LINEARE QUANTORENELIMINATION IN BEWERTETEN KÖRPERN

Thomas Sturm

19. Februar 1995

Eingereicht als Diplomarbeit an der Universität Passau,
Fakultät für Mathematik und Informatik,
Lehrstuhl Prof. Dr. Weispfenning.

Zusammenfassung

Ein Quantoreneliminationsverfahren für eine Theorie über einer Sprache L ist ein Algorithmus, der zu jeder L-Formel erster Stufe eine äquivalente L-Formel berechnet, die keine Quantoren enthält. Diese Arbeit beschäftigt sich mit linearer Quantorenelimination für die Theorie der bewerteten Körper. Dabei bedeutet *linear*, daß die angegebenen Verfahren nur auf Formeln anwendbar sind, in denen die quantifizierten Variablen gewissen Linearitätsbedingungen genügen. Nach einer kurzen Einführung in die Bewertungstheorie stellen wir ein bereits bekanntes Quantoreneliminationsverfahren für lineare Formeln über diskret bewerteten Körpern vor. Dieses wird dahingehend weiterentwickelt, daß Eliminationsmengen angegeben werden, mit denen man uniform über allen diskret bewerteten Körpern eliminieren kann. Ergänzend beschreiben wir ein Eliminationsverfahren für beliebig, also nicht notwendigerweise diskret, bewertete Körper. Es folgt eine Beschreibung von Methoden zur Simplifikation von Formeln in der Bewertungstheorie, die im Zusammenhang mit einer experimentellen Implementierung unseres Verfahrens für den Körper der rationalen Zahlen mit p-adischer Bewertung entwickelt wurden. Abschließend geben wir einige Beispiele für automatisch durchgeführte Eliminationen.

Inhaltsverzeichnis

KAPITEL 1

Bewertete Körper

In diesem einleitenden Kapitel fassen wir die später verwendeten Grundlagen der Bewertungstheorie zusammen. Wir betrachten nur Exponentenbewertungen. Für die Einordnung dieser Bewertungen in die Bewertungstheorie verweisen wir auf [vdW93b]. Eine tiefergehende Einführung in die Bewertungstheorie bietet [End72].

1.1. Bewertungen

Definition 1.1. Sei K ein Körper, Γ eine total geordnete additive abelsche Gruppe. Sei ∞ ein positives unendliches Element bezüglich Γ, d. h., für $\gamma \in \Gamma$ ist $\gamma < \infty$ und $\gamma + \infty = \infty$, und es gilt auch $\infty + \infty = \infty$. Eine Abbildung $v : K \to \Gamma \cup \{\infty\}$ heißt **Bewertung** von K, falls sie die folgenden Bedingungen erfüllt:

(V_1) $v(a) = \infty$ genau dann wenn $a = 0$,
(V_2) $v(ab) = v(a) + v(b)$, und
(V_3) $v(a + b) \geqslant \min \{v(a), v(b)\}$.

Die **Wertegruppe** von K unter der Bewertung v ist definiert als $v(K^\times)$, wobei $K^\times$ die multiplikative Gruppe des Körpers bezeichnet. Wir gehen im folgenden davon aus, daß alle betrachteten Bewertungen surjektiv sind, d. h. $v(K^\times) = \Gamma$.

Definition 1.2. Sei K ein Körper mit Bewertung v. Dann heißt v **diskret**, falls Γ ein minimales Element 1_Γ von positivem Wert enthält. In diesem Fall sind alle $\gamma \in \Gamma$ ganzzahlige Vielfache von 1_Γ.

Die Bedingung (V_2) besagt, daß v ein Homomorphismus von der multiplikativen Gruppe $K^\times$ des Körpers nach Γ ist. Die Bedingungen (V_2) und (V_3) setzen sich auf beliebige Summen und Produkte fort:

$$v\Big(\prod_{i=1}^{n} a_i\Big) = \sum_{i=1}^{n} v(a_i), \quad v\Big(\sum_{i=1}^{n} a_i\Big) \geqslant \min \{\, v(a_i) \mid 1 \leqslant i \leqslant n \,\}.$$

Diese allgemeineren Bedingungen werden im folgenden ebenfalls mit (V_2) und (V_3) bezeichnet. Das folgende Lemma faßt einige grundlegende Eigenschaften von Bewertungen zusammen.

Lemma 1.3. Sei K ein Körper und v eine Bewertung von K.

(1) $v(1) = v(-1) = 0$.
(2) $v(-a) = v(a)$ für $a \in K$.
(3) $v(a/b) = v(a) - v(b)$ für a, $b \in K$ mit $b \neq 0$.
(4) Für a, $b \in K$ mit $v(a) \neq v(b)$ gilt $v(a + b) = \min \{v(a), v(b)\}$.

Beweis. (1) Da v ein Gruppenhomomorphismus von einer multiplikativen in eine additive Gruppe ist, gilt $v(1) = 0$. Aus $v(-1) + v(-1) = v\big((-1)\cdot(-1)\big) = 0$ folgt $v(-1) = 0$.

(2) Aus (V_2) und Teil (1) folgt $v(-a) = v\big((-1)\cdot a\big) = v(-1) + v(a) = v(a)$.

(3) Mit (V_2) erhalten wir $v(b) + v(1/b) = v(b \cdot 1/b) = v(1) = 0$, also $v(1/b) = -v(b)$. Daraus folgt mit (V_2) die Behauptung.

(4) Sei o. B. d. A. $v(a) < v(b)$. Dann ist $v(a+b) \geqslant v(a)$. Andererseits gilt

$$v(a) = v\big((a+b) - b\big) \geqslant \min\big\{v(a+b), v(b)\big\}.$$

Da $v(a) \geqslant v(b)$ widersprüchlich ist, folgt $v(a) \geqslant v(a+b)$, und zusammen $v(a+b) = v(a) = \min\big\{v(a), v(b)\big\}$. □

Für einen Ring R kann man auf natürliche Weise eine Multiplikation zwischen Elementen von R und ganzen Zahlen definieren. Man betrachtet die Multiplikation mit einem $z \in \mathbb{Z}$ als z-fache Addition.

Definition 1.4. Sei R ein Ring. Wir definieren $\odot : \mathbb{Z} \times R \to R$ durch $0 \odot a = 0$, $z \odot a = \sum_{i=1}^{z} a$ für $z > 0$ und $z \odot a = \sum_{i=1}^{|z|} (-a)$ für $z < 0$.

Wenn $R \supseteq \mathbb{Z}$, so ist $\odot$ einfach eine Einschränkung der Multiplikation von R. Diese Beobachtung erlaubt uns, auf die Notation $z \odot a$ zu verzichten und $z \cdot a$ oder einfach za zu schreiben. Offensichtlich gilt für $z \in \mathbb{Z}$ und $a \in R$:

$$v(a^z) = zv(a), \quad v(za) \geqslant v(a).$$

Beispiel 1.5. (1) Jeder Körper erlaubt die *triviale Bewertung* τ, die definiert ist durch $\tau(a) = \infty$ genau dann wenn $a = 0$, und $\tau(a) = 0$ sonst. Jeder endliche Körper erlaubt *nur* die triviale Bewertung: Sei K ein Körper mit $|K| = n$ und v eine Bewertung von K. Dann ist $K^\times$ zyklisch, wird also von einer primitiven $(n-1)$-ten Einheitswurzel ζ erzeugt. Es gilt

$$(n-1)v(\zeta) = v(\zeta^{n-1}) = v(1) = 0,$$

und damit $v(\zeta) = 0$. Für alle $a \in K^\times$ existiert ein $m \in \mathbb{N}$, so daß $a = \zeta^m$, und wir erhalten $v(a) = v(\zeta^m) = mv(\zeta) = 0$.

(2) Für jede Primzahl p erlaubt der Körper der rationalen Zahlen die **p-adische Bewertung** $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$, die definiert ist durch $v_p(0) = \infty$ und

$$v_p(r/s) = \max\big\{\, n \in \mathbb{N} \,\big|\, p^n \mid r \,\big\} - \max\big\{\, n \in \mathbb{N} \,\big|\, p^n \mid s \,\big\} \quad \text{für } r/s \in \mathbb{Q}^\times.$$

Man beachte, daß v_p surjektiv ist, denn für $z \in \mathbb{Z}$ ist $v(p^z) = z$.

(3) Wir betrachten den Körper $F((t))$ der formalen LAURENT-Reihen über einem Grundkörper F. Man definiert für

$$f = \sum_{i=z}^{\infty} a_i t^i \in F((t)), \quad \text{wobei } z \in \mathbb{Z} \text{ und } a_z \neq 0,$$

die *Ordnung* von f als $\operatorname{ord}(f) = z$. Die Ordnung ist eine Bewertung von $F((t))$.

(4) Entsprechend kann kann man auf dem Körper $F((t^*))$ der PUISEUX-Reihen über F eine Ordnung definieren. Für

$$f = \sum_{i=z}^{\infty} a_i t^{i/k} \in F((t^*)), \quad \text{wobei } k \in \mathbb{N},\ z \in \mathbb{Z} \text{ und } a_z \neq 0,$$

ist $\operatorname{ord}(f) = z/k \in \mathbb{Q}$. Auch in diesem Fall ist die Ordnung eine Bewertung.

Die Bewertungen in (1)–(3) sind diskret, die Bewertung in (4) hingegen nicht.

1.2. Induzierte algebraische Strukturen und abstrakte Teilbarkeit

Lemma 1.6. Sei K ein Körper mit Bewertung v. Wir definieren

$$\begin{aligned} R_v &= \{\, a \in K \mid v(a) \geqslant 0 \,\}, \\ U_v &= \{\, a \in K \mid v(a) = 0 \,\}, \\ I_{v,\gamma} &= \{\, a \in K \mid v(a) > \gamma \,\} \quad \text{für jedes } 0 \leqslant \gamma \in \Gamma. \end{aligned}$$

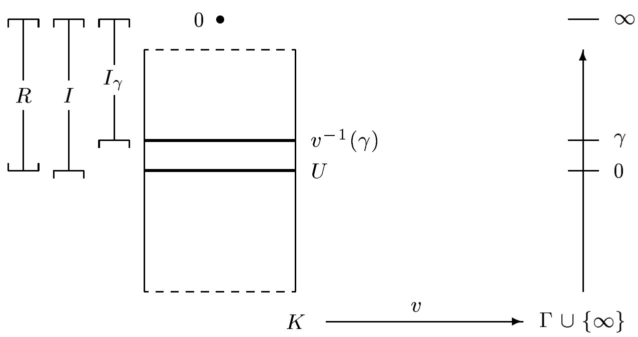
Dann ist R_v ein Unterring von K, U_v enthält genau die Einheiten von R_v, jedes $I_{v,\gamma}$ ist ein Ideal von R_v, $I_{v,0}$ ist ein maximales Ideal von R_v, und zwar das einzige.

Beweis. Man sieht leicht, daß R_v ein Ring ist, und daß die $I_{v,\gamma}$ Ideale sind. Ein $a \in R_v$ ist genau dann Einheit, wenn sein Inverses $a^{-1} \in K$ ebenfalls in R_v liegt, also wenn $v(a) \geqslant 0$ und $-v(a) \geqslant 0$, mit anderen Worten $v(a) = 0$. Das Ideal $I_{v,0}$ ist echt wegen $v(1) = 0$. Sei $J \neq I_{v,0}$ ein beliebiges Ideal von R_v. Dann ist entweder $J \subsetneq I_{v,0}$ und damit nicht maximal, oder J enthält eine Einheit, und damit $J = R_v$. □

Definition 1.7. Für einen gegebenen Körper bezeichnen wir R_v aus Lemma 1.6 als **Bewertungsring** und $I_{v,0}$ als **Bewertungsideal** von v. Im folgenden schreiben wir für $I_{v,0}$ einfach I_v. Da I_v maximal ist, ist der Restklassenring $K_v = R_v/I_v$ ein Körper, der **Resklassenkörper** von v.

Definition 1.8. Für $\gamma \in \Gamma \cup \{\infty\}$ bezeichnen wir das Urbild $v^{-1}(\gamma) \subseteq K$ als **Niveau** γ von K. Falls $a \in v^{-1}(\gamma)$, so sagen wir, daß *a auf dem Niveau γ* liegt.

Das folgende Bild soll die Zusammenhänge zwischen den eingeführten Begriffen veranschaulichen.



Bemerkung 1.9. Bedingung (V_1) besagt, daß auf dem Niveau ∞ nur die 0 liegt. Folgende Überlegung zeigt, daß für eine gegebene Bewertung alle Niveaus außer dem Niveau ∞ gleich mächtig sind: Betrachte ein $\gamma \in \Gamma$. Da wir v als surjektiv vorausgesetzt haben, ist $v^{-1}(\gamma) \subseteq K$ nicht leer. Wir wählen $c \in v^{-1}(\gamma)$ und bilden jedes $u \in U$ auf cu ab. Offensichtlich ist $v(cu) = v(c) + v(u) = \gamma$. Aus $cu = cu'$ folgt $u = u'$, d. h., die Abbildung ist injektiv. Für $c' \in K$ mit $v(c') = \gamma$ gilt $c' = c(c^{-1}c')$, und es ist $v(c^{-1}c') = v(c') - v(c) = 0$, also ist die Abbildung auch surjektiv.

Wir haben gesehen, daß eine Bewertung gewisse algebraische Strukturen im Körper induziert. Außerdem induziert sie in Form der Niveaus eine Partition auf dem Körper. Die induzierten algebraischen Strukturen sind offensichtlich durch die induzierten Niveaus eindeutig bestimmt. Es ist klar, daß sich bei Umbenennung der Elemente der Wertegruppe an den Niveaus und damit an den induzierten algebraischen Strukturen nichts ändert. Diese Überlegung führt uns zum Begriff äquivalenter Bewertungen.

Definition 1.10. Zwei Bewertungen $v : K \to \Gamma \cup \{\infty\}$ und $v' : K \to \Gamma' \cup \{\infty\}$ eines Körpers K heißen **äquivalent**, falls ein Isomorphismus geordneter Gruppen $\varphi : \Gamma \to \Gamma'$ existiert mit $v' = \varphi \circ v$.

$$\begin{tikzcd} \Gamma \arrow[rr, "\varphi"] & & \Gamma' \\ & K^\times \arrow[ul, "v"] \arrow[ur, "v'"'] & \end{tikzcd}$$

Natürlicherweise stellt sich die Frage, ob zwei nicht äquivalente Bewertungen dieselben Niveaus induzieren können. Das ist nicht möglich. In der Tat können sie noch nicht einmal dieselben Bewertungsringe induzieren. Mit anderen Worten: Eine Bewertung ist schon durch Kenntnis der Elemente von nichtnegativem Wert bis auf Äquivalenz eindeutig bestimmt.

Proposition 1.11. *Zwei Bewertungen v und v' von K sind genau dann äquivalent, wenn ihre Bewertungsringe gleich sind.*

Beweis. Die Implikation ist klar. Seien v, v' Bewertungen mit $R_v = R_{v'}$. Die Bewertungen sind Gruppenhomomorphismen auf $K^\times$, und es ist $\operatorname{kern}(v) = U_v = U_{v'} = \operatorname{kern}(v')$. Aus dem Homomorpiesatz folgt, daß

$$\Gamma = v(K^\times) \simeq K^\times / \operatorname{kern}(v) = K^\times / \operatorname{kern}(v') \simeq v'(K^\times) = \Gamma'.$$

Wegen $I_v = I_{v'}$ bildet der Isomorphismus positive Werte surjektiv auf positive Werte ab. Damit ist er ordnungserhaltend. $\square$

Korollar 1.12. Sei K ein Körper, und seien v, v' Bewertungen von K. Dann sind folgende Aussagen äquivalent:

(1) v und v' induzieren dieselben Niveaus,
(2) $R_v = R_{v'}$,
(3) v und v' sind äquivalent. $\square$

Damit kann man bei der Betrachtung von bewertungstheoretischen Problemen von der konkreten Wertegruppe abstrahieren.

