\mathfrak{A}}\}$ sein. Letzteres wird klar, wenn man sich überlegt, dass $\mathbf{0}^{\mathfrak{A}}$ keinen Vorgänger haben darf. Wegen S4 dürfen natürlich keine Loops entstehen. Deshalb muss $|\,\mathfrak{A}\,|$ folgende Standardelemente enthalten, die alle verschieden sein müssen:

$$\mathbf{0}^{\mathfrak{A}} \to \mathbf{S}^{\mathfrak{A}}(\mathbf{0}^{\mathfrak{A}}) \to \mathbf{S}^{\mathfrak{A}}(\mathbf{S}^{\mathfrak{A}}(\mathbf{0}^{\mathfrak{A}})) \to \ldots$$

Wenn es noch andere Elemente a in $|\,\mathfrak{A}\,|$ gibt, so gibt es auch deren Nachfolger, den Nachfolger des Nachfolgers usw., wegen S2 und S3 muss $|\,\mathfrak{A}\,|$ sogar den Vorgänger von a, dessen Vorgänger usw. enthalten.

Damit auch hier kein Loop entsteht, müssen diese Elemente natürlich alle verschieden sein. Die Vorgänger von a, a selbst und seine Nachfolger bilden eine Kette, die so angeordnet ist wie die Menge $\mathbb{Z}$ der ganzen Zahlen ($\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$). Deshalb sagt man, dass sie eine so genannte *Z-Kette* bilden, die wie folgt aussieht:

$$\ldots \to \ldots \to \ldots \to a \to \mathbf{S}^{\mathfrak{A}}(a) \to \mathbf{S}^{\mathfrak{A}}(\mathbf{S}^{\mathfrak{A}}(a)) \to \ldots$$

Die Entstehung der Z-Ketten kann man auch mit Hilfe von Äquivalenzklassen erklären: Wenn a und b zwei Elemente aus $|\,\mathfrak{A}\,|$ sind, sind sie äquivalent, wenn die Nachfolgerfunktion endlich oft auf das eine Element angewendet werden kann, um das andere zu ergeben. Dabei handelt es sich um eine Äquivalenzrelation, denn sie ist:

1. reflexiv, weil $\mathbf{S}^0(a) = a$
2. symmetrisch, weil für a,$b \in |\,\mathfrak{A}\,|$ gilt: $\mathbf{S}^x(a) = b \to \mathbf{S}^{-x}(b) = a$
3. transitiv, weil für a, b, $c \in |\,\mathfrak{A}\,|$ gilt: $(\mathbf{S}^x(a) = b \wedge \mathbf{S}^y(b) = c) \to \mathbf{S}^{x+y}(a) = c$

Die Äquivalenzklasse für ein Element a ist die Menge, die man erhält, wenn man $\mathbf{S}^{\mathfrak{A}}$ und die dazu inverse Funktion –nennen wir sie $\mathbf{S}^{-\mathfrak{A}}$– auf $\{a\}$ anwendet. Das Resultat ist dann eine Z-Kette. Die Äquivalenzklasse, die $\mathbf{0}^{\mathfrak{A}}$ enthält, ist der Standardteil von $|\,\mathfrak{A}\,|$. Es gibt beliebig viele Z-Ketten. Je zwei Z-Ketten müssen disjunkt sein, da die Nachfolgerfunktion injektiv ist. Ebenso muss jede Z-Kette disjunkt zum Standardteil sein.

Man kann nun sagen, wie Modelle für A_S beschaffen sein müssen:
Jede Struktur $\mathfrak{B}$ mit dem Standardteil

$$\mathbf{0}^{\mathfrak{B}} \to \mathbf{S}^{\mathfrak{B}}(\mathbf{0}^{\mathfrak{B}}) \to \mathbf{S}^{\mathfrak{B}}(\mathbf{S}^{\mathfrak{B}}(\mathbf{0}^{\mathfrak{B}})) \to \ldots,$$

die einen Nicht-Standardteil hat, der aus beliebig vielen Z-Ketten besteht, ist ein Modell für A_S.

Ausserdem sind zwei Modelle für A_S, die dieselbe Anzahl an Z-Ketten haben, isomorph. Die Anzahl kann dabei beliebig sein. $\mathfrak{R}_S$ besitzt aber keine Z-Ketten, weil man für ein Element aus $\mathbb{N}$ nicht beliebig viele Vorgänger, deren Vorgänger usw. auflisten kann. Nach "links" ist bei $\mathbf{0}$ sozusagen "Schluss".

