QUANTORENELIMINATION VON $\mathbb{C}$ UND $\mathbb{R}$ NACH KREISEL–KRIVINE

MARTIN ZIEGLER

Ich gebe eine verbesserte Version des Verfahrens in [1].

1. Die komplexen Zahlen

Äquivalenz von Formeln bedeutet Äquivalenz in $\mathbb{C}$.

Lemma 1.1. *Jede quantorenfreie Formel $\phi(\bar{x})$ ist äquivalent zu einer Disjunktion von Formeln der Form*

$$p_1(\bar{x}) \doteq 0 \wedge \cdots \wedge p_m(\bar{x}) \doteq 0 \wedge \neg q(\bar{x}) \doteq 0.$$

Dabei sind die p_i und q Polynome aus $\mathbb{Z}[\bar{x}]$. □

Wir fixieren eine Variable x und verstehen unter dem Grad $\deg(p)$ von p den Grad von p in x. Wenn $p = \sum x^i s_i(\bar{y})$, sei $p \equiv 0$ die Formel $\bigwedge_i s_i \doteq 0$.

Lemma 1.2. *Jede Konjunktion $p_1(x,\bar{y}) \doteq 0 \wedge \cdots \wedge p_m(x,\bar{y}) \doteq 0$ ist äquivalent zu einer Disjunktion von Formeln der Form*

$$\delta(\bar{y}) \wedge p(x,\bar{y}) \doteq 0.$$

Dabei ist δ quantorenfrei und der Grad von p beschränkt durch den größten Grad der p_i.

Beweis. Wir nehmen an, daß die p_i alle ungleich Null sind, und beweisen den Satz durch Induktion über die Summe der Grade der p_i. Sei k der Grad von p_1, der kleinste vorkommende Grad. Wir schreiben $p_1(x,\bar{y}) = x^k s(\bar{y}) + t(x,\bar{y})$ für ein t mit kleinerem Grad als k. Für genügend großes N können wir alle $s^N p_i$ durch p_1 mit Rest dividieren:

$$s^N p_i = f_i p_1 + \bar{p}_i,$$

wobei $\deg(\bar{p}_i) < k$. Dann ist $\bigwedge_{i=1}^m p_i \doteq 0$ äquivalent zur Disjunktion von

$$s \doteq 0 \wedge \big(t \doteq 0 \wedge \bigwedge_{i=2}^{m} p_i \doteq 0\big)$$

und

$$\neg s \doteq 0 \wedge \big(p_1 \doteq 0 \wedge \bigwedge_{i=2}^{m} \bar{p}_i \doteq 0\big)$$

Auf beide Klammerausdrücke können wir Induktion anwenden. □

Folgerung 1.3. *Jede quantorenfreie Formel $\chi(x,\bar{y})$ ist äquivalent zu einer Disjunktion von Formeln der Form*

$$\delta(\bar{y}) \wedge p(x,\bar{y}) \doteq 0 \wedge \neg q(x,\bar{y}) \doteq 0.$$

Datum 23.4.2009.

Skript zur *Logik für Informatiker* SS02.

Lemma 1.4. *Für alle Polynome $p(x,\bar{y})$ und $q(x,\bar{y})$ gibt es eine quantorenfreie Formel $div(p,q)(\bar{y})$, die auf $\bar{c} \in \mathbb{C}$ genau dann zutrifft, wenn $p(x,\bar{c})$ in $\mathbb{C}[x]$ ein Teiler von $q(x,\bar{c})$ ist.*

Beweis. Wenn p das Nullpolynom ist, nimmt man $q \equiv 0$ für $div(p,q)$. Sonst schreiben wir $p = x^k s + t$ und $s^N q = gp + \bar{q}$ wie oben. Dann ist $p(x,\bar{c}) \mid q(x,\bar{c})$ äquivalent zur Disjunktion von

$$s(c) \doteq 0 \wedge t(x,\bar{c}) \mid q(x,\bar{c})$$

und

$$\neg s(c) \doteq 0 \wedge \bar{q}(x,\bar{c}) \equiv 0$$

und die Behauptung folgt durch Induktion über den Grad von p. □

Satz 1.5. *$\mathbb{C}$ hat Quantorenelimination.*

Beweis. Wir müssen zeigen, daß $\exists x\ (p \doteq 0 \wedge \neg q \doteq 0)$ quantorenfrei ist. Das ist aber in algebraisch abgeschlossenen Körpern, für genügend großes N, äquivalent zu $\neg div(p, q^N)$. □

2. Die reellen Zahlen

Äquivalenz von Formeln bedeutet Äquivalenz in $\mathbb{R}$. Man beachte, daß Lemma 1.2 für beliebige Körper, also auch für $\mathbb{R}$, gilt.