Definition 1.13. Sei K ein Körper mit Bewertung v. Wir definieren zweistellige Relationen auf K. Für $a, b \in K$ gilt $a \mid b$, falls $v(a) \leqslant v(b)$. Wir sagen dann a **teilt** b. Falls $a \mid b$ und auch $b \mid a$, so sagen wir, daß a und b **assoziiert** sind und notieren $a \sim b$. Falls $v(a) < v(b)$, so sagen wir a **teilt** b **strikt** und notieren $a \parallel b$.

Offensichtlich ist $\mid$ eine totale Quasiordnung, $\sim$ ist eine Äquivalenzrelation, und $\parallel$ ist der strikte Teil von $\mid$. Bezüglich $\mid$ gibt es ein größtes Element, nämlich die 0. Die von $\sim$ induzierte Partition $K/\sim$ besteht genau aus den bereits definierten Niveaus.

Man sieht leicht, daß für $a, b \in R_v$ genau dann $a \mid b$ gilt, wenn ein $c \in R_v$ existiert mit $ac = b$, also ist $\mid$ eingeschränkt auf den Bewertungsring die Teilbarkeit im üblichen Sinne. Alle drei Relationen sind auf dem ganzen Körper in folgendem Sinne mit der Multiplikation verträglich:

Lemma 1.14. Sei $\varrho \in \{\parallel, \mid, \sim\}$. Für $a, b, c \in K$ mit $c \neq 0$ gilt $a \mathrel{\varrho} b$ genau dann, wenn $ca \mathrel{\varrho} cb$. $\square$

Bemerkung 1.15. Wir wissen aus Proposition 1.11, daß die Bewertung durch den Bewertungsring R_v bis auf Äquivalenz festgelegt ist. Für $a \neq 0$ ist $v(a) \leqslant v(b)$, falls $b/a \in R_v$. Der Beweis der Proposition zeigt, wie man bei bekanntem Bewertungsring eine Wertegruppe und Bewertung konstruieren kann: Man nimmt die Faktorgruppe $K^\times/U_v$, notiert die Multiplikation als $+$ und definiert, daß $aU_v \leqslant bU_v$ genau dann, wenn $b/a \in R_v$.

Beispiel 1.16. Betrachte einen angeordneten Körper $(K,<)$, der ein echter Erweiterungskörper von $(\mathbb{Q},<)$ ist, und setze

$$\begin{aligned} R &= \{\, a \in K \mid \text{es existiert ein } q \in \mathbb{Q} \text{ mit } -|q| < a < |q| \,\}, \\ U &= \{\, a \in K \mid \text{für alle } q \in \mathbb{Q} \text{ mit } q \neq 0 \text{ gilt } -|q| < a < |q| \,\}. \end{aligned}$$

Das heißt, die Elemente von R sind endlich und die Elemente von U sind infinitesimal bezüglich $\mathbb{Q}$. Dann ist R ein Unterring von K, R ist Bewertungsring einer Bewertung, und U ist die Einheitengruppe von R. Man kann die bis auf Äquivalenz eindeutige Bewertung wie in Bemerkung 1.15 konstruieren. Offensichtlich enthält die Wertegruppe $K^\times/U$ beliebig kleine rationale Zahlen, also ist die Bewertung nicht diskret, [Wei84].

1.3. Charakteristik und körpertheoretische Grundlagen

Definition 1.17. Sei R ein Ring. Falls im Sinne der Multiplikation in Definition 1.4 die 0 von R ein natürliches Vielfaches der 1 von R ist, so existiert ein minimales $n \in \mathbb{N}$ mit dieser Eigenschaft. Wir sagen dann, daß R hat die **Charakteristik** n hat, $\operatorname{char}(R) = n$. Falls alle natürlichen Vielfachen der 1 von 0 verschieden sind, so definiert man $\operatorname{char}(R) = 0$.

Ist die Charakteristik eines Körpers nicht 0, so ist sie prim. Nimmt man nämlich an, daß $\operatorname{char}(K) = p_1p_2$ ist, so folgt $(p_1 1)(p_2 1) = (p_1p_2)1 = 0$ und damit $p_1 1 = 0$ oder $p_2 1 = 0$, was der Minimalität von p_1p_2 widerspricht. Offensichtlich gilt für einen Unterring $R \subseteq K$, daß $\operatorname{char}(R) = \operatorname{char}(K)$, also insbesondere $\operatorname{char}(R_v) = \operatorname{char}(K)$. Wir wollen nun untersuchen, wie sich $\operatorname{char}(K_v)$ zu $\operatorname{char}(K)$ verhält.

Lemma 1.18. Sei R ein Ring mit $\operatorname{char}(R) \neq 0$. Sei I ein Ideal in R. Dann gilt $\operatorname{char}(R/I)$ teilt $\operatorname{char}(R)$.

Beweis. Sei $\operatorname{char}(R) = n$ und $\operatorname{char}(R/I) = m$. Dann gilt $n\overline{1} = \overline{n1} = 0$, und da m minimal mit dieser Eigenschaft ist, folgt $m \leqslant n$. Angenommen $m \nmid n$, dann ist $n = sm + r$ mit $0 < r < m$, und es folgt $\overline{r}1 = \overline{sm1} + \overline{r1} = \overline{n}1 = 0$, was der Minimalität von m widerspricht. □

Proposition 1.19. *Wenn* $\operatorname{char}(K) = p \neq 0$, *so ist auch* $\operatorname{char}(K_v) = p$.

Beweis. $\operatorname{char}(K_v) = \operatorname{char}(R_v/I_v)$ teilt $\operatorname{char}(R_v) = \operatorname{char}(K) = p$, und da p prim ist, folgt die Gleichheit. □

Bemerkung 1.20. Damit impliziert $\operatorname{char}(K_v) = 0$, daß $\operatorname{char}(K) = 0$. Das ist die logische Kontraposition von Proposition 1.19. Im Fall $\operatorname{char}(K) = 0$ ist sowohl $\operatorname{char}(K_v) = 0$, als auch $\operatorname{char}(K_v) = p$ für p prim möglich. Wir sprechen in diesem Zusammenhang vom *charakteristikgleichen* oder *charakteristikungleichen Fall.*

Beispiel 1.21. Wir untersuchen den bewerteten Körper $K = F((t))$ der LAURENT-Reihen aus Beispiel 1.5. Wegen $F \subseteq K$ gilt $\mathrm{char}(K) = \mathrm{char}(F)$. Der Bewertungsring R_v ist der Ring der formalen Potenzreihen $F[[t]]$ über F. Das Bewertungsideal I_v besteht aus den Potenzreihen $\sum a_i t^i$ mit $a_0 = 0$. Damit ist $K_v = R_v/I_v = F$, und zusammen folgt $\mathrm{char}(K_v) = \mathrm{char}(K)$. Hier liegt also stets der charakteristikgleiche Fall vor. Im nächsten Abschnitt werden wir sehen, daß die p-adischen Bewertungen von $\mathbb{Q}$ Beispiele für den charakteristikungleichen Fall sind.

Wir fassen einige körpertheoretische Grundlagen zusammen, die wir im Zusammenhang mit K_v verwenden werden. Für eine ausführliche Darstellung verweisen wir auf [vdW93a], §37, §39 und §43.

Sei F ein Körper. Falls $\mathrm{char}(F) = 0$, so ist $\mathbb{Q} \subseteq F$. Falls $\mathrm{char}(F) = p$ für eine Primzahl p, so ist $\mathbb{Z}/p \subseteq F$, und es ist entweder $|F| = p^k$ für ein $k \in \mathbb{N}$, oder $|F|$ ist unendlich.

Betrachten wir den Fall, daß $|F| = p^k$. Die multiplikative Gruppe eines endlichen Körpers ist zyklisch, d. h., $F^\times$ wird von einer primitiven $(p^k - 1)$-ten Einheitswurzel erzeugt. Falls $k > 1$, so ist F durch Adjunktion eines algebraischen Elements ϑ an $\mathbb{Z}/p$ entstanden. Offensichtlich ist dann ϑ die erzeugende Einheitswurzel. Ferner wissen wir, daß ϑ Nullstelle eines Polynoms über $\mathbb{Z}/p$ ist, und falls f über $\mathbb{Z}/p$ von minimalem Grad ist mit $f(\vartheta) = 0$, so ist $\deg(f) = k$ und $F = (\mathbb{Z}/p)(X)/\,\mathrm{Id}(f)$, wobei $(\mathbb{Z}/p)(X)$ den rationalen Funktionenkörper über $(\mathbb{Z}/p)$ bezeichnet. Es folgt

$$F = \left\{\, a_0 + a_1\vartheta + \cdots + a_{k-1}\vartheta^{k-1} \;\middle|\; (a_0, \ldots, a_{k-1}) \in (\mathbb{Z}/p)^k \,\right\}.$$

Damit bildet F einen Vektorraum der Dimension k über $\mathbb{Z}/p$.

Im Fall $|F|$ unendlich ist F ein Erweiterungskörper von $(\mathbb{Z}/p)(X)$. Dabei ist X transzendent über $\mathbb{Z}/p$, d. h., für jedes Polynom f über $\mathbb{Z}/p$ gilt $f(X) \neq 0$, und damit folgt sofort auch $f(X) \notin \mathbb{Z}/p$.

1.4. Die p-adischen Bewertungen der rationalen Zahlen

Wir wollen die in Beispiel 1.5 eingeführten p-adischen Bewertungen der rationalen Zahlen genauer untersuchen. Zunächst illustrieren wir am Beispiel dieser Bewertungen noch einmal die in Definition 1.7 eingeführten Begriffe des Bewertungsrings, des Bewertungsideals und des Restklassenkörpers einer Bewertung. Dazu benötigen wir folgendes Lemma, das [Mah81] entnommen ist.

Lemma 1.22. Sei $r/s \in \mathbb{Q}$ vollständig gekürzt, und sei p eine Primzahl so daß $p \nmid s$. Dann existierten $m, r' \in \mathbb{Z}$ so daß $r/s = m + pr'/s$.

Beweis. Da p prim ist und $p \nmid s$, gilt $\mathrm{ggT}(p, s) = 1$, und damit existieren $x, y \in \mathbb{Z}$ so daß $sx + py = 1$. Es folgt $sxr + pyr = r$. Setzt man $m = xr$ und $r' = yr$, so erhält man $sm + pr' = r$ und damit $r/s = m + pr'/s$. □

Wir werden auch den ersten Isomorphiesatz für Ringe verwenden, den wir an dieser Stelle der Vollständigkeit halber zitieren. Ein Beweis findet sich z. B. in [BWK93].

Satz 1.23 (Erster Isomorphiesatz). *Sei R ein Ring, S ein Unterring von R und I ein echtes Ideal von R. Dann ist $S \cap I$ ein echtes Ideal von S, $S + I$ ist ein Unterring von R mit $I \subseteq S + I$, und $S/(S \cap I) \simeq (S + I)/I$.* □

Beispiel 1.24. Betrachten wir den Körper $\mathbb{Q}$ der rationalen Zahlen. Für eine Primzahl p sei v die p-adische Bewertung aus Beispiel 1.5. Der Bewertungsring von v ist der PRÜFER-Ring

$$R_v = \mathbb{Z}_p = \left\{\, r/s \in \mathbb{Q} \;\middle|\; \mathrm{ggT}(r, s) = 1 \text{ und } p \nmid s \,\right\}.$$

Offensichtlich ist $\mathbb{Z}_p$ ein Oberring von $\mathbb{Z}$ in $\mathbb{Q}$. Das Bewertungsideal von v und die Einheitengruppe von $\mathbb{Z}_p$ sind gegeben durch

$$I_v = p\mathbb{Z}_p = \{\, r/s \in \mathbb{Q} \mid \operatorname{ggT}(r,s) = 1 \text{ und } p \mid r \,\}$$

und $U_v = \mathbb{Z}_p \setminus p\mathbb{Z}_p = \{\, r/s \in \mathbb{Q} \mid \operatorname{ggT}(r,s) = 1,\, p \nmid r \text{ und } p \nmid s \,\}$. Wir wenden uns nun dem Restklassenkörper von v zu. Man sieht leicht, daß $\mathbb{Z} \cap p\mathbb{Z}_p = p\mathbb{Z}$. Nach Lemma 1.22 gilt $\mathbb{Z} + p\mathbb{Z}_p \supseteq \mathbb{Z}_p$, woraus zusammen mit der offensichtlichen Beziehung $\mathbb{Z} + p\mathbb{Z}_p \subseteq \mathbb{Z}_p$ folgt, daß $\mathbb{Z} + p\mathbb{Z}_p = \mathbb{Z}_p$. Also können wir den ersten Isomorphiesatz anwenden und erhalten

$$K_v = R_v/I_v = \mathbb{Z}_p/p\mathbb{Z}_p = (\mathbb{Z} + p\mathbb{Z}_p)/p\mathbb{Z}_p \simeq \mathbb{Z}/(\mathbb{Z} \cap p\mathbb{Z}_p) = \mathbb{Z}/p\mathbb{Z}.$$

Man sieht leicht, daß $0, 1, \ldots, p-1 \in \mathbb{Z}_p$ paarweise nicht kongruent modulo $p\mathbb{Z}_p$ sind. Also besteht der Restklassenkörper $\mathbb{Z}_p/p\mathbb{Z}_p$ aus den p Äquivalenzklassen $p\mathbb{Z}_p$, $1 + p\mathbb{Z}_p, \ldots, (p-1) + p\mathbb{Z}_p$.

Der folgende Satz von OSTROWSKI besagt, daß es im wesentlichen keine anderen Bewertungen der rationalen Zahlen als die bereits betrachteten p-adischen Bewertungen gibt, und daß diese für verschiedene Primzahlen paarweise nicht äquivalent sind.

Satz 1.25 (Ostrowski). *Jede nicht triviale Bewertung von $\mathbb{Q}$ ist äquivalent zu einer p-adischen Bewertung für genau eine Primzahl p.*

Beweis. Sei v eine Bewertung von $\mathbb{Q}$. Wegen $1 \in R_v$ folgt $\mathbb{Z} \subseteq R_v$. Das Bewertungsideal I_v ist prim, da es maximal ist. Damit ist $\mathbb{Z} \cap I_v$ ein Primideal von $\mathbb{Z}$, also entweder $\mathbb{Z} \cap I_v = \{0\}$ oder $\mathbb{Z} \cap I_v = p\mathbb{Z}$ für eine Primzahl p. Im ersten Fall sieht man leicht, daß $v(a) = 0$ für alle $a \in \mathbb{Q}^\times$, d. h., v ist die triviale Bewertung. Sonst gilt $R = \mathbb{Z}_p$:

Wir zeigen zunächst $R_v \subseteq \mathbb{Z}_p$. Sei $r/s \in R_v$ mit $\operatorname{ggT}(r,s) = 1$. Dann ist $v(r) \geqslant v(s)$. Angenommen $p \mid s$, dann ist $v(s) > 0$, also auch $v(r) > 0$, und damit gilt $p \mid r$, was $\operatorname{ggT}(r,s) = 1$ widerspricht.