Es gibt keinen Satz in $\mathfrak{R}_S$ der besagt, dass es keine Z-Ketten gibt. Tatsächlich hat ein Modell $\mathfrak{A}$ von A_S keine Z-Ketten gdw. es keine Menge von Sätzen gibt, die von $\mathfrak{A}$ erfüllt werden. $\mathfrak{A}$ hat aber abzählbar viele Z-Ketten, deshalb gibt es auch eine Menge von Sätzen, die von $\mathfrak{A}$ erfüllt werden.

Zwei nicht abzählbare Modelle $\mathfrak{A}$ und $\mathfrak{B}$ von A_S sind isomorph, wenn sie die gleiche Kardinalität haben. Das bedeutet nämlich, dass sie die gleiche Anzahl an Z-Ketten haben.

Mit Hilfe des Łoś-Vaught Theorems [1] kann man zeigen, dass $Cn\,A_S$ eine vollständige Theorie ist. Wir wissen nun, dass $Cn\,A_S$ vollständig ist, dass $\mathrm{Th}\,\mathfrak{R}_S$ erfüllbar ist und dass $Cn\,A_S \subseteq \mathrm{Th}\,\mathfrak{R}_S$ ist. Alles das ergibt zusammen $Cn\,A_S = \mathrm{Th}\,\mathfrak{R}_S$.

A_S ist eine entscheidbare Menge von Axiomen für $\mathrm{Th}\,\mathfrak{R}_S$. Diese Theorie ist also axiomatisierbar und, wie weiter oben festgestellt wurde, auch vollständig. Somit ist $\mathrm{Th}\,\mathfrak{R}_S$ entscheidbar.

Kapitel 2

Quantorenelimination

Da nun gezeigt wurde, dass $\mathrm{Th}\,\Re_S$ entscheidbar ist, kann man prüfen, ob Quantorenelimination in $\mathrm{Th}\,\Re_S$ möglich ist. Zuerst wird das Verfahren der Quantorenelimination allgemein erläutert und danach auf die Theorie $\mathrm{Th}\,\Re_S$ angewandt.

Es wird auch ein weiterer Anwendungsbereich der Quantorenelimination vorgestellt: die Geometrie. Hier wird nur die Intuition gegeben, und die Quantorenelimination wird an einem Beispiel durchgeführt.

2.1 Allgemeines Verfahren

In einer Theorie $\mathbf{T}$ darf man genau dann Quantoren eliminieren, wenn es für jede Formel φ eine quantorenfreie Formel ψ gibt, sodass gilt

$$\mathbf{T} \models (\varphi \leftrightarrow \psi).$$

Es reicht aus, nur Formeln φ der Form

$$\exists x(\alpha_0 \wedge \ldots \wedge \alpha_n)$$

zu betrachten, bei der jedes α_i eine atomare Formel oder deren Negation ist. Wenn es für jedes dieser φ eine quantorenfreie Formel ψ gibt, sodass $\mathbf{T} \models (\varphi \leftrightarrow \psi)$, darf man die Quantorenelimination in $\mathbf{T}$ durchführen.

2.1.1 Beweis zum allgemeinen Verfahren

Wenn θ quantorenfrei ist, dann wird behauptet, dass man für jede Formel der Gestalt $\exists x\,\theta$ eine quantorenfreie, aber trotzdem äquivalente Formel finden kann. θ wird in disjunktive Normalform gebracht. Es entsteht eine Formel der Form

$$\exists x[(\alpha_0 \wedge \ldots \wedge \alpha_m) \vee (\beta_0 \wedge \ldots \wedge \beta_n) \vee \ldots \vee (\xi_0 \wedge \ldots \wedge \xi_t)].$$

Diese ist logisch äquivalent zu

$$\exists x(\alpha_0 \wedge \ldots \wedge \alpha_m) \vee \exists x(\beta_0 \wedge \ldots \wedge \beta_n) \vee \ldots \vee \exists x(\xi_0 \wedge \ldots \wedge \xi_t).$$

Der Behauptung nach kann man nun jedes Disjunktionsglied dieser Formel wieder durch eine quantorenfreie Formel ersetzen, da es die Form $\exists x(\alpha_0 \wedge \ldots \wedge \alpha_n)$ hat.