Lemma 2.1. *Jede quantorenfreie Formel $\phi(\bar{x})$ ist äquivalent zu einer Disjunktion von Formeln der Form*

$$p_1(\bar{x}) \doteq 0 \wedge \cdots \wedge p_m(\bar{x}) \doteq 0 \wedge q_1(\bar{x}) > 0 \wedge \cdots \wedge q_n(\bar{x}) > 0.$$

Dabei sind die p_i und q_i Polynome aus $\mathbb{Z}[\bar{x}]$. □

Wir fixieren eine Variable x und verstehen unter dem Grad $\deg(p)$ von p den Grad von p in x. Der Grad einer Disjunktion der oben beschriebenen Form ist das Maximum aller $\deg(p_i)$ und $\deg(q_i) + 1$.

Folgerung 2.2. *Jede quantorenfreie Formel ist äquivalent zu einer Disjunktion von Formeln der Form*

$$\delta(\bar{y}) \wedge p \doteq 0 \wedge q_1 > 0 \wedge \cdots \wedge q_n > 0,$$

die höchstens denselben Grad hat.

Beweis. Lemma 1.2. □

Lemma 2.3. *Sei $p(x,\bar{y})$ vom Grad $k \geq 0$ und $\chi(x,\bar{y})$ quantorenfrei. Dann ist $\neg p \equiv 0 \wedge p \doteq 0 \wedge \chi$ äquivalent zu einer quantorenfreien Formel von höchstens dem Grad k.*

Beweis. Durch Induktion über k. Für $k = 0$ ist, ist die Formel $\neg p \equiv 0 \wedge p \doteq 0 \wedge \chi$ immer falsch. Also ist alles klar.

Wenn $k > 0$, schreiben wir $p(x,\bar{y}) = x^k s(\bar{y}) + t(x,\bar{y})$ für ein t mit kleinerem Grad als k. Nach Folgerung 2.2 können wir annehmen, daß χ die Form $r \doteq 0 \wedge \bigwedge_{i=0}^{n} q_i > 0$ hat.

Für genügend großes geradzahliges N dividieren wir $s^N r$ und alle $s^N q_i$ durch p:

$$s^N r = fp + \bar{r}$$
$$s^N q_i = g_i p + \bar{q}_i,$$

wobei $\deg(\bar{r}) < k$ und $\deg(\bar{q}_i) < k$. $\neg p \equiv 0 \wedge p \doteq 0 \wedge \chi$ ist dann äquivalent zur Disjunktion von

$$s \doteq 0 \wedge \big(\neg t \equiv 0 \wedge t \doteq 0 \wedge \chi\big) \tag{1}$$

und

$$\neg s \doteq 0 \wedge \big(p \doteq 0 \wedge \bar{r} \doteq 0 \wedge \bigwedge_{i=1}^{n} \bar{q}_i > 0\big) \tag{2}$$

Das Disjunktionsglied (2) hat schon die gewünschte Form. Wenn in (1) t Null ist, ist (1) immer falsch und wir sind fertig. Sonst können wir Induktion auf die Klammer in (1) anwenden (t in der Rolle von p.). □

Lemma 2.4. *Für jedes Polynom $p(x, \bar{y})$ gibt es eine quantorenfreie Formel $Q_p^+(u, \bar{y})$, die auf a und $\bar{c} \in \mathbb{R}$ genau dann zutrifft, wenn $p(x, \bar{c})$ in einer Umgebung von a rechts von a nur positive Werte annimmt.*

Beweis. Sei k der Grad von p. Setze

$$Q_p^+(u, \bar{y}) = \bigvee_{i=0}^{k} \big(p^{(i)}(u, \bar{y}) > 0 \wedge \bigwedge_{j<i} p^{(j)}(u, \bar{y}) \doteq 0\big)$$

□

Man definiert entsprechend Q_p^-, ${}^+Q_p$ und ${}^-Q_p$.

Lemma 2.5. *Für jede quantorenfreie Formel $\phi(x, \bar{y})$ ist $\exists x \in (a, b)\ \phi$ äquivalent zu einer quantorenfreien Formel $\chi(a, b, \bar{y})$.*

Beweis. Wir beweisen die Behauptung durch Induktion über den Grad k von ϕ. Nach Folgerung 2.2 können wir annehmen, daß für $n > 0$ und nicht–verschwindendes p einer der drei folgenden Fälle vorliegt

$$\phi = q_1 > 0 \wedge \cdots \wedge q_n > 0$$
$$\phi = p \doteq 0$$
$$\phi = p \doteq 0 \wedge q_1 > 0 \wedge \cdots \wedge q_n > 0$$

Wir verwenden die Notation $Q(u)$ für $\bigwedge_{i=1}^n Q_{q_i}(u, \bar{y})^+$.

Sei $Pos(a, b) = Pos(a, b, \bar{y})$ die Formel, die ausdrückt, daß alle q_i in (a, b) nur positive Werte annehmen. $Pos(a, b)$ ist äquivalent zu

$$Q(a) \wedge \bigwedge_{i=1}^{n} \neg\exists x \in (a, b)\ q_i(x) \doteq 0.$$

Aus der Induktionsvoraussetzung folgt also, daß $Pos(a, b)$ äquivalent zu einer quantorenfreien Formel ist.