Schließlich gilt auch $\mathbb{Z}_p \subseteq R_v$. Sei nämlich $r/s \in \mathbb{Z}_p$ mit $\operatorname{ggT}(r,s) = 1$. Dann gilt $p \nmid s$, also $s \in \mathbb{Z} \setminus p\mathbb{Z} \subseteq R_v \setminus I_v$, somit $v(s) = 0$. Andererseits wissen wir $r \in \mathbb{Z} \subseteq R_v$, also $v(r) \geqslant 0$. Es folgt $v(r/s) \geqslant 0$, und somit $r/s \in R_v$. □

KAPITEL 2

Eliminationsverfahren für diskrete Bewertungen

In diesem Kapitel betrachten wir ausschließlich diskret bewertete Körper. Wir legen die Sprache der Körper zugrunde. Diese erweitern wir um zweistellige Relationssymbole $\neq$, $\|$, $|$, $\sim$ und zwei zusätzliche Konstanten π und ζ.

Wir interpretieren 0^{-1} durch 0, was aber für das Verfahren keine Rolle spielt. Die Relationssymbole sind bezüglich v wie in Definition 1.13 interpretiert. Die Konstante π ist durch ein Körperelement von minimalem positivem Wert interpretiert, also $v(\pi) = 1_\Gamma$. Falls $|K_v| = p^k$, so ist ζ derart interpretiert, daß $\overline{\zeta}$ eine primitive $(p^k - 1)$-te Einheitswurzel ist. Falls $\mathrm{char}(K_v)$ endlich, aber $|K_v|$ unendlich, so ist ζ derart, daß $\overline{\zeta}$ transzendent über $\mathbb{Z}/p$ ist. Falls $\mathrm{char}(K_v) = 0$, so ist $\zeta = 2$.

Im folgenden gehen wir davon aus, daß alle Terme von der Form p oder p/q für distributiv dargestellte Polynome p und q sind. Ein Term t heißt **linear** in einer Menge L von Variablen, falls in dieser Darstellung keine Variable aus L in q vorkommt und in p der Totalgrad in diesen Variablen höchstens 1 ist. Eine quantorenfreie Formel heißt linear in L, falls alle enthaltenen Terme linear in L sind, und entsprechend setzen wir die Definition auf Mengen von Termen und Mengen von quantorenfreien Formel fort. Wenn wir sagen, daß etwas linear in einer Variable X ist, so meinen wir linear in $\{X\}$. Eine pränexe Formel heißt linear, falls ihre Matrix linear in der Menge der quantifizierten Variablen ist.

Die in diesem Kapitel vorgestellten Verfahren eliminieren die Quantoren einer linearen pränexen Formel. Die Forderung, daß die Ausgangsformel pränex sein muß, ist keine Einschränkung, da man zu jeder Formel eine äquivalente pränexe Formel berechnen kann. Tatsächlich ist das noch nicht einmal notwendig: Eine quantifizierte Formel enthält stets eine pränexe Subformel, das gilt insbesondere auch nach der Elimination eines pränexen Quantorenblocks, sofern noch Quantoren vorhanden sind. Offensichtlich ist es korrekt, quantifizierte Subformeln durch quantorenfreie Äquivalente zu ersetzen.

2.1. Elimination durch Eliminationsmengen

Definition 2.1. Für eine quantorenfreie Formel φ bezeichnen wir mit $L_X(\varphi)$ die Menge aller endlichen Variablenmengen L mit $X \in L$ und φ linear in L. Wir sagen eine quantorenfreie Formel ψ ist **linear** in $L_X(\varphi)$, falls ψ linear in allen Variablenmengen aus $L_X(\varphi)$ ist, mit anderen Worten, falls $L_X(\varphi) \subseteq L_X(\psi)$. Mit $A(\varphi)$ bezeichnen wir die Menge aller in φ enthaltenen atomaren Formeln und mit $A_X(\varphi)$ die Menge all derer, in denen die Variable X vorkommt. Mit pr_1 und pr_2 bezeichnen wir die erste bzw. zweite Projektion eines kartesischen Produkts.

Falls ψ linear in $L_X(\varphi)$ ist, so kann man intuitiv sagen, daß ψ bezüglich der Variablenmengen, die X enthalten, *mindestens so linear* wie φ ist. Die Definition von L_X läßt sich in natürlicher Weise auf Mengen Φ von atomaren Formeln übertragen. Ebenso ist klar, wann ein Term linear in $L_X(\varphi)$ oder $L_X(\Phi)$ ist.

Definition 2.2. Sei φ eine quantorenfreie Formel, die linear in X ist. Sei E eine endliche Menge von Termen, die X nicht enthalten und linear in $L_X(\varphi)$ sind. Falls

$$\exists X(\varphi) \longleftrightarrow \bigvee_{t\in E} \varphi[X/t]$$

gilt, so heißt E eine **Eliminationsmenge** für $\exists X(\varphi)$. Entsprechend heißt E eine Eliminationsmenge für $\forall X(\varphi)$ falls $\forall X(\varphi) \longleftrightarrow \bigwedge_{t\in E} \varphi[X/t]$ gilt.

Bemerkung 2.3. Offensichtlich gilt für jede Menge T von Termen, in denen X nicht vorkommt, daß $\bigvee_{t\in T} \varphi[X/t] \longrightarrow \exists X(\varphi)$ und $\forall X(\varphi) \longrightarrow \bigwedge_{t\in T} \varphi[X/t]$. Für den Beweis, daß eine gegebene Menge eine Eliminationsmenge ist, genügt es daher, die jeweils andere Richtung der entsprechenden Äquivalenz in Definition 2.2 zu überprüfen.

Wenn man in der Lage ist, für jede gegebene quantorenfreie Formel φ und lineare Variable X algorithmisch Eliminationsmengen für $\exists X(\varphi)$ und $\forall X(\varphi)$ zu bestimmen, so hat man ein Quantoreneliminationsverfahren für lineare pränexe Formeln: Sei nämlich L die Menge der quantifizierten Variablen, dann ist nach Definition die Eliminationsmenge für den innersten Quantor linear in L. Damit ist auch das Ergebnis der Substitution der Eliminationsterme in die Matrix linear in L, und somit kann man alle Variablen sukzessive von innen nach außen eliminieren. Wir haben den folgenden Algorithmus verifiziert:

Algorithmus 2.4. *Eingabe:* Eine lineare pränexe Formel $Q_1X_1 \dots Q_nX_n(\varphi)$. *Ausgabe:* Eine äquivalente quantorenfreie Formel φ'. *Verwendete Subalgorithmen:* Berechnung einer Eliminationsmenge. *Methode:*

$\langle$*Berechne eine quantorenfreie Formel* φ' *mit* $\varphi' \longleftrightarrow Q_1X_1 \dots Q_nX_n(\varphi)\rangle \equiv$
  $\langle$*Initialisierung* 2.29$\rangle$
  $\varphi' := \varphi$
  for $i := n$ **downto** 1 **do**
    $\langle$*Berechne eine Eliminationsmenge* E *für* $Q_iX_i(\varphi')$ 2.13, 2.46$\rangle$
    if $Q_i = \exists$ **then** $\varphi' := \bigvee_{t\in E} \varphi'[X/t]$ **else** $\varphi' := \bigwedge_{t\in E} \varphi'[X/t]$ **fi**
  od
  $\langle$*Berechne zusätzliche Ausgaben* 2.29$\rangle$

Betrachten wir den Fall, daß in der Eingabeformel von Algorithmus 2.4 zwei Quantoren desselben Typs aufeinanderfolgen, etwa zwei Existenzquantoren. Nach Elimination des ersten entsteht eine Formel der Form $\exists X(\bigvee \Phi)$. Man kann nun, statt einfach zu iterieren, den Quantor in die Disjunktion ziehen und alle Äste unabhängig voneinander eliminieren. Das hat den Vorteil, daß Eliminationsterme, die für die Elimination des Quantors in einem gewissen Disjunktionsglied notwendig sind, nicht in andere Disjunktionsglieder substituiert werden. Für rein existentiell oder rein universell quantifizierte Probleme verbessern sich Zeit- und Platzkomplexität durch diese *blockweise Elimination* um eine Größenordnung. Eine Untersuchung der Komplexität des Verfahrens findet sich in [Wei88].

Für das Finden von Eliminationsmengen ist es oft instruktiv, davon auszugehen, daß die Formel eine gewisse Form hat. Wir werden z. B. verlangen, daß die quantifizierte Variable nur mit gewissen Relationen vorkommt. Solche Einschränkungen sind nicht wesentlich, solange man in der Lage ist, jede lineare Formel ohne Einführung neuer Quantoren und ohne Zerstörung von Linearitätseigenschaften in die entsprechende Form zu bringen.

Lemma 2.5. Gegeben sei für $Q \in \{\exists, \forall\}$ eine lineare Formel $QX(\varphi)$ mit φ quantorenfrei. Sei ψ quantorenfrei mit $\psi \longleftrightarrow \varphi$, und ψ sei linear in $L_X(\varphi)$. Falls dann E eine Eliminationsmenge für $QX(\psi)$ ist, so ist E auch eine Eliminationsmenge für $QX(\varphi)$.

Beweis. Aus $\varphi \longleftrightarrow \psi$ folgt $\exists X(\varphi) \longleftrightarrow \exists X(\psi)$ und $\varphi[X/t] \longleftrightarrow \psi[X/t]$ für einen beliebigen Term t. Damit ist $\exists X(\varphi) \longleftrightarrow \exists X(\psi) \longleftrightarrow \bigvee_{t \in E} \psi[X/t] \longleftrightarrow \bigvee_{t \in E} \varphi[X/t]$. Den Fall $Q = \forall$ zeigt man analog. $\square$

Bemerkung 2.6. Die Eliminationsmengen, die wir für Formeln $QX(\varphi)$ angeben, werden stets Linearkombinationen von Subtermen einer Formel ψ wie in Lemma 2.5 sein. Daraus folgt sofort, daß sie linear in $L_X(\varphi)$ sind. Wir werden das an entsprechender Stelle nicht mehr explizit erwähnen.

2.2. Skolemmengen

Eliminationsmengen wurden von Weispfenning in Form von *Skolemmengen* eingeführt, [Wei88]. Dabei wird für die Elimination von $QX(\varphi)$ von der booleschen Struktur der Matrixformel φ abstrahiert. Die Skolemmenge enthält für jede Belegung von X einen Term, der das Verhalten aller atomaren Formeln für diese Belegung simuliert:

Definition 2.7. Sei Φ eine endliche Menge von atomaren Formeln, die linear in X ist. Sei S eine endliche Menge von Termen, die X nicht enthalten und linear in $L_X(\Phi)$ sind. Falls dann

$$\forall X\big(\bigvee_{t \in S} \bigwedge_{\alpha \in \Phi} (\alpha \longleftrightarrow \alpha[X/t])\big)$$

gilt, so heißt S eine **Skolemmenge** für Φ und X.

Die Begriffsbildung geht zurück auf die bekannte *Skolemisierung*, bei der zu einer gegebenen quantifizierten Formel eine *erfüllbarkeitsgleiche* quantorenfreie Formel in einer Erweiterungssprache konstruiert wird. Beim Skolemisieren wird für das Auflösen eines Existenzquantors unter Erweiterung der Sprache ein Term konstruiert, der falls die Matrix erfüllbar ist, durch ein erfüllendes Element interpretiert werden kann. Bei der Elimination eines Existenzquantors mit Skolemmengen hingegen probiert man genügend viele Terme über der gegebenen Sprache disjunktiv aus. Man beachte, daß wir die Quantoren im Gegensatz zur Skolemisierung von innen nach außen abarbeiten

Lemma 2.8. Sei φ eine quantorenfreie Formel, X linear in φ, und sei S eine Skolemmenge für $A_X(\varphi)$ und X. Dann ist S eine Eliminationsmenge sowohl für $\exists X(\varphi)$, als auch für $\forall X(\varphi)$.

Beweis. Wir zeigen zunächst, daß S Eliminationsmenge für $\exists X(\varphi)$ ist: Falls X in einer atomaren Formel α nicht vorkommt, so gilt offensichtlich $\forall X(\alpha \longleftrightarrow \alpha[X/t])$ für jeden Term t. Daher ist S eine Skolemmenge für $A(\varphi)$ und X. Da φ quantorenfrei, also eine boolesche Kombination seiner atomaren Formeln ist, folgt

$$\forall X\big(\bigvee_{t \in S} (\varphi \longleftrightarrow \varphi[X/t])\big) \quad \text{und damit} \quad \forall X\big(\varphi \longrightarrow \bigvee_{t \in S} \varphi[X/t]\big).$$

Sei β eine Belegung aller Variablen außer X. Gelte $\beta \models \exists X(\varphi)$, und sei etwa $a \in K$ ein erfüllendes Element, d. h., für die Fortsetzung β_a von β, die X durch a interpretiert, gilt $\beta_a \models \varphi$. Dann gilt $\beta_a \models \bigvee_{t \in S} \varphi[X/t]$, und da X nicht mehr vorkommt auch $\beta \models \bigvee_{t \in S} \varphi[X/t]$, was zu zeigen war. Da S auch Skolemmenge für $\exists X(\neg\varphi)$ ist, folgt $\forall X(\varphi) \longleftrightarrow \neg\exists X(\neg\varphi) \longleftrightarrow \neg \bigvee_{t \in S} \neg\varphi[X/t] \longleftrightarrow \bigwedge_{t \in S} \varphi[X/t]$. $\square$

In der Arbeit von Weispfenning [Wei88] sind bereits Skolemmengen für lineare Formeln in diskret bewerteten Körpern angegeben. Diese wollen wir in diesem Abschnitt vorstellen. Die Arbeit beschränkt sich auf die Fälle $\mathrm{char}(K_v) = 0$ und $|K_v|$ endlich.

Man zieht sich zunächst auf Formeln zurück, in denen alle atomaren Formeln, die die quantifizierte Variable X enthalten, $\parallel$ als Relation haben, wobei X nur auf einer Seite vorkommt, und zwar mit dem Koeffizienten 1. Wir wollen solche Formeln als **gut eliminierbar** bezeichnen.

Lemma 2.9. Es gelten folgende Äquivalenzen:

$$\begin{aligned} t \neq 0 &\longleftrightarrow t \parallel 0, & t = 0 &\longleftrightarrow \neg(t \parallel 0), \\ s \mid t &\longleftrightarrow \neg(t \parallel s), & s \sim t &\longleftrightarrow \neg(t \parallel s) \wedge \neg(s \parallel t). \quad \square \end{aligned}$$

Da in obigem Lemma in den atomaren Formeln auf beiden Seiten der einzelnen Äquivalenzen jeweils dieselben Terme vorkommen, sind diese atomaren Formeln jeweils linear in denselben Variablenmengen.

Lemma 2.10. Seien $s, t, u \in K$, und bezeichne φ die Aussage $v(s)+v(t) < v(s+u)$. Im Fall $v(t) \geqslant 0$ ist φ äquivalent zu $v(tu) < v(s+u)$. Falls hingegen $v(t) < 0$, so ist φ äquivalent zu $v(s) + v(t) < v(u)$.