Dieses Verfahren kann man sogar auf beliebige Formeln anwenden, da es immer möglich ist, sie in Bestandteile der Form $\exists x(\alpha_0 \wedge \ldots \wedge \alpha_n)$ aufzuteilen. Dazu bringt man die Formel zuerst in Pränexform. Das Ergebnis ist dann von der Bauart $Q_1 y_1 \ldots Q_n y_n F$. Dabei sind die Q_i Quantoren, die y_i Variablen und F ist quantorenfrei. Nun muss man die Allquantoren in Existenzquantoren umwandeln ($\forall x \lambda \leftrightarrow \neg \exists x \neg \lambda$) und die dabei entstehenden Negationen in die Formel F hineinbringen. Dann bringt man F in disjunktive Normalform. Die Existenzquantoren werden vor die einzelnen Disjunktionsglieder geschrieben. Jedes Disjunktionsglied hat nun die geforderte Form.

2.2 Quantorenelimination in $\operatorname{Th} \Re_S$

Wie im allgemeinen Verfahren beschrieben, reicht es aus, Formeln der Gestalt

$$\exists x(\alpha_0 \wedge \ldots \wedge \alpha_q)$$

zu betrachten.

Dabei sei wieder jedes α_i eine atomare Formel oder deren Negation. Es wird gezeigt, dass man eine solche Formel in eine äquivalente quantorenfreie Formel umwandeln kann.

Die einzigen Terme, die es aufgrund der Einschränkungen in $\Re_S$ geben kann, haben die Form $\mathbf{S}^k u$. Hier kann u nur $\mathbf{0}$ oder eine Variable sein. Die einzig möglichen atomaren Formeln sind Gleichungen.

$\exists x(\alpha \wedge \beta)$ wäre tautologisch äquivalent zu $\alpha \wedge \exists x \beta$, wenn x nicht in jedem α_i vorkäme. Daher wird angenommen, dass x in *jedem* α_i vorkommt. Jede atomare Formel α_i muss deshalb entweder die Form

$$\mathbf{S}^m x \approx \mathbf{S}^n u$$

oder die Form

$$\mathbf{S}^m x \not\approx \mathbf{S}^n u$$

haben.

Weiterhin wird davon ausgegangen, dass u verschieden von x ist, da man ansonsten $\mathbf{S}^m x \approx \mathbf{S}^n x$ einfach durch eine Tautologie ersetzen könnte, wenn $m = n$ wäre (denn diese Aussage wäre für jedes x wahr) bzw. durch ein Oxymoron, wenn $m \neq n$ wäre (denn diese Aussage wäre für jedes x falsch). In der Sprache $\Re_S$ drücken wir die Tautologie durch $\mathbf{0} \approx \mathbf{0}$ aus und das Oxymoron durch $\mathbf{0} \not\approx \mathbf{0}$.

Im nun folgenden Teil des Beweises müssen die beiden möglichen Formen für α_i getrennt betrachtet werden:

1. Fall: Jedes α_i ist die Negation einer Gleichung und die Gleichung hat die oben beschriebene Form.

   Dann kann man die gesamte Formel durch $\mathbf{0} \approx \mathbf{0}$ ersetzen, denn man kann immer ein x finden, auf das die Ungleichung zutrifft. Es kommt dann in der gesamten Formel kein x mehr vor, und der Existenzquantor kann weggelassen werden.

2. Fall: Mindestens ein α_i ist nicht negiert. Angenommen, dieses α_i sei α_0 und habe die Form

$$\mathbf{S}^m x \approx t$$

wobei der Term t kein x enthalte.

Die Lösung für x darf nicht negativ sein. Deshalb wird $\mathbf{S}^m x \approx t$ durch

$$t \not\approx \mathbf{0} \wedge \ldots \wedge t \not\approx \mathbf{S}^{m-1}\mathbf{0}$$

ersetzt bzw. durch $\mathbf{0} \approx \mathbf{0}$, wenn $m = 0$ ist (denn man findet immer ein x, das gleich t ist).

Im Falle $m \neq 0$ kann man sich diese Ersetzung folgendermaßen klar machen: $\mathbf{S}^m x \approx t$ wird unwahr, sobald m grösser als t ist. Denn dann findet man kein x mehr, dessen m-ter Nachfolger gleich t ist. Genau dann wird auch $t \not\approx \mathbf{0} \wedge \ldots \wedge t \not\approx \mathbf{S}^{m-1}\mathbf{0}$ unwahr: das $(t+1)$-te Konjunktionsglied ist nämlich gleich t.
Danach wird in jeder anderen atomaren Formel α_j

$$\mathbf{S}^k x \approx u$$

durch

$$\mathbf{S}^{k+m} x \approx \mathbf{S}^m u$$

ersetzt.