<u>Fall 1</u>
$\exists x \in (a, b)\ \bigwedge_{i=1}^n q_i > 0$ ist äquivalent zu

$$Q(a) \vee \bigvee_{i=1}^{n} (\exists u \in (a, b)\ q_i(u) \doteq 0 \wedge Q(u))$$

Weil $Q(u)$ impliziert, daß $\neg q_i \equiv 0$, können wir $q_i(u) \doteq 0 \wedge Q(u)$ durch $\neg q_i \equiv 0 \wedge q_i(u) \doteq 0 \wedge Q(u)$ ersetzen. Diese Formel hat aber nach Folgerung 2.3 (o.E.) kleineren Grad als k. Die Behauptung folgt jetzt aus der Induktionsvoraussetzung.

Fall 2
$\exists x \in (a,b)\ p \doteq 0$ ist äquivalent zur Disjunktion der Formeln

$$p \equiv 0$$
$$Q_p^+(a) \wedge {}^-Q_p(b)$$
$$Q_p^-(a) \wedge {}^+Q_p(b)$$
$$Q_p^+(a) \wedge {}^+Q_p(b) \wedge \exists x \in (a,b)\ (p'(x) = 0 \wedge p(x) \leq 0)$$
$$Q_p^-(a) \wedge {}^-Q_p(b) \wedge \exists x \in (a,b)\ (p'(x) = 0 \wedge p(x) \geq 0)$$

Die Formeln sind alle zu quantorenfreien äquivalent. Die letzte Formel zum Beispiel impliziert, daß p nicht konstant ist, wir können also $p'(x) = 0 \wedge p(x) \geq 0$ durch $\neg p' \equiv 0 \wedge p'(x) = 0 \wedge p(x) \geq 0$ ersetzen. Das erlaubt die Anwendung von Folgerung 2.3 und der Induktion.

Wir schreiben $PN(a,b,\bar{y})$ für die quantorenfreie Formel, die ausdrückt, daß $Pos(a,b)$ und $\exists x \in (a,b)\ p \doteq 0$. Beachte, daß diese Formel $\neg q_i \equiv 0$ impliziert.

Fall 3
$\exists x \in (a,b)\ \big(p \doteq 0 \wedge \bigwedge_{i=1}^n q_i > 0\big)$ ist äquivalent zur Disjunktion der Formeln

$$PN(a,b)$$
$$\bigvee_{i=0}^n \exists u \in (a,b)\ (q_i(u) \doteq 0 \wedge PN(u,b))$$
$$\bigvee_{j=0}^n \exists v \in (a,b)\ (q_j(v) \doteq 0 \wedge PN(a,v))$$
$$\bigvee_{i,j=0}^n \exists u \in (a,b)\ \big(q_i(u) \doteq 0 \wedge \exists v \in (u,b)\ (q_j(v) \doteq 0 \wedge PN(u,v))\big)$$

Diese Formeln sind alle zu quantorenfreien Formeln äquivalent. Zum Beispiel die letzte Formel: Weil $PN(u,v)$ impliziert, daß $\neg q_j \equiv 0$, ist $q_j(v) \doteq 0 \wedge PN(u,v)$ zu einer quantorenfreien Formel $\chi_1(u,v)$ von kleinerem Grad als k äquivalent (Folgerung 2.3). Nach Induktion ist $\exists v \in (u,b)\ \chi_1(u,v)$ zu einer quantorenfreien Formel $\chi_2(u,b)$ äquivalent. Weil $\chi_2(u,b)$ impliziert, daß $\neg q_j \equiv 0$, ist $q_i(u) \doteq 0 \wedge \chi_2(u,b)$ zu einer quantorenfreien Formel $\chi_3(u,b)$ vom Grad kleiner als k äquivalent. Induktion liefert, daß $\exists u \in (a,b) \chi_3(u,b)$ quantorenfrei ist. □

Satz 2.6. *$\mathbb{R}$ hat Quantorenelimination.*

Beweis. $\exists x \phi(x)$ ist äquivalent zur Disjunktion der Formeln

$$\exists x \in (-1,1) \phi(x)$$
$$\phi(-1) \vee \phi(1)$$
$$\exists x \in (-1,1)(\neg x \doteq 0 \wedge \phi(x^{-1}))$$

□

Das hier angegebene Quantoreneliminationverfahren ist sehr ineffektiv. In [2] findet man ein Verfahren, das Formeln der Länge n in 2^{2^n} Schritten in eine äquivalente quantorenfreie umwandelt. Man weiß, daß es kein Verfahren gibt, das weniger als 2^n Schritte braucht.

Literatur

[1] Kreisel, Georg und Jean-Louis Krivine: *Modelltheorie. Eine Einführung in die mathematische Logik und Grundlagentheorie*. Springer, 1972.

[2] Specker, Ernst und Volker Strassen (Herausgeber): *Komplexität von Entscheidungsproblemen*, Band 43 der Reihe *Lecture Notes in Computer Science*. Springer, 1976.