Beweis. Sei zunächst $v(t) \geqslant 0$. Sowohl aus φ als auch aus $v(tu) < v(s+u)$ folgt dann wegen der starken Dreiecksungleichung $v(s) = v(u)$, womit die Äquivalenz klar ist. Sei nun $v(t) < 0$. Wir zeigen zunächst die Kontraposition der Implikation: Sei $v(s) + v(t) \geqslant v(u)$. Dann folgt $v(s) > v(u)$, also $v(u) = v(s+u)$ und zusammen $v(s) + v(t) \geqslant v(s+u)$. Die Replikation folgt wegen $v(s+u) \geqslant \min\{v(s), v(u)\}$. $\square$

Lemma 2.11. Seien $a \neq 0$, $a' \neq 0$, b, b', $x \in K$, und φ bezeichne die Aussage $v(ax+b) < v(a'x+b')$. Falls $v(a) \geqslant v(a')$, so ist φ äquivalent zu

$$v\bigl(a/a'(b'/a' - b/a)\bigr) < v(x + b'/a').$$

Falls $v(a) < v(a')$, so gilt φ genau dann, wenn $v(x + b/a) < v\bigl(a'/a(b'/a' - b/a)\bigr)$.

Beweis. φ ist äquivalent zu $v(x + b/a) + v(a/a') < v\bigl((x + b/a) + (b'/a' - b/a)\bigr)$. Wende nun Lemma 2.10 an. $\square$

Korollar 2.12. Unabhängig von der Definition von 0^{-1} gilt folgende Äquivalenz:

$$\begin{aligned} aX + b \parallel a'X + b' \longleftrightarrow\ & (a = 0 \wedge a' = 0 \wedge b \parallel b') \vee \\ & (a = 0 \wedge a' \neq 0 \wedge b/a' \parallel X + b'/a') \vee \\ & (a \neq 0 \wedge a' = 0 \wedge X + b/a \parallel b'/a) \vee \\ & \bigl(a \neq 0 \wedge a' \neq 0 \wedge a' \mid a \wedge a/a'(b'/a' - b/a) \parallel X + b'/a\bigr) \vee \\ & \bigl(a \neq 0 \wedge a' \neq 0 \wedge a \parallel a' \wedge X + b/a \parallel a'/a(b'/a' - b/a)\bigr). \end{aligned}$$

Ferner ist die rechte Seite der Äquivalenz linear in $L_X(aX + b \parallel a'X + b')$. $\square$

Tatsächlich sind in der Äquivalenz des obigen Korollars die Mengen L_X von linker und rechter Seite gleich. Man beachte ferner, daß es hier entscheidend ist, nur Variablenmengen zu betrachten, in denen X vorkommt. Sei etwa a eine Variable, die in b, a' und b' nicht vorkommt, so ist $aX + b \parallel a'X + b'$ linear in a, nicht aber die linke Seite der Äquivalenz.

Aus dem bisher Gesagten folgt, daß es für die Elimination der Quantoren einer pränexen linearen Formel genügt, Skolemmengen für gut eliminierbare Formeln bestimmen zu können.

Algorithmus 2.13. *Eingabe:* Eine lineare pränexe Formel. *Ausgabe:* Eine äquivalente quantorenfreie Formel. *Verwendete Subalgorithmen:* Berechnung einer Skolemmenge für gut eliminierbare atomare Formeln. *Methode:* Ergänze Algorithmus 2.4 durch folgenden Subalgorithmus:

⟨*Berechne eine Eliminationsmenge E für $QX(\varphi)$*⟩ ≡
  Konstruiere $A_X(\varphi)$
  Berechne $A_X(\psi)$ für ein gut eliminierbares $\psi \longleftrightarrow \varphi$ mit ψ linear in $L_X(\varphi)$
  ⟨*Berechne eine Skolemmenge E für $A_X(\psi)$ und X* 2.20⟩

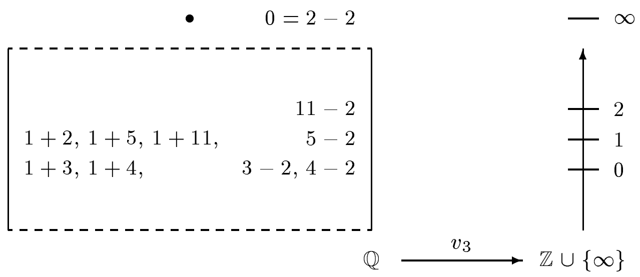
Beweis. Man berechnet $A_X(\psi)$ unter Verwendung der Äquivalenzen in Lemma 2.9 und Korollar 2.12 direkt aus $A_X(\varphi)$, d. h., ψ muß überhaupt nicht konstruiert werden. Nach Lemma 2.8 ist E eine Eliminationsmenge für $QX(\psi)$ und damit nach Lemma 2.5 auch eine Eliminationsmenge für $QX(\varphi)$. □

Die Beweise für alle hier vorgestellten Eliminationsmengen nutzen auf vielfältige Weise die Dreiecksungleichung aus. Der folgende Sachverhalt spielt eine zentrale Rolle.

Lemma 2.14. Sei $a \in K$, $C \subseteq K$ endlich, $c_0 \in C$ derart, daß $v(a + c_0)$ maximal unter allen $v(a + c)$ für $c \in C$. Dann gilt für $c \in C$, daß $v(c - c_0) \geqslant v(a + c)$, und falls $v(a + c) < v(a + c_0)$, so gilt sogar $v(c - c_0) = v(a + c)$.

Beweis. $v(c - c_0) = v\big(a + c - (a + c_0)\big) \geqslant \min\big\{v(a + c), v(a + c_0)\big\} = v(a + c)$, und man sieht, daß im Fall $v(a + c) < v(a + c_0)$ sogar Gleichheit gilt. □

Beispiel 2.15. Betrachte $\mathbb{Q}$ mit der 3-adischen Bewertung v_3. Setze $a = 1$ und $C = \{2, 3, 4, 5, 11\}$, wähle $c_0 = 2$.

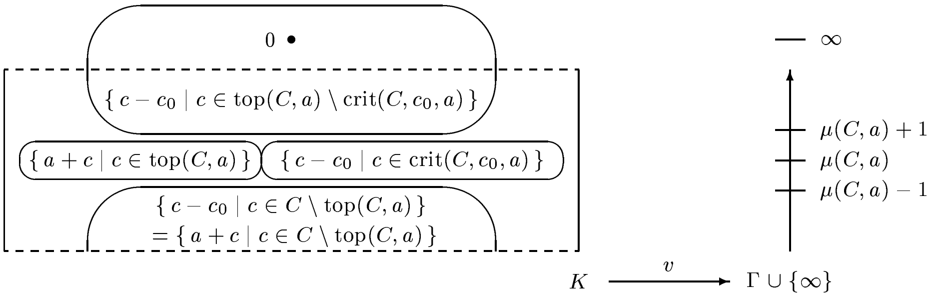


Definition 2.16. Betrachte eine endliche Menge $C \subseteq K$. Für $a \in K$ definiere $\mu(C, a) = \max\left\{\, v(a + c) \;\middle|\; c \in C \,\right\}$. Setze damit

$$\begin{aligned} \operatorname{top}(C, a) &= \left\{\, c \in C \;\middle|\; v(a + c) = \mu(C, a) \,\right\}, \\ \operatorname{crit}(C, c_0, a) &= \left\{\, c \in \operatorname{top}(C, a) \;\middle|\; v(c - c_0) = \mu(C, a) \,\right\} \quad \text{für jedes } c_0 \in \operatorname{top}(C, a). \end{aligned}$$

Für $c_0 \in \operatorname{top}(C, a)$ heißt (a, c_0) **kritisch**, falls $-a \notin C$ und $\operatorname{crit}(C, c_0, a) \neq \emptyset$, und a heißt kritisch, falls (a, c_0) kritisch für ein c_0. Wir wollen sagen, daß eine endliche Menge $S \subseteq K$ **gute Kongruenzeigenschaften** bezüglich C hat, falls für jedes kritische (a, c_0) ein $s \in S$ existiert, so daß $v(s + c_0) = \mu(C, a)$ und $v(s + c) = \mu(C, a)$ für alle $c \in \operatorname{crit}(C, c_0, a)$.

In Beispiel 2.15 ist $\operatorname{crit}(C, c_0, a) \neq \emptyset$. Es wird leer, wenn man die 5 aus C streicht. Das folgende Bild soll die Definitionen von top und crit veranschaulichen. Hier ist $-a \notin C$, denn sonst wäre $\mu(C, a) = 0$.



Es ist für die Theorie unerheblich, ob die beiden Mengen auf Niveau $\mu(C, a)$ disjunkt sind oder nicht. Tatsächlich ist, selbst wenn $\operatorname{crit}(C, c_0, a)$ nicht leer ist, beides möglich: In Beispiel 2.15 sind sie nicht disjunkt, würde man dort jedoch $c_0 = 11$ wählen, so wären sie disjunkt.

Lemma 2.17. Seien C, $S \subseteq K$ endlich, S habe gute Kongruenzeigenschaften bezüglich C. Dann existiert für jedes kritische $a \in K$ ein $s \in S$, so daß $v(s + c) = v(a + c)$ für alle $c \in C$.

Beweis. Sei (a, c_0) kritisch. Für $c \in C \setminus \operatorname{top}(C, a)$ gilt $v(s+c) = v(s+c_0+c-c_0) = v(c-c_0) = v(a+c)$. Für $c \in \operatorname{top}(C, a) \setminus \operatorname{crit}(C, c_0, a)$ gilt $v(s+c) = v(s+c_0+c-c_0) = v(s + c_0) = v(a + c)$. □

Bemerkung 2.18. Wir wenden den Begriff *gute Kongruenzeigenschaften* auch auf Mengen von Termen an: Eine Termmenge S hat gute Kongruenzeigenschaften bezüglich einer Termmenge C, falls S unter jeder Belegung aller Variablen gute Kongruenzeigenschaften bezüglich C hat.

Satz 2.19. *Es sei* $\Phi = \{\, X + \check{c} \parallel \check{d},\ \hat{d} \parallel X + \hat{c} \mid (\check{c}, \check{d}) \in \check{I},\ (\hat{c}, \hat{d}) \in \hat{I} \,\}$, *und* X *komme in den* $\check{c}$, $\check{d}$, $\hat{c}$, $\hat{d}$ *nicht vor. Mit* $C = \operatorname{pr}_1(\check{I} \cup \hat{I})$ *und* $D = \operatorname{pr}_2(\check{I} \cup \hat{I})$ *setze*

$$S_1 = \{\, d - c,\ \pi d - c,\ \pi(c' - c) - c,\ \pi^{-1} d - c,\ \pi^{-1}(c' - c) - c \mid c,\ c' \in C,\ d \in D \,\}.$$

Sei nun S *eine endliche Menge von Termen, die* X *nicht enthalten und linear in* $L_X(\Phi)$ *sind. Weiter habe* S *gute Kongruenzeigenschaften bezüglich* C. *Setze* $S_2 = S \cup \{\, -c \mid c \in C \,\}$. *Dann ist* $S_1 \cup S_2$ *eine Skolemmenge für* Φ *und* X.

Beweis. Fixiere eine Interpretation β aller Variablen außer X. Zu zeigen ist, daß $S_1 \cup S_2$ für jede Fortsetzung β_a von β, die X durch $a \in K$ interpretiert, ein Term $t \in S_1 \cup S_2$ existiert, so daß

$$\beta_a \models \textstyle\bigwedge_{\alpha \in \Phi} \bigl(\alpha \longleftrightarrow \alpha[X/t]\bigr).$$

Wähle $a \in K$. Falls $-a \in C$, so setze $t = a \in S_2$. Sonst wähle $c_0 \in \operatorname{top}(C, a)$. Falls $\operatorname{crit}(C, c_0, a) \neq \emptyset$, so ist a kritisch und nach Lemma 2.17 existiert ein $s \in S$, so daß $v(s + c) = v(a + c)$ für alle $c \in C$.

Falls $\operatorname{crit}(C, c_0, a) = \emptyset$, so enthält S_1 einen geeigneten Testpunkt:

(1) Falls ein $d_1 \in D$ mit $v(d_1) = \mu(C, a)$ existiert, so ist $d_1 - c_0 \in S_1$ ein geeigneter Testpunkt: Falls $c \in C \setminus \operatorname{top}(C, a)$, so ist $v(d_1 + c - c_0) = v(c - c_0) = v(a + c)$. Falls $c \in \operatorname{top}(C, a)$, so ist $v(c - c_0) > \mu(C, a)$, da $\operatorname{crit}(C, c_0, a) = \emptyset$, und damit ist $v(d_1 + c - c_0) = v(d_1) = v(a + c)$.

Wir nehmen im folgenden an, daß $v(d) \neq \mu(C, a)$ für alle $d \in D$.

(2) Es existiert ein $d \in D$ mit $v(d) < \mu(C, a)$. Dann wähle $d_1 \in D$ von maximalem Wert mit dieser Eigenschaft.

(2.1) Es existiert kein $c \in C$ mit $v(d_1) < v(c-c_0) < \mu(C,a)$. Setze $t = \pi d_1 - c_0 \in S_1$, und betrachte ein $c \in C$. Falls $v(c-c_0) < \mu(C,a)$, so ist

$$v(t+c) = v(\pi d_1 + c - c_0) = v(c-c_0) = v(a+c).$$

Falls $\mu(C,a) < v(c-c_0)$, so ist $v(t+c) = v(\pi d_1 + c - c_0) = v(\pi d_1)$, und wegen der Wahl von d_1 existiert kein $d \in D$ mit $v(t+c) = v(\pi d_1) \geqslant v(d) \leqslant \mu(C,a) = v(a+c)$.

(2.2) Es existiert ein $c \in C$ mit $v(d_1) < v(c-c_0) < \mu(C,a)$, $c_1 \in C$ sei von maximalem Wert mit dieser Eigenschaft. Wähle $t = \pi(c_1 - c_0) - c_0 \in S_1$ und argumentiere wie in (2.1).

(3) Für alle $d \in D$ ist $v(d) > \mu(C,a)$, wähle $d_1 \in D$ von minimalem Wert.

(3.1) Es existiert kein $c \in C$ mit $\mu(C,a) < v(c-c_0) < v(d_1)$. In diesem Fall setze $t = \pi^{-1} d_1 - c_0 \in S_1$. Falls $v(c-c_0) < \mu(C,a)$, so gilt

$$v(t+c) = v(\pi^{-1} d_1 + c - c_0) = v(c-c_0) = v(a+c).$$

Falls hingegen $v(a+c) = \mu(C,a) \leqslant v(\pi^{-1} d_1) < v(c-c_0)$, so gilt

$$v(t+c) = v(\pi^{-1} d_1 + c - c_0) = v(\pi^{-1} d_1),$$

und wegen der Minimalität des Wertes von d_1 existiert kein $d \in D$ mit

$$v(t+c) = v(\pi^{-1} d_1) \geqslant v(d) > \mu(C,a) = v(a+c).$$

(3.2) Es existiert ein $c \in C$ mit $v(a+c_0) < v(c-c_0) < v(d_1)$, $c_1 \in C$ sei von minimalem Wert mit dieser Eigenschaft. Setze $t = \pi^{-1}(c_1 - c_0) - c_0 \in S_1$ und argumentiere wie in (3.1). $\square$

Algorithmus 2.20. *Eingabe:* Eine lineare pränexe Formel. *Ausgabe:* Eine äquivalente quantorenfreie Formel. *Verwendete Subalgorithmen:* Berechnung einer Menge mit guten Kongruenzeigenschaften. *Methode:* Ergänze Algorithmus 2.13 durch folgenden Subalgorithmus:

$\langle$*Berechne eine Skolemmenge* E *für* $A_X(\psi)$ *und* $X\rangle \equiv$
  Konstruiere C, D und daraus S_1 wie in Satz 2.19
  $\langle$*Konstruiere* S *mit guten Kongruenzeigenschaften bezüglich* C 2.26, 2.29, 2.34$\rangle$
  Konstruiere S_2 aus C und S wie in Satz 2.19
  $E := S_1 \cup S_2$

Damit müssen wir, um unseren Algorithmus zu vervollständigen, nur noch zeigen, wie man für eine gegebene endliche Termmenge C eine Termmenge S mit guten Kongruenzeigenschaften bezüglich C konstruiert. Zuerst behandeln wir den Fall, daß K_v endlich ist, etwa $|K_v| = p^k$. Fixieren wir eine Belegung aller Variablen, und wählen ein kritisches (a, c_0). Nehmen wir nun für einen Moment an, daß $\mu(C,a) = 0$. Die Forderungen an das $s \in S$, das wir suchen, lassen sich dann formulieren als $\overline{s+c_0} \neq 0$ und $\overline{s+c_0} \neq \overline{-(c-c_0)}$ für alle $c \in \operatorname{crit}(C, c_0, a)$. Andererseits wissen wir, daß es ein solches $\overline{s+c_0}$ gibt, nämlich $\overline{a+c_0}$. Durch Ausprobieren aller $p^k - 1$ Restklassen außer $0 \in K_v$ kann man die Restklasse von $a + c_0$ finden und damit die Restklassen der $-(c-c_0)$ *vermeiden.* Das gesuchte s erhält man, indem man c_0 von einem Urbild der Restklasse subtrahiert. Das folgende Lemma überträgt dieses Argument auf alle Niveaus von endlichem Wert.