Wegen der anfänglichen Annahme, dass α_0 die Form $\mathbf{S}^m x \approx t$ hat, kann man dies auch als

$$\mathbf{S}^k t \approx \mathbf{S}^m u$$

schreiben.
Es ist nun eine Formel entstanden, in der kein x mehr vorkommt. Also kann der Existenzquantor weggelassen werden. Das Resultat ist auch hier eine quantorenfreie Formel.

2.2.1 Ein Nebenprodukt der Quantorenelimination in $\mathrm{Th}\,\Re_S$

Die oben beschriebene Quantorenelimination liefert nebenbei einen weiteren Beweis für die Vollständigkeit von $Cn\,A_S$. Aus einem Satz σ macht die Quantorenelimination einen quantorenfreien Satz τ sodass $A_S \models (\sigma \leftrightarrow \tau)$.

τ besteht aus atomaren Sätzen, Negationen und Implikationen, und daher wird behauptet, dass entweder $A_S \models \tau$ oder $A_S \models \neg\tau$. Ein atomarer Satz muss die Gestalt $\mathbf{S}^k\mathbf{0} \approx \mathbf{S}^l\mathbf{0}$ haben. Wenn $k = l$ ist, ist er ableitbar von A_S, das heisst er ist in $Cn\,A_S$. Wenn $k \neq l$ ist, ist er von A_S widerlegbar. Somit ist seine Negation von A_S ableitbar und in $Cn\,A_S$. Jeder quantorenfreie Satz kann abgeleitet oder widerlegt werden, weil dies auch für jeden atomaren Satz möglich ist. Das begründet die Behauptung und zeigt, dass entweder $A_S \models \sigma$ oder $A_S \models \neg\sigma$.

2.3 Quantorenelimination in der Geometrie

Eine geometrische Aussage wird in einen algebraischen Satz übersetzt. Aus diesem Satz werden lineare oder quadratische Variablen eliminiert, sodass der Existenzquantor, der sie bindet, weggelassen werden kann. Vorhandene Allquantoren werden durch Existenzquantoren ausgedrückt ($\forall x \lambda \leftrightarrow \neg \exists x \neg \lambda$). Wenn der Satz keine Quantoren mehr enthält, wird es sehr viel einfacher zu zeigen, dass er wahr ist.

Die zu beweisende Formel darf aus polynomialen Gleichungen ($f = 0$) und (strengen) polynomialen Ungleichungen ($f \leq 0, f \geq 0$ bzw. $f < 0, f > 0$ und$f \neq 0$) bestehen, die durch logische Operatoren verknüpft werden. f ist ein Polynom mit mehreren Unbekannten und rationalen Koeffizienten.

Wir nehmen an, dass ψ eine quantorenfreie Formel ist, in der die Variable x höchstens mit Grad zwei vorkommt und deuten eine Formel der Art $\exists x(\psi(x, u_1, \ldots, u_n))$ durch $\varphi(u_1, \ldots, u_n)$ an. Dabei ist jedes u_i entweder ein Parameter oder durch einen weiter außen stehenden Quantor gebunden. Wenn u_i durch einen Quantor gebunden ist, wird es mittels wiederholter Anwendung der hier beschriebenen Prozedur eliminiert. Aus φ wird durch Umformungen eine quantorenfreie Formel $\varphi^*(u_1, \ldots, u_n)$ gemacht, in der kein x vorkommt. Über den reellen Zahlen muss dann gelten:

$$\varphi(u_1, \ldots, u_n) \leftrightarrow \varphi^*(u_1, \ldots, u_n).$$

Das kann man auch anders ausdrücken: u_i nehme beliebige Werte $a_1, \ldots, a_n \in \mathbb{R}$ an. Dann ist $\varphi^*(a_1, \ldots, a_n)$ genau dann in $\mathbb{R}$ wahr, wenn ein $b \in \mathbb{R}$ existiert, das $\psi(b, a_1, \ldots, a_n)$ in $\mathbb{R}$ wahr macht.

2.3.1 Beispiel zur Quantorenelimination in der Geometrie

Die folgende Behauptung wird mit Hilfe der Quantorenelimination bewiesen:

Zwei Geraden kreuzen sich in genau einem Punkt.

Dem Beweis liegt folgende Idee zugrunde: Die x-Achse stellt die erste Gerade dar, die zweite Gerade wird durch die lineare Funktion $mx + b$ dargestellt.

Als erstes wird die Behauptung als Formel aufgeschrieben:

$$\exists x(mx + b = 0 \wedge \forall y(y \neq x \rightarrow my + b \neq 0))$$

Alle Quantoren müssen außen stehen, daher wird die Formel in Pränexform gebracht. Die Implikation wird aufgelöst:

$$\exists x \forall y(mx + b = 0 \wedge (y = x \vee my + b \neq 0))$$

Der Allquantor wird in einen Existenzquantor umgewandelt:

$$\exists x \neg \exists y \neg(mx + b = 0 \wedge (y = x \vee my + b \neq 0))$$

Das de Morgansche Gesetz wird auf die äußere Klammer angewandt:

$$\exists x \neg \exists y(\neg(mx + b = 0) \vee \neg(y = x \vee my + b \neq 0))$$

Das de Morgansche Gesetz wird auf die hintere innere Klammer angewandt:

$$\exists x \neg \exists y (\neg (mx + b = 0) \vee (\neg (y = x) \wedge \neg (my + b \neq 0)))$$

Die Negationen werden umgewandelt:

$$\exists x \neg \exists y (mx + b \neq 0 \vee (y \neq x \wedge my + b = 0))$$

Das ist dasselbe wie:

$$\exists x \neg \exists y (mx + b \neq 0 \vee (y \neq x \wedge my = -b))$$

Nun wird $m \neq 0$ zu der Theorie hinzugefügt. Das heisst, dass die zweite Gerade nicht parallel zur x-Achse verlaufen darf. Dann ist die Gleichung $my = -b$ nicht trivial und man kann y durch $\frac{-b}{m}$ ersetzen. Das ergibt:

$$\exists x \neg \exists y (mx + b \neq 0 \vee (-b \neq mx \wedge -b = -b))$$

In der entstandenen Formel kommt kein y mehr vor. Daher kann man $\exists y$ weglassen und die Negation in die Formel "hineinziehen". Danach wird noch zwei mal das de Morgansche Gesetz angewandt. Das ergibt:

$$\exists x (mx + b = 0 \wedge -b = mx \vee -b \neq -b)$$

Der Teil $-b \neq -b$ kann weggelassen werden, da er 0 ergibt und *oder*-verknüpft ist. Das ergibt dann:

$$\exists x (mx + b = 0 \wedge -b = mx)$$

Da $m \neq 0$ gilt und die Gleichung $mx = -b$ nichttrivial ist, darf man x durch $\frac{-b}{m}$ ersetzen:

$$\exists x (-b + b = 0 \wedge -b = -b)$$

In dieser Formel kommt kein x mehr vor. Deshalb kann man auch den letzten Existenzquantor eliminieren und erhält:

$$(-b + b = 0 \wedge -b = -b)$$

Diese Aussage ist offensichtlich wahr. Damit wurde mit Hilfe der Quantorenelimination bewiesen, dass sich zwei Geraden in genau einem Punkt schneiden, wenn sie nicht parallel sind.

Kapitel 3

Zusammenfassung

In dieser Seminararbeit wurde ein Entscheidungsverfahren für spezielle logische Theorien vorgestellt: Die Quantorenelimination.

Im ersten Kapitel wurden Grundlagen zum Umgang mit logischen Theorien vermittelt und die Sprache der natürlichen Zahlen mit Nachfolgern wurde erklärt. Des Weiteren wurde gezeigt, dass die Theorie dieser Sprache entscheidbar ist.

Darauf wurde im zweiten Kapitel aufgebaut. Zuerst wurde hier ein allgemeines Verfahren für die Quantorenelimination in einer Theorie beschrieben und bewiesen. Danach wurde gezeigt, dass man dieses Verfahren auf die Theorie der natürlichen Zahlen mit Nachfolgern anwenden kann. Ein dabei entstehendes "Nebenprodukt" wurde erklärt.

Schliesslich wurde noch eine Intuition davon gegeben, wie man Quantorenelimination in der Geometrie einsetzen kann. Dies wurde an einem Beispiel vorgeführt.

Literaturverzeichnis

[1] Herbert B. Enderton, A Mathematical Introduction to Logic, Academic Press, 1972

[2] Uwe Schöning, Logik für Informatiker, Spektrum Akademischer Verlag, Heidelberg, Berlin, 2000

[3] Dolzmann, Sturm, Weispfenning, A New Approach for Automatic Theorem Proving in Real Geometry, Journal of Automated Reasoning, 1998

[4] Mátyás Sustik, http://www.cs.utexas.edu/users/sustik/quantifier-elimination/qe-slides.pdf