Lemma 2.21 (Vermeiden von Restklassen bei endlicher Kardinalität). Sei $|K_v|$ endlich, und sei $B \subseteq K$ endlich, derart daß $\overline{B} = K_v^\times$. Sei $\mu \in \Gamma$, $x \in K$ mit $v(x) = \mu$ und $Y \subseteq K$ endlich mit $v(y) = \mu$ für alle $y \in Y$. Ferner sei x derart, daß $v(x+y) = \mu$ für alle $y \in Y$. Dann existiert für beliebiges $y_0 \in Y$ ein $b \in B$, so daß $v(by_0 + y) = \mu$ für alle $y \in Y \cup \{0\}$.

Beweis. Für alle $y \in Y$ ist nach Voraussetzung $v(x+y) = v(y_0)$, also $v(x/y_0 + y/y_0) = 0$ und somit $\overline{y/y_0} \neq \overline{-x/y_0}$. Für ein $b \in B$ gilt $\overline{x/y_0} = \overline{b}$ und damit gilt für alle $y \in Y$, daß $\overline{y/y_0} \neq \overline{-b}$. Mit anderen Worten $v(y/y_0 + b) = 0$, also $v(y + by_0) = v(y_0)$. Wegen $\overline{b} \neq 0$ ist $v(b) = 0$ und damit $v(by_0) = v(y_0) = \mu$. □

Korollar 2.22. Sei $|K_v|$ endlich, und sei $B \subseteq K$ endlich, derart daß $\overline{B} = K_v^\times$. Dann hat für endliches $C \subseteq K$ die Menge $\{\, b(c_1 - c_0) - c_0 \mid c_0,\, c_1 \in C,\, b \in B \,\}$ gute Kongruenzeigenschaften bezüglich C.

Beweis. Sei (a, c_0) kritisch. Wende Lemma 2.21 mit $x = a + c_0$, $Y = \{\, c - c_0 \mid c \in \operatorname{crit}(C, c_0, a) \,\}$ und $y_0 = c_1 - c_0$ für ein $c_1 \in \operatorname{crit}(C, c_0, a)$ an. □

Die Konstruktion einer geeigneten Menge B wird uns später noch beschäftigen. Wir geben zunächst die in [Wei88] vorgeschlagene Möglichkeit an.

Bemerkung 2.23. Sei p prim und $k \in \mathbb{N}$, sei $|K_v| = p^k$. Setze

$$B(p,k) = \{\, \textstyle\sum_{i=0}^{k-1} a_i \zeta^i \mid (a_0, \dots, a_{k-1}) \in (\mathbb{Z}/p)^k \,\} \setminus \{0\}.$$

Dann ist $B(p,k)$ offensichtlich endlich, und es gilt $\overline{B(p,k)} = K_v^\times$.

Falls $|K_v|$ unendlich, so ist entweder $K_v \supseteq (\mathbb{Z}/p)(X)$, wobei X transzendent, oder aber $\operatorname{char}(K_v) = 0$. Falls letzteres der Fall ist, oder aber p genügend groß ist, so greift das folgende Lemma.

Lemma 2.24 (Vermeiden von Restklassen bei großer Charakteristik). Es sei $\mu \in \Gamma$, $Y \subseteq K$ endlich mit $v(y) = \mu$ für alle $y \in Y$. Falls $\operatorname{char}(K_v) = 0$ oder $\operatorname{char}(K_v) > |Y| + 1$, so existiert für beliebiges $y_0 \in Y$ ein $y_1 \in Y$, so daß $v(-y_0 - y_1 + y) = \mu$ für alle $y \in Y \cup \{0\}$.

Beweis. Sei $y_0 \in Y$. Angenommen, für alle $y_1 \in Y$ existiert ein $y \in Y \cup \{0\}$ mit $v(-y_1 - y_0 + y) \neq \mu = v(y_0)$. Wegen der Dreiecksungleichung gilt dann insbesondere $v(-y_1 - y_0 + y) > v(y_0)$. Wir konstruieren eine Folge in $Y \cup \{0\}$:

$$a_0 = y_0 \in Y, \quad a_{i+1} = y \in Y \cup \{0\} \text{ mit } v(-a_i - y_0 + y) > v(y_0).$$

Nach dem *pigeon-hole-Prinzip* existieren $1 \leqslant j < k \leqslant |Y \cup \{0\}| + 1$, so daß $a_j = a_k$. Für alle $i \in \mathbb{N}$ ist $a_i/y_0 \in R_v$, setze $f_i = \overline{a_i/y_0}$. Dann gilt $f_{i+1} = f_i + 1$, denn

$$v\left(\frac{-a_i - y_0 + a_{i+1}}{y_0}\right) > 0 \implies \overline{\frac{-a_i - y_0 + a_{i+1}}{y_0}} = 0 \implies -\overline{\frac{a_i}{y_0}} - 1 + \overline{\frac{a_{i+1}}{y_0}} = 0.$$

Wegen $a_j = a_k$ gilt aber auch $f_j = f_k$ und zusammen $f_j = f_k = f_j + (k-j)1$, also $(k-j)1 = 0$, d. h., $\operatorname{char}(K_v)$ teilt $k - j$. Somit gilt

$$0 \neq \operatorname{char}(K_v) \leqslant k - j \leqslant |Y \cup \{0\}| = |Y| + 1,$$

was den Voraussetzungen des Lemmas widerspricht. □

Korollar 2.25. Sei $C \subseteq K$ endlich. Falls $\operatorname{char}(K_v) = 0$ oder $\operatorname{char}(K_v) > |C|$, so hat $\{\, c_0 - c_1 - c_2 \mid c_0,\, c_1,\, c_2 \in C \,\}$ gute Kongruenzeigenschaften bezüglich C.

Beweis. Sei (a, c_0) kritisch. Dann ist $|\operatorname{crit}(C, c_0, a)| < |C|$, da $c_0 \notin \operatorname{crit}(C, c_0, a)$. Wende Lemma 2.24 mit $Y = \{\, c - c_0 \mid c \in \operatorname{crit}(C, c_0, a) \,\}$ und $y_0 = c_1 - c_0$ für ein $c_1 \in \operatorname{crit}(C, c_0, a)$ an. □

Damit können wir in den Fällen $|K_v|$ endlich oder $\operatorname{char}(K_v) = 0$ eliminieren, allerdings je nach Fall mit verschiedenen Eliminationsmengen für dieselbe Eingabeformel. Unser Algorithmus bekommt daher $|K_v|$ und $\operatorname{char}(K_v)$ als zusätzliche Parameter.

Algorithmus 2.26 (Elimination in einem bestimmten Modell).
Eingabe: Eine lineare pränexe Formel, $|K_v|$, $\mathrm{char}(K_v)$. *Bedingungen:* $|K_v|$ endlich oder $\mathrm{char}(K_v) = 0$. *Ausgabe:* Eine zur Eingabeformel äquivalente quantorenfreie Formel. *Methode:* Ergänze Algorithmus 2.20 durch folgenden Subalgorithmus:

$\langle$*Konstruiere S mit guten Kongruenzeigenschaften bezüglich C*$\rangle \equiv$
  if $|K_v|$ endlich **then**
    $S :=$ Die Menge aus Korollar 2.22 (mit B z. B. nach Bemerkung 2.23)
  else if $\mathrm{char}(K_v) = 0$ **then**
    $S :=$ Die Menge aus Korollar 2.25
  fi

Genau durch die beiden Parameter $|K_v|$ und $\mathrm{char}(K_v)$ geht Information über das Modell, in dem man eliminiert, in das Verfahren ein. Für unsere Zwecke liegt es daher nahe, die diskret bewerteten Körper aufgrund dieser beiden Parameter in Modellklassen einzuteilen.

Definition 2.27. Mit $\mathfrak{K}_0$ bezeichnen wir die Klasse aller diskret bewerteten Körper mit $\mathrm{char}(K_v) = 0$. Für p prim und $k \in \mathbb{N}$ bezeichnen wir mit $\mathfrak{K}_p^k$ die Klasse aller diskret bewerteten Körper mit $\mathrm{char}(K_v) = p$ und $|K_v| = p^k$. Schließlich bezeichnen wir für p prim mit $\mathfrak{K}_p^\infty$ die Klasse aller diskret bewerteten Körper mit $\mathrm{char}(K_v) = p$ und $|K_v|$ unendlich.

Der Fall, daß $\mathrm{char}(K_v) = p$ für eine Primzahl p, aber $|K_v|$ unendlich, wird durch die Spezifikation von Algorithmus 2.26 ausgeschlossen, d. h., für bewertete Körper aus den Klassen $\mathfrak{K}_p^\infty$ haben wir bisher kein Eliminationsverfahren angegeben.

Bemerkung 2.28. Übergibt man Algorithmus 2.26 eine pränexe lineare Formel φ und spezifiziert, daß $\mathrm{char}(K_v) = p$ und $|K_v| = p^k$ für p prim und $k \in \mathbb{N}$, so erhält man nach dem bisher Gezeigten eine quantorenfreie Formel φ', so daß $\mathfrak{K}_p^k \models \varphi \longleftrightarrow \varphi'$. Falls nun q prim und $l \in \mathbb{N}$ mit $q \leqslant p$ und $l \leqslant k$, so ist $B(q,l) \subseteq B(p,k)$. Diese Inklusion setzt sich auf die entsprechenden Mengen S_2 in Satz 2.19 fort, und da jede Obermenge einer Eliminationsmenge offensichtlich wieder eine Eliminationsmenge ist, gilt sogar $\mathfrak{K}_q^l \models \varphi \longleftrightarrow \varphi'$ für alle Modellklassen $\mathfrak{K}_q^l$ mit $q \leqslant p$ und $l \leqslant k$.

Wählt man $\mathrm{char}(K_v) = 0$, so liefert der Algorithmus eine quantorenfreie Formel φ', so daß $\mathfrak{K}_0 \models \varphi \longleftrightarrow \varphi'$. Die dabei für die Elimination jedes Quantors verwendete Menge $S_1 \cup S_2'$ aus Satz 2.19, ist jedoch nicht nur im Fall $\mathrm{char}(K_v) = 0$ eine Skolemmenge, sondern auch, falls $\mathrm{char}(K_v)$ in einem gewissen Sinne groß ist. Betrachten wir folgenden Algorithmus:

Algorithmus 2.29 (Elimination bei großer Charakteristik).
Eingabe: Eine lineare pränexe Formel. *Ausgabe:* Eine äquivalente quantorenfreie Formel. *Methode:* Ergänze Algorithmus 2.20 durch folgenden Subalgorithmus:

$\langle$*Initialisierung*$\rangle \equiv$
  $p_0 := 2$

$\langle$*Konstruiere S mit guten Kongruenzeigenschaften bezüglich C*$\rangle \equiv$
  $S :=$ Die Menge aus Korollar 2.25
  $p_0 := \max\{p_0, |C| + 1\}$

$\langle$*Berechne zusätzliche Ausgaben*$\rangle \equiv$
  $p_0 :=$ Die kleinste Primzahl $\geqslant p_0$

Dann gilt $\mathfrak{K}_p^k \models \varphi \longleftrightarrow \varphi'$ für alle Primzahlen $p \geqslant p_0$ und alle $k \in \mathbb{N} \cup \{\infty\}$. Dies folgt sofort aus Satz 2.19 und der Tatsache, daß p_0 in Algorithmus 2.29 monoton wächst.

Der Körper $\mathbb{Q}$ erlaubt nach dem Satz 1.25 von OSTROWSKI nur die p-adischen Bewertungen. Ist v eine p-adische Bewertung, so ist $\mathrm{char}(K_v) = p$. Damit liefert Algorithmus 2.29 ein Eliminationsergebnis, das in $\mathbb{Q}$ für alle bis auf endlich viele Bewertungen richtig ist.

2.3. Uniformes Vermeiden von Restklassen

Wir wollen nun einen weiteren Ansatz für das Vermeiden von Restklassen vorstellen. Damit werden wir in der Lage sein, Eliminationsergebnisse zu berechnen, die in allen diskret bewerteten Körpern korrekt sind. Das schließt insbesondere die Körper aus $\mathfrak{K}_p^\infty$ ein.

Zur Motivation von Lemma 2.21 hatten wir unsere Problemstellung auf das Niveau 0 verschoben. Wir testeten alle Restklassen, und aus der Existenz einer vermeidenden folgte, daß sie unter den getesteten ist. Wenn der Restklassenkörper unendlich oder auch nur größer als die Anzahl n der zu vermeidenden Restklassen ist, so folgt aus dem *pigeon-hole-Prinzip*, daß es eine vermeidende Restklasse gibt, und man braucht nur $n + 1$ viele zu testen, um eine zu finden.

Lemma 2.30 (Vermeiden von Restklassen bei großer Kardinalität). Sei $\mu \in \Gamma$, $Y \subseteq K$ endlich mit $v(y) = \mu$ für alle $y \in Y$. Sei $B \subseteq K$ endlich, derart daß $\overline{B} \subseteq K_v^\times$ und $|\overline{B}| > |Y|$. Dann existiert für beliebiges $y_0 \in Y$ ein $b \in B$, so daß $v(by_0 + y) = \mu$ für alle $y \in Y \cup \{0\}$.

Beweis. Sei $y_0 \in Y$. Für alle $y \in Y$ ist $v(-y/y_0) = 0$, also $\overline{-y/y_0} \neq 0$. Wegen $|\overline{B}| > |Y|$, existiert nach dem *pigeon-hole-Prinzip* ein $b \in B$, so daß für alle $y \in Y$ $\overline{b} \neq \overline{-y/y_0}$, also $v(b + y/y_0) = 0$, und somit $v(by_0 + y) = v(y_0) = \mu$. Wegen $\overline{b} \neq 0$ ist $v(b) = 0$ und damit $v(by_0) = v(y_0) = \mu$. □

Korollar 2.31. Sei $C \subseteq K$ endlich. Sei $B \subseteq K$ endlich, derart daß $\overline{B} \subseteq K_v$ und $|\overline{B}| \geqslant |C|$. Dann hat die Menge $\{\, b(c_1 - c_0) - c_0 \mid c_0, c_1 \in C, b \in B \,\}$ gute Kongruenzeigenschaften bezüglich C.

Beweis. Sei (a, c_0) kritisch. Wegen $c_0 \notin \mathrm{crit}(C, c_0, a)$ ist $|\mathrm{crit}(C, c_0, a)| < |C|$. Wende Lemma 2.30 mit $Y = \{\, c - c_0 \mid c \in \mathrm{crit}(C, c_0, a) \,\}$ und $y_0 = c_1 - c_0$ für ein $c_1 \in \mathrm{crit}(C, c_0, a)$ an. □

Proposition 2.32. *Für $n \in \mathbb{N}$ definieren wir $B'(n) = \{1, \zeta, \dots, \zeta^{n-1}\}$. Dann gilt $|\overline{B'(n)}| = |B'(n)| = n$ oder $\overline{B'(n)} = K_v^\times$.*

Beweis. Im Fall $\mathrm{char}(K_v) = 0$ ist $\zeta = 2$. Da nach Bemerkung 1.20 auch $\mathrm{char}(K) = 0$ ist, sind die Elemente von $B'(n)$ die natürlichen Zahlen 1, 2, 4, …, 2^{n-1}, also $|B'(n)| = n$. Für $i \in \mathbb{N}$ ist $\overline{2^i 1} = 2^i \overline{1}$. Angenommen es gibt $1 \leqslant i < j \leqslant n - 1$ mit $2^j \overline{1} - 2^i \overline{1} = 0$. Dann ist $\mathrm{char}(K_v) = 2^j - 2^i > 0$, ein Widerspruch; es folgt $|\overline{B'(n)}| = |B'(n)|$.

Sei nun $\mathrm{char}(K_v) = p$. Falls $|K_v| = \infty$, so ist $\overline{\zeta}$ transzendent über $\mathbb{Z}/p$, d. h. für $1 \leqslant i < j \leqslant n - 1$ ist $\overline{\zeta^i} - \overline{\zeta^j} = \overline{\zeta}^i - \overline{\zeta}^j \neq 0$. Damit ist $|\overline{B'(n)}| = n$, und es folgt $|B'(n)| = n$.

Falls $|K_v| = p^k$, so ist $\overline{\zeta}$ eine primitive $(p^k - 1)$-te Einheitswurzel. Falls $|K_v| = p^k \leqslant n+1$, so ist $\overline{B'(n)} = K_v^\times$, und falls $|K_v| = p^k \geqslant n+1$, so ist $|\overline{B'(n)}| = |B'(n)| = n$. □

Korollar 2.33. *Sei $C \subseteq K$ endlich. Dann hat die Menge*

$$\{\, b(c_1 - c_0) - c_0 \mid c_0, c_1 \in C, b \in \{1, \zeta, \dots, \zeta^{|C|-1}\} \,\}$$

gute Kongruenzeigenschaften bezüglich C.

Beweis. Nach Proposition 2.32, Korollar 2.22 und Korollar 2.31. □

Algorithmus 2.34 (Uniforme Elimination).
Eingabe: Eine lineare pränexe Formel. *Ausgabe:* Eine äquivalente quantorenfreie Formel. *Methode:* Ergänze Algorithmus 2.20 durch folgenden Subalgorithmus:

$\langle$*Konstruiere S mit guten Kongruenzeigenschaften bezüglich C*$\rangle \equiv$
$S :=$ Die Menge aus Korollar 2.33

Da $\mathbb{Q}$ nur p-adische Bewertungen erlaubt und für diese $K_v = \mathbb{Z}/p$ ist, folgt im Fall $p \leqslant n+1$, daß $\overline{B'(n)} = \{1, \dots, p-1\}$. Das erreicht man auch durch Wahl von $\{1, \dots, n-1\} \subseteq \mathbb{Q}$ als Urbild. Außerdem sind für $p \geqslant n+1$ die Elemente 1, …, $n-1$ verschieden in $\mathbb{Z}/p$. Damit gilt folgendes Korollar, das zeigt, daß wir für Elimination in $\mathbb{Q}$ auf die Konstante ζ verzichten können.

Korollar 2.35. *Im Fall $K = \mathbb{Q}$ hat für endliches $C \subseteq \mathbb{Q}$ die Menge*

$$\{\, b(c_1 - c_0) - c_0 \mid c_0,\, c_1 \in C,\, b \in \{1, \dots, |C|\} \,\}$$

gute Kongruenzeigenschaften bezüglich C. □

In Anwendungen kann es aus Komplexitätsgründen sinnvoll sein, nicht vollkommen uniforme Ergebnisse zu berechnen. Untersuchen wir in Satz 2.19 die Größe der Eliminationsmenge in Abhängigkeit von $|C|$ und $|D|$. Wir verwenden die O-Notation wie in [Knu68]. Zunächst ist

$$|S_1| = O\big(|C|^2 + |C| \cdot |D|\big) = O\big(\max\{|C|, |D|\}^2\big).$$

Berechnet man S_2 nach dem uniformen Algorithmus 2.34, also mit S aus Korollar 2.33, so ist $|S_2| = O\big(|C|^3\big)$, und damit

$$|S_1 \cup S_2| = O\big(|C|^3\big).$$

Rechnet man für einen bestimmten Körper aus $\mathfrak{K}_p^k$ mit Algorithmus 2.26, also mit S aus Korollar 2.22 und $B = B(p,k)$, so ist $|S_2| = O\big(|C|^2\big)$, und damit

$$|S_1 \cup S_2| = O\big(\max\{|C|, |D|\}^2\big).$$

Aus Uniformitätsgründen ist es günstiger, auch bei der Elimination für konkrete Modelle statt den $B(p,k)$ eine geeignete gleich große Menge von ζ-Potenzen zu verwenden. Nach dem Beweis von Lemma 2.32 und nach Korollar 2.22 gilt folgendes Korollar.

Korollar 2.36. *Falls $|K_v| \leqslant p^k$, so hat für endliches $C \subseteq K$ die Menge*

$$\{\, b(c_1 - c_0) - c_0 \mid c_0,\, c_1 \in C,\, b \in \{1, \zeta, \dots, \zeta^{p^k - 2}\} \,\}$$

gute Kongruenzeigenschaften bezüglich C. □

Damit gilt $\mathfrak{K}_q^l \models \varphi \longleftrightarrow \varphi'$ für alle Primzahlen q und $l \in \mathbb{N}$ mit $q^l \leqslant p^k$, bei Eingabe φ und Ausgabe φ'. Vergleiche hierzu Bemerkung 2.28. Schließlich kann man für die rationalen Zahlen wieder auf das ζ verzichten.

Korollar 2.37. *Betrachtet man $\mathbb{Q}$ mit einer p-adischen Bewertung, so hat für endliches $C \subseteq \mathbb{Q}$ die Menge $\{\, b(c_1 - c_0) - c_0 \mid c_0,\, c_1 \in C,\, b \in \{1, \dots, p-1\} \,\}$ gute Kongruenzeigenschaften bezüglich C.* □

2.4. Eliminationsmengen für positive Formeln

Betrachten wir noch einmal den Anfang des Beweises zu Lemma 2.8, wo gezeigt wird, daß Skolemmengen Eliminationsmengen sind. Man benötigt die Äquivalenz $\forall X(\alpha \longleftrightarrow \alpha[X/t])$ der Skolemmengendefinition, um

$$\forall X\big(\bigvee_{t\in S}(\varphi \longleftrightarrow \varphi[X/t])\big)$$

zeigen zu können, wovon man schließlich nur die Richtung $\forall X\big(\bigvee_{t\in S}(\varphi \longrightarrow \varphi[X/t])\big)$ benutzt. Der Grund dafür, daß aus $\forall X(\alpha \longrightarrow \alpha[X/t])$ nicht schon das gewünschte folgt, liegt in der Tatsache, daß die α im Skopus einer Negation stehen können, z. B. auf der linken Seite einer Implikation. Durch die Betrachtung von *positiven* Formeln umgeht man dieses Problem.

Definition 2.38. Eine quantorenfreie Formel heißt **positiv**, falls sie eine $\wedge$-$\vee$-Kombination von atomaren Formeln ist. Eine pränexe Formel heißt positiv, falls ihre Matrix positiv ist.

Die Idee, sich im Zusammenhang mit Eliminationsmengen auf positive Formeln zurückzuziehen, stammt aus einer Arbeit von Loos und Weispfenning über lineare reelle Probleme, [LW93].

Lemma 2.39. Unter Verwendung folgender Äquivalenzen läßt sich jede quantorenfreie Formel in eine äquivalente quantorenfreie positive Formel umformen.

$$\neg(t=0) \longleftrightarrow t \neq 0, \quad \neg(t \neq 0) \longleftrightarrow t = 0, \quad \neg(s \sim t) \longleftrightarrow s \parallel t \vee t \parallel s,$$
$$\neg(s \parallel t) \longleftrightarrow t \mid s, \qquad \neg(s \mid t) \longleftrightarrow t \parallel s. \quad \square$$

In den Äquivalenzen kommen auf beiden Seiten dieselben Terme vor, also sind beide Seiten in denselben Variablenmengen linear.

Auch bei der Konstruktion von Eliminationsmengen für positive Formeln werden wir von der Menge der enthaltenen atomaren Formeln ausgehen. Die folgende Definition liefert ein Gegenstück zu den Skolemmengen aus Abschnitt 2.2.

Definition 2.40. Sei Φ eine Menge von atomaren Formeln, die linear in X sind. Eine *Testmenge für konjunktive Erfüllbarkeit,* kurz **KE-Menge**, für Φ und X ist eine Menge, die für alle $\Psi \subseteq \Phi$ eine Eliminationsmenge für $\exists X(\bigwedge \Psi)$ ist.

Lemma 2.41. Sei φ eine quantorenfreie positive Formel, die linear in X ist. Sei E eine KE-Menge für $A_X(\varphi)$ und X. Dann ist E eine Eliminationsmenge für $\exists X(\varphi)$.

Beweis. Es existiert eine positive disjunktive Normalform φ', die äquivalent zu φ ist und dieselben atomaren Formeln enthält. Offensichtlich ist E eine Eliminationsmenge für $\exists X(\varphi')$ und damit nach Lemma 2.5 auch für φ. $\square$

Die Einschränkung auf den Fall eines Existenzquantors ist nicht wesentlich, wie das folgende Lemma zeigt.

Lemma 2.42. Die Eliminationsmengen für $\forall X(\varphi)$ sind genau die Eliminationsmengen für $\exists X(\neg\varphi)$, und die Eliminationsmengen für $\exists X(\varphi)$ sind genau die Eliminationsmengen für $\forall X(\neg\varphi)$.

Beweis. Es gilt $\exists X(\neg\varphi) \longleftrightarrow \neg\forall X(\varphi) \longleftrightarrow \neg \bigwedge_{t\in E}\big(\varphi[X/t]\big) \longleftrightarrow \bigvee_{t\in E}\big(\neg\varphi[X/t]\big)$, falls E Eliminationsmenge für $\forall X(\varphi)$. Falls E eine Eliminationsmenge für $\exists X(\neg\varphi)$, so gilt $\forall X(\varphi) \longleftrightarrow \neg\exists X(\neg\varphi) \longleftrightarrow \neg \bigvee_{t\in E}\big(\neg\varphi[X/t]\big) \longleftrightarrow \bigwedge_{t\in E}\big(\varphi[X/t]\big)$. Die andere Äquivalenz zeigt man analog. $\square$

Wie schon bei der Elimination mit Skolemmengen wollen wir von gewissen Normalformen ausgehen. Da man Gleichungen nicht positiv in strikte Ungleichungen codieren kann, lockern wir unseren Begriff einer bezüglich einer Variablen X *gut eliminierbaren Formel* dahingehend, daß wir nun auch Gleichungen in X zulassen. Eine positive Formel dieser Form bezeichnen wir als **gut positiv eliminierbar** bezüglich X.

Lemma 2.43. Unter Verwendung folgender Äquivalenzen läßt sich jede quantorenfreie positive Formel in eine äquivalente quantorenfreie positive Formel umformen, in der X nur mit $=$ und $\parallel$ vorkommt:

$$\begin{aligned} t \neq 0 &\longleftrightarrow t \parallel 0, \\ s \mid t &\longleftrightarrow s \parallel \pi t \vee t = 0, \\ s \sim t &\longleftrightarrow (s \parallel \pi t \wedge t \parallel \pi s) \vee s - t = 0. \quad \square \end{aligned}$$

Auch bei diesen Äquivalenzen bleiben auf den rechten Seiten die Linearitätseigenschaften der linken Seiten erhalten.

Definition 2.44. Betrachte eine quantorenfreie positive Formel φ, die linear in X ist. Sei $G \subseteq A_X(\varphi)$ die Menge aller Gleichungen in φ, in denen X vorkommt. Wir gehen o. B. d. A. davon aus, daß die Gleichungen in der Form $aX = b$ für Terme a und b, die X nicht enthalten, gegeben sind, etwa $G = \{ aX = b \mid (a,b) \in I \}$. Damit definieren wir $\mathrm{eqsol}_X(\varphi) = \{ b/a \mid (a,b) \in I \}$. Außerdem definieren wir $A'_X(\varphi) = A_X(\varphi) \setminus G$.

Lemma 2.45. Sei φ eine positive quantorenfreie Formel, und sei E eine KE-Menge für $A'_X(\varphi)$ und X. Dann ist $E \cup \mathrm{eqsol}_X(\varphi)$ eine KE-Menge für $A_X(\varphi)$ und X.

Beweis. Sei $\Psi \subseteq \Phi$. Fixiere eine Interpretation β aller Variablen außer X. Gelte $\exists X(\bigwedge \Psi)$. Falls Ψ unter β eine nichttriviale Gleichung enthält, also eine eine Gleichung $aX = b$ mit $a \neq 0$, so erfüllt genau $b/a \in \mathrm{eqsol}_X(\varphi)$ die Gleichung und damit $\bigwedge \Psi$. Sonst enthält E einen erfüllenden Term. $\square$

Diese Technik kann man immer anwenden, wenn man Prädikate hat, deren Erfüllungsmengen höchstens endlich sind, und man aus den Argumenten alle erfüllenden Elemente konstruieren kann. Offenbar enthält $A'_X(\varphi)$ für gut positiv eliminierbares φ nur atomare Formeln der Form $X + c \parallel d$ und $d \parallel X + c$. Wir müssen KE-Mengen für Mengen von atomaren Formeln dieses Typs konstruieren. Wir fassen die bisherigen Ergebnisse algorithmisch zusammen.

Algorithmus 2.46. *Eingabe:* Eine lineare pränexe positive Formel. *Ausgabe:* Eine äquivalente quantorenfreie Formel. *Verwendete Subalgorithmen:* Berechnung einer KE-Menge für $A'_X(\psi)$, wobei ψ gut positiv eliminierbar. *Methode:* Ergänze Algorithmus 2.4 durch folgenden Subalgorithmus:

⟨*Berechne eine Eliminationsmenge E für $QX(\varphi)$*⟩ $\equiv$
  if $Q = \exists$ **then** $\psi_0 := \varphi$ **else** $\psi_0 := \neg\varphi$ **fi**
  Konstruiere $A_X(\psi)$ für ein gut positiv eliminierbares $\psi \longleftrightarrow \psi_0$
  Berechne $A'_X(\psi)$ und $\mathrm{eqsol}_X(\psi)$ aus $A_X(\psi)$
  ⟨*Berechne eine KE-Menge für $A'_X(\psi)$* 2.48⟩
  $E := E' \cup \mathrm{eqsol}_X(\psi)$

Beweis. Zunächst sei wieder angemerkt, daß ψ nicht konstruiert werden muß, sondern $A_X(\psi)$ unter Verwendung von Lemma 2.39 und Lemma 2.46 direkt aus ψ_0 berechnet werden kann. Am Ende ist E nach Lemma 2.45 eine KE-Menge für $A_X(\psi)$, also nach Lemma 2.41 eine Eliminationsmenge für $\exists X(\psi)$, damit nach Lemma 2.5

auch eine Eliminationsmenge für $\exists X(\psi_0)$ und schließlich nach Lemma 2.42 eine Eliminationsmenge für $QX(\varphi)$. $\square$

Aus naheliegenden Gründen bezeichnen wir atomare Formeln der Form $X+c \parallel d$ als **obere Schranken** für X und entsprechend atomare Formeln der Form $d \parallel X+c$ als **untere Schranken**. Für eine Menge von oberen Schranken kann man leicht eine KE-Menge finden, wie das folgende Lemma zeigt.

Lemma 2.47. Es sei $\Phi = \{\, X+c \parallel d \mid (c,d) \in I \,\}$, und X komme in den c, d nicht vor. Dann ist $E = \{\, 1,\, \pi^{-1}c,\, \pi^{-1}d \mid (c,d) \in I \,\}$ eine KE-Menge für Φ und X.

Beweis. Wähle $\Psi = \{\, X+c \parallel d \mid (c,d) \in I' \,\} \subseteq \Phi$. Fixiere eine Interpretation aller Variablen außer X. Wähle $d_0 \in \mathrm{pr}_2(I')$ von minimalem Wert. Falls $d_0 = 0$ so setze $t = 1 \in E$. Sonst unterscheiden wir zwei Fälle: Falls ein $c \in \mathrm{pr}_1(I')$ existiert mit $v(c) < v(d_0)$, so wähle $c_1 \in \mathrm{pr}_1(I')$ von minimalem Wert, und setze $t = \pi^{-1}c_1 \in E$. Falls hingegen $v(c) \geqslant v(d_0)$ für alle $c \in \mathrm{pr}_1(I')$, so setze $t = \pi^{-1}d_0 \in E$. In jedem Fall wird $\bigwedge \Psi$ von t erfüllt. $\square$

Obiger Beweis zeigt, daß jede Konjunktion über obere Schranken für X erfüllbar ist. Dies läßt i. a. jedoch keine Rückschlüsse auf die Erfüllbarkeit der Ausgangsformel φ zu, da diese noch weitere atomare Formeln enthalten kann, in denen X nicht vorkommt.

Satz 2.48. *Gegeben sei $\Phi = \{\, X+\check{c} \parallel \check{d},\ \hat{d} \parallel X+\hat{c} \mid (\check{c},\check{d}) \in \check{I},\ (\hat{c},\hat{d}) \in \hat{I} \,\}$, und X komme in den $\check{c}$, $\check{d}$, $\hat{c}$, $\hat{d}$ nicht vor. Mit $\check{C} = \mathrm{pr}_1(\check{I})$, $\check{D} = \mathrm{pr}_2(\check{I})$, $\hat{C} = \mathrm{pr}_1(\hat{I})$ und $\hat{D} = \mathrm{pr}_2(\hat{I})$ setze*

$$E_1 = \{\, 1,\, \pi^{-1}\check{c},\, \pi^{-1}\check{d},\, \pi\hat{d} - \check{c},\, \pi(\check{c} - \check{c}') - \check{c}' \mid \check{c}, \check{c}' \in \check{C},\ \check{d} \in \check{D},\ \hat{d} \in \hat{D} \,\}.$$

Sei nun S eine endliche Menge von Termen, die X nicht enthalten und linear in $L_X(\Phi)$ sind. Weiter habe S gute Kongruenzeigenschaften bezüglich $\check{C}$. Setze $E_2 = S \cup \{\, -\hat{c} \mid \hat{c} \in \hat{C} \,\}$. Dann ist $E_1 \cup E_2$ eine KE-Menge für Φ und X.

Beweis. Wähle $\Psi = \{\, X+\check{c} \parallel \check{d},\ \hat{d} \parallel X+\hat{c} \mid (\check{c},\check{d}) \in \check{I}',\ (\hat{c},\hat{d}) \in \hat{I}' \,\} \subseteq \Phi$. Fixiere eine Belegung aller Variablen außer X. Gelte $\exists X(\bigwedge \Psi)$. Sei etwa $a \in K$ ein erfüllendes Element. Zu zeigen ist, daß E ein erfüllendes Element für $\bigwedge \Psi$ enthält. Setze $\check{C}' = \mathrm{pr}_1(\check{I}') \subseteq \check{C}$, $\check{D}' = \mathrm{pr}_2(\check{I}') \subseteq \check{D}$, $\hat{C}' = \mathrm{pr}_1(\hat{I}') \subseteq \hat{C}$, $\hat{D}' = \mathrm{pr}_2(\hat{I}') \subseteq \hat{D}$ und $C' = \check{C}' \cup \hat{C}'$.

Falls $\hat{I}' = \emptyset$, so ist $\{\, 1, \pi^{-1}\check{c}, \pi^{-1}\check{d} \mid \check{c} \in \check{C}, \check{d} \in \check{D} \,\} \subseteq E_1$ nach Lemma 2.47 eine KE-Menge für $\exists X(\varphi)$. Sei nun $\hat{I}' \neq \emptyset$. Da a erfüllt, ist sicher $-a \notin \check{C}'$. Falls $-a \in \hat{C}'$ teste $-a \in E_2$. Sonst wissen wir, daß $\mu(C',a) < \infty$.

(1) Falls $\check{C}' \cap \mathrm{top}(C',a) = \emptyset$, so wähle $\hat{c}_0 \in \hat{C}' \cap \mathrm{top}(C',a)$. Dann ist $-\hat{c}_0$ ein geeigneter Testpunkt: $v(\check{c} - \hat{c}_0) = v(a + \check{c} - (a + \hat{c}_0)) = v(a+\check{c})$ und $v(\hat{c} - \hat{c}_0) = v(a + \hat{c} - (a + \hat{c}_0)) \geqslant v(a+\hat{c})$.

(2) Falls $\check{C}' \cap \mathrm{top}(C',a) \neq \emptyset$, so wähle $\check{c}_0 \in \check{C}' \cap \mathrm{top}(C',a)$.

(2.1) Falls $\check{C}' \cap \mathrm{crit}(C',\check{c}_0,a) \neq \emptyset$, so gibt es ein $s \in S$, so daß $v(s+\check{c}) = v(a+\check{c})$ für alle $\check{c} \in \check{C}$, und da insbesondere $v(s+\check{c}_0) = \mu(\check{C}',a) = \mu(C',a)$, gilt auch $v(s+\hat{c}) = v(s+\check{c}_0+\hat{c}-\check{c}_0) \geqslant v(a+\hat{c})$ für alle $\hat{c} \in \hat{C}$.

(2.2) Betrachte nun den Fall $\check{C} \cap \mathrm{crit}(C',\check{c}_0,a) = \emptyset$. Wähle $\hat{d}_0 \in \hat{D}'$ von maximalem Wert. Da ψ erfüllbar ist, gilt sicher $v(\hat{d}_0) < \mu(C',a)$.

(2.2.1) Falls es kein $\check{c}$ gibt mit $v(\hat{d}_0) < v(\check{c} - \check{c}_0) < \mu(C,a)$, so teste $\pi\hat{d}_0 - \check{c}_0$. Für $\check{c} \in \check{C}$ ist dann $v(\pi\hat{d}_0 + \check{c} - \check{c}_0) = v(\pi\hat{d}) \leqslant v(a+\check{c})$ falls $\check{c} \in \mathrm{top}(C',a)$ und $v(\pi\hat{d}_0 + \check{c} - \check{c}_0) = v(a+\check{c})$ sonst. Für $\hat{c} \in \hat{C}$ gilt $v(\pi\hat{d}_0 + \hat{c} - \check{c}_0) = v(a+\hat{c})$ falls

$v(a+\hat{c}) \leqslant v(\hat{d}_0)$, und $v(\pi\hat{d}_0+\hat{c}-\check{c}_0) \geqslant v(\pi\hat{d}_0)$ falls $v(a+\hat{c}) > v(\hat{d}_0)$, und $\hat{d}_0$ ist von maximalem Wert in $\hat{D}$.

(2.2.2) Sonst wähle $\check{c}_1 \in \check{C}$, so daß $\check{c}_1 - \check{c}_0$ von maximalem Wert mit $v(\hat{d}_0) < v(\check{c}_1 - \check{c}_0) < \mu(C, a)$. Dann ist $\pi(\check{c}_1 - \check{c}_0) - \check{c}_0$ ein geeigneter Testpunkt. Der Beweis geht analog zu Fall (2.2.1). □

Korollar 2.49. Es sei $\Phi = \{\, d \parallel X + c \mid (c, d) \in I \,\}$. Setze $C = \mathrm{pr}_1(I)$. Dann ist $\{\, -c \mid c \in C \,\}$ eine KE-Menge für Φ und X.

Beweis. Nach dem Beweis zu Satz 2.48 benötigt man die 1 in diesem Fall nicht. □

Wir erinnern noch einmal daran, daß eine pränexe Formel linear heißt, falls ihre Matrix linear in der Menge der quantifizierten Variablen ist. Wir nennen eine allgemeine Formel **linear**, falls sie ein boolesche Kombination von linearen pränexen Formeln ist. Der folgende Sachverhalt ist eine unmittelbare Konsequenz aus der *Existenz eines Eliminationsverfahrens,* das in der Weise uniform ist, wie das vorangehend beschriebene.

Satz 2.50 (Lineares Ax–Kochen–Ershov-Prinzip). *Sei (K, v) ein diskret bewerteter Körper und (L, v) ein entsprechender Erweiterungskörper. Falls $|K_v|$ unendlich oder $K_v = L_v$, so ist die Erweiterung elementar bezüglich linearer Formeln.*

Beweis. Wir zeigen, daß man die gegebene Erweiterung zu einer bezüglich der betrachteten Formeln elementaren Erweiterung $(K, v, \zeta) \subseteq (L, v, \zeta)$ expandieren kann, wobei ζ wie in der Einleitung dieses Kapitels interpretiert ist. Interpretiere ζ in (K, v, ζ) in Abhängigkeit von K_v wie verlangt. Die Interpretation ist auch bezüglich L_v korrekt: Für den Fall $|K_v|$ endlich haben wir $K_v = L_v$ verlangt; in den Fällen mit $|K_v|$ unendlich folgt dies aus der Tatsache, der Primkörper des Restklassenkörpers unter Erweiterungen erhalten bleibt. Für eine lineare Formel φ über der Sprache mit ζ gibt es wegen der uniformen Quantorenelimination eine quantorenfreie Formel φ', so daß

$$(K, v, \zeta) \models \varphi \longleftrightarrow \varphi' \quad \text{und} \quad (L, v, \zeta) \models \varphi \longleftrightarrow \varphi',$$

und jede Erweiterung ist trivialerweise elementar für quantorenfreie Formeln. □

2.5. Elimination mit Dummysymbolen

In Lemma 2.47 werden zahlreiche Punkte getestet, um einen Testpunkt t zu erhalten, von dem man nur eine einzige Eigenschaft verlangt: sein Wert muß so klein sein, daß $v(t + c) < v(d)$ für alle (c, d). Man beachte, daß man t von beliebig kleinem Wert wählen kann. Anschaulich wird unsere Strategie nun folgende sein: Wir legen uns an entsprechender Stelle nicht auf einen konkreten Term fest, sondern merken uns die Tatsache, daß wir einen Punkt mit sehr kleinem Wert testen wollen, indem wir ein Symbol ∞ in die Eliminationsmenge eintragen. Ein vergleichbarer Ansatz für Ordnungsrelationen wurde schon in der im letzten Abschnitt erwähnten Arbeit [LW93] verwendet.

Definition 2.51. Wir definieren eine **modifizierte Substitution** $[v/\!/t]$ auf atomaren Formeln. Diese setzt die gewöhnliche Substitution fort, d. h., für atomare Formeln α, Variablen X und Terme t gilt $\alpha[X/\!/t] \equiv \alpha[X/t]$. Darüber hinaus erlauben wir die Substitution das Einsetzen eines Symbols ∞: Für Terme a, b, a', b', die

X nicht enthalten, definieren wir

$$\begin{aligned}
(aX+b=0)[X/\!\!/\infty] &\longleftrightarrow a=0 \wedge b=0,\\
(aX+b\neq 0)[X/\!\!/\infty] &\longleftrightarrow a\neq 0 \vee b\neq 0,\\
(aX+b\sim a'X+b')[X/\!\!/\infty] &\longleftrightarrow (a\neq 0 \wedge a\sim a') \vee b\sim b',\\
(aX+b\sim b')[X/\!\!/\infty] &\longleftrightarrow a=0 \wedge b\sim b',\\
(b\sim a'X+b')[X/\!\!/\infty] &\longleftrightarrow a'=0 \wedge b\sim b'
\end{aligned}$$

und schließlich für $\varrho \in \{\|, |\}$:

$$\begin{aligned}
(aX+b\;\varrho\; a'X+b')[X/\!\!/\infty] &\longleftrightarrow a\;\varrho\; a' \vee (a'=0 \wedge b\;\varrho\; b'),\\
(aX+b\;\varrho\; b')[X/\!\!/\infty] &\longleftrightarrow a\neq 0 \vee b\;\varrho\; b',\\
(b\;\varrho\; a'X+b')[X/\!\!/\infty] &\longleftrightarrow a'=0 \wedge b\;\varrho\; b'.
\end{aligned}$$

Man beachte, daß das Symbol ∞ auf der jeweils rechten Seite der Äquivalenzen nicht vorkommt.

Lemma 2.52. Sei α eine atomare Formel, die linear in X ist. Dann gibt es ein $a \in K$, so daß $\alpha[X/t] \longleftrightarrow \alpha[X/\!\!/\infty]$ für alle $t \in K$ mit $v(t) \leqslant v(a)$. □

Definition 2.53. Wir verallgemeinern die Definition einer **Eliminationsmenge** aus Definition 2.2 folgendermaßen: Wir lassen zu, daß Eliminationsmengen das Symbol ∞ enthalten. Es ist linear in allen Variablenmengen. Außerdem ersetzen wir die Substitution durch die modifizierte Substitution.

Proposition 2.54. *Es sei $\Phi = \{\, X + c \parallel d \mid (c,d) \in I \,\}$, und X komme in den c, d nicht vor. Dann ist $\{\infty\}$ eine KE-Menge für Φ und X.* □

Korollar 2.55. *Bei der Eliminationsmenge $E_1 \cup E_2$ aus Satz* 2.48 *kann man bei Verwendung der modifizierten Substitution aus Definition* 2.51

$$E_1 = \{\, \infty,\ \pi\hat{d} - \check{c},\ \pi(\check{c} - \check{c}') - \check{c}' \mid \check{c},\ \check{c}' \in \check{C},\ \hat{d} \in \hat{D} \,\} \quad \textit{setzen.}$$

Beweis. Vergleiche den Beweis zu Satz 2.48. Die drei aus E_1 gestrichenen Terme 1, $\pi^{-1}\check{c}$ und $\pi^{-1}\check{d}$ werden genau dann verwendet, wenn es nur obere Schranken gibt. In dieser Situation greift Proposition 2.54. □

KAPITEL 3

Ein Eliminationsverfahren für beliebige Bewertungen

Das vorangegangene Kapitel beschränkte sich auf diskrete Bewertungen. In diesem Kapitel wollen wir ein Verfahren vorstellen, das für beliebige bewertete Körper anwendbar ist. Es stammt ebenfalls von Weispfenning und wurde 1984 veröffentlicht [Wei84]. Das Verfahren eliminiert Quantoren über Körpervariablen, führt aber neue Quantoren über Gruppenvariablen ein. Quantorenelimination in geordneten abelschen Gruppen wird in [Wei86] behandelt.

Dieser Ansatz legt nahe, im Gegensatz zum vorigen Kapitel eine zweisortige Sprache zugrundezulegen. Diese besteht aus der Sprache der Körper mit einer zweistelligen Relation $\neq$ und der Sprache, der additiven geordneten abelschen Gruppen, erweitert um eine Konstante ∞. Außerdem gibt es ein einstelliges Funktionssymbol V und für jedes $n \in \mathbb{N}$ ein nullstelliges Prädikatensymbol E_n.

Das Symbol ∞ bezeichnet das bezüglich Γ unendliche positive Element. Wir setzen $\gamma + \infty = \infty + \gamma = \infty$ für $\gamma \in \Gamma \cup \{\infty\}$, das verlangt die Definition einer Bewertung. Um alle Funktionen total zu machen setzen wir $0_K^{-1} = 0_K$ und $-\infty = \infty$, was für das Verfahren keine Rolle spielt. Wir gehen davon aus, daß die Bewertung V surjektiv ist. Für $n \in \mathbb{N}$ ist E_n genau dann wahr, wenn $|K_v| \geqslant n$.

Wie im vorigen Kapitel betrachten wir nur K-pränexe Formeln. Γ-Quantoren können dabei in beliebigen Positionen stehen. Wir nehmen o. B. d. A. an, daß unsere Ausgangsformeln keine atomaren K-Formeln enthalten. Man kann diese nämlich unter Verwendung der Äquivalenzen

$$s = t \longleftrightarrow V(s-t) = \infty, \quad s \neq t \longleftrightarrow V(s-t) < \infty$$

in atomare Γ-Formeln kodieren. Ferner gehen wir davon aus, daß in Γ-Termen keine disjunkten K-Terme vorkommen, mit anderen Worten: Summen und Differenzen der Form $V(s) + V(t)$ oder $V(s) - V(t)$ werden als $V(st)$ bzw. $V(st^{-1})$ dargestellt. Unter dieser Bedingung heißt eine Formel **linear** in einer Menge L von Variablen, falls alle enthaltenen K-Terme linear in L sind.

Die folgende Beschreibung des Verfahrens dient dem Zweck, die verwendeten Techniken darzustellen, und nicht einen implementierbaren Algorithmus zu entwickeln. Wir lassen in diesem Kapitel Effizienzgesichtspunkte außer acht.

Lemma 3.1 (Isolieren von X-Termen). Sei φ eine K-quantorenfreie Formel, und sei ξ eine Γ-Variable, die in φ nicht vorkommt. Für einen Γ-Term γ gilt dann $\varphi \longleftrightarrow \exists\xi(\psi \wedge \xi = \gamma)$, wobei ψ die Formel ist, die entsteht, wenn man in φ jedes freie Auftreten von γ durch ξ ersetzt.

Beweis. $\varphi \longleftrightarrow \varphi \wedge \exists\xi(\xi = \gamma) \longleftrightarrow \exists\xi(\varphi \wedge \xi = \gamma) \longleftrightarrow \exists\xi(\psi \wedge \xi = \gamma)$. $\square$

Das folgende Lemma zeigt wie ein Quantor in einem bestimmten Kontext eliminiert werden kann. Man beachte, daß hier eine der Eliminationsmengen-Technik verwandte Idee verwendet wird.

Lemma 3.2. Für $i \in I$ seien y_i, z_i K-Terme, in denen X nicht vorkommt, ξ_i seien Γ-Variablen, und ψ_i seien Formeln, in denen X nicht vorkommt. Dann gilt

$$\bigvee_{j \in I} \exists X \Big(\bigwedge_{i \in I} \big[\big(y_i \neq 0 \wedge V(y_i X + z_i) = \xi_i \wedge \xi_j = \infty \big) \vee \psi_i \big] \Big) \longleftrightarrow$$
$$\bigvee_{j \in I} \Big(\bigwedge_{i \in I} \big[\big(y_i \neq 0 \wedge V\big(y_i(-z_j/y_j) + z_i\big) = \xi_i \wedge \xi_j = \infty \big) \vee \psi_i \big] \Big).$$

Beweis. Fixiere eine Belegung aller freien Variablen. Sei $k \in I$ mit $\xi_k = \infty$. Interpretiere X so, daß

$$\bigwedge_{i \in I} \big(y_i \neq 0 \wedge V(y_i X + z_i) = \xi_i \wedge \xi_k = \infty \big)$$

gilt. Für $i = k$ folgt $y_k \neq 0$ und $y_k X + z_k = 0$, also war $X = -z_k/y_k$ die einzig mögliche erfüllende Interpretation von X. Damit folgt die Äquivalenz. $\square$

Lemma 3.3. Sei φ eine K-quantorenfreie Formel, die linear in X ist, und sei $\{\, y_i X + z_i \mid i \in I \,\}$ die Menge der K-Terme in φ, die X enthalten. Dann gibt es eine zu $\exists X(\varphi)$ äquivalente Formel der Form

$$\exists \xi_1 \ldots \exists \xi_n \Big(\bigvee_{J \subseteq I} \Big[\exists X \Big(\bigwedge_{j \in J} \big(y_j \neq 0 \wedge V(y_j X + z_j) = \xi_j \wedge \xi_j < \infty \big) \Big) \wedge \psi_J \Big] \Big) \vee \psi'.$$

Dabei haben wir $I = \{1, \ldots, n\}$ angenommen, um die ξ_i benennen zu können. Dies sind Γ-Variablen, die in φ nicht vorkommen. Die ψ_J und ψ' sind K-quantorenfreie Formeln, in denen X nicht vorkommt und die linear in allen K-Variablen sind, in denen φ linear ist.

Beweis. Durch iterative Anwendung von Lemma 3.1 für jedes $V(y_i X + z_i)$ erhält man eine zu $\exists X(\varphi)$ äquivalente Formel der Form

$$\exists \xi_1 \ldots \exists \xi_n \Big[\exists X \Big(\bigwedge_{i \in I} V(y_i X + z_i) = \xi_i \Big) \wedge \psi'' \Big].$$

Dabei ist ψ'' aus φ entstanden, indem jedes $V(y_i X + z_i)$ durch ξ_i ersetzt wurde. Dies ist wiederum äquivalent zu folgender Formel, wobei ψ_i für $V(z_i) = \xi_i$ steht.

$$\exists \xi_1 \ldots \exists \xi_n \Big[\exists X \Big(\bigwedge_{i \in I} \big[\big(y_i \neq 0 \wedge V(y_i X + z_i) = \xi_i \big) \vee \psi_i \big] \Big) \wedge \psi'' \Big].$$

Unter Verwendung von Lemma 3.2 und eines Distributivgesetzes erhält man eine Formel der Form

$$\exists \xi_1 \ldots \exists \xi_n \Big[\exists X \Big(\bigwedge_{i \in I} \big[\big(y_i \neq 0 \wedge V(y_i X + z_i) = \xi_i \wedge \xi_i < \infty \big) \vee \psi_i \big] \Big) \wedge \psi'' \Big] \vee \psi'.$$

Wir konstruieren eine DNF vom Skopus des Existenzquantors. Das Ergebnis sieht folgendermaßen aus:

$$\exists \xi_1 \ldots \exists \xi_n \Big[\exists X \Big(\bigvee_{J \subseteq I} \Big[\bigwedge_{j \in J} \big(y_j \neq 0 \wedge V(y_j X + z_j) = \xi_j \wedge \xi_j < \infty \big) \wedge$$
$$\bigwedge_{i \in I \setminus J} \psi_i \Big] \Big) \wedge \psi'' \Big] \vee \psi'.$$

Daraus erhält man leicht die gewünschte Form. $\square$

Lemma 3.4. Für $\mu \in \Gamma$, $a \in K$ und $I \subseteq \mathbb{N}$ endlich gilt $\bigwedge_{i \in I} v(a + c_i) = \mu$ genau dann, wenn eine Teilmenge $J \subseteq I$ existiert, so daß

$$\bigwedge_{j \in J} \big(v(a + c_j) = \mu\big) \wedge \bigwedge_{\substack{j,j' \in J \\ j \neq j'}} \big(v(c_j - c_{j'}) = \mu\big) \wedge \bigwedge_{i \in I \setminus J} \bigvee_{j \in J} \big(v(c_j - c_i) > \mu\big).$$

Beweis. Wir zeigen die Implikation durch Induktion über $|I|$. Falls $|I| = 1$, setze $J = I$. Falls $|I| > 1$ wähle $k \in I$ setze $I' = I \setminus \{k\}$. Nach Induktionsannahme existiert $J' \subseteq I'$ mit den geforderten Eigenschaften. Wegen der Dreiecksungleichung ist

$$v(c_k - c_j) = v(a + c_k - (a + c_j)) \geqslant \mu \quad \text{für alle } j \in J'.$$

Falls für alle $j' \in J'$ Gleichheit gilt, setze $J = J' \cup \{k\}$. Sonst setze $J = J'$. Die Replikation folgt sofort unter Verwendung der Dreiecksungleichung. $\square$

Lemma 3.5. Gegeben sei eine Formel φ von folgender Form:

$$\bigwedge_{i \in I} \big(y_i \neq 0 \wedge V(y_i X + z_i) = \xi_i \wedge \xi_i < \infty\big),$$

Dabei sind die die y_i und z_i K-Terme, die X nicht enthalten, und die ξ_i sind Γ-Variablen. Dann kann man eine äquivalente Formel φ' von folgender Form konstruieren:

$$\bigvee_{J \subseteq I} \bigvee_{L \subseteq J} \Big(\bigwedge_{l \in L} \big(V(X + c_l) = \gamma_l \wedge \gamma_l = \gamma_m \wedge \gamma_m < \infty \wedge \psi_L\big) \wedge \bigwedge_{\substack{l,l' \in L \\ l \neq l'}} V(c_l - c_{l'}) = \gamma_l \Big).$$

Dabei sind die c_l K-Terme, die X nicht enthalten, es ist $m \in J$ in jedem Zweig der äußeren Disjunktion, und die ψ_L sind quantorenfreie Formeln, in denen X nicht vorkommt.

Beweis. Zunächst normieren wir überall die Faktoren von X weg. Setze $a = \prod_{i \in I} y_i$ und für $i \in I$ setze $c_i = z_i / a_i$ und $\gamma_i = \xi_i - V(a_i)$. Damit ist φ äquivalent zu

$$\bigwedge_{i \in I} \big(a \neq 0 \wedge V(X + c_i) = \gamma_i \wedge \gamma_i < \infty\big). \qquad (\varphi_1)$$

Im nächsten Schritt konstruieren wir eine Fallunterscheidung darüber, was die Menge J aller $j \in I$ mit $\gamma_j = \max\{\, \gamma_i \mid i \in I \,\}$ ist. Dabei sei $m \in J$, also γ_m maximal in $\{\, \gamma_i \mid i \in I \,\}$. Für die $i \in I \setminus J$ gilt nach Lemma 2.14, daß $V(X + c_i) = V(c_i - c_m)$. Damit ist φ_1 äquivalent zu

$$\bigvee_{J \subseteq I} \Big[\bigwedge_{j \in J} \big(V(X + c_j) = \gamma_j \wedge \gamma_j = \gamma_m \wedge \gamma_m < \infty\big) \wedge \bigwedge_{i \in I \setminus J} \big(V(c_i - c_m) = \gamma_i \wedge \gamma_i < \gamma_m\big) \wedge a \neq 0 \Big], \qquad (\varphi_2)$$

wobei in jedem Disjunktionsglied m irgendein Element aus J ist. Unter jeder φ_1 und damit φ_2 erfüllenden Belegung aller Variablen ist in φ_2 wegen der Anordnung der γ_i genau ein Zweig der Disjunktion wahr. Nach Lemma 3.4 ist φ_2 äquivalent zu

$$\begin{aligned}\bigvee_{J\subseteq I}\Big[\bigvee_{L\subseteq J}\Big(&\bigwedge_{l\in L}\big(V(X+c_l)=\gamma_l\wedge\gamma_l=\gamma_m\wedge\gamma_m<\infty\big)\wedge\\ &\bigwedge_{l\neq l'\in L}V(c_l-c_{l'})=\gamma_l\wedge\\ &\bigwedge_{j\in J\setminus L}\bigvee_{l\in L}\big(V(c_l-c_j)>\gamma_j\wedge\gamma_j=\gamma_m)\big)\Big)\wedge\\ \bigwedge_{i\in I\setminus J}&\big(V(c_i-c_m)=\gamma_i\wedge\gamma_i<\gamma_m\big)\wedge a\neq 0\Big].\end{aligned}\tag{φ_3}$$

Durch Anwendung eines Distributivgesetzes erhält man die gewünschte Form φ'. □

In Termini von Definition 2.16 ist in φ_2 unter jeder erfüllenden Interpretation genau der Zweig mit $J=\operatorname{top}\big(\{\,c_i\mid i\in I\,\},X\big)$ wahr. Der folgende Schritt nach φ_3 weicht vom Vorgehen im vorigen Kapitel ab. Nehmen wir wieder $\gamma_m=0$ an, so wird hier eine Fallunterscheidung darüber aufgestellt, wie viele verschiedene $\overline{-c_l}$ es in K_v gibt, also wie viele Restklassen $\overline{X}$ vermeiden muß. Während bei den Verfahren im vorigen Kapitel an entsprechender Stelle genügend viele Restklassen disjunktiv ausprobiert werden, bleibt man bei diesem Verfahren nichtkonstruktiv. Die im vorigen Kapitel verwendeten Testpunkte tauchen im Beweis zu folgender Proposition auf. Man beachte, daß die Formulierung der Proposition nichtkonstruktiv ist.

Proposition 3.6. *Sei $\mu\in\Gamma$, $c_1,\ \dots,\ c_n\in K$, so daß $v(c_i-c_j)=\mu$ für alle i, $j\in\{1,\dots,n\}$ mit $i\neq j$. Dann sind folgende Aussagen äquivalent:*

(1) *Es existiert ein $a\in K$ mit $v(a+c_i)=\mu$ für alle $i\in\{1,\dots,n\}$.*
(2) *Es gibt $c_1',\ \dots,\ c_n'\in K$, so daß $v(c_i')=\mu$ und $v(c_i'-c_j')=\mu$ für alle i, $j\in\{1,\dots,n\}$ mit $i\neq j$.*
(3) *Es ist $|K_v|\geqslant n+1$, mit anderen Worten: Es gilt E_{n+1}.*

Beweis. (1) $\Longrightarrow$ (2): Für $i\in\{1,\dots,n\}$ setze $c_i'=a+c_i$. Dann gilt $v(c_i')=\mu$ und für $j\in\{1,\dots,n\}$ mit $j\neq i$ ist $v(c_i'-c_j')=v\big(a+c_i-(a+c_j)\big)=v(c_i-c_j)=\mu$.

(2) $\Longrightarrow$ (3): Für $i\in\{1,\dots,n\}$ ist $v(c_i'/c_1')=0$, also $\overline{c_i'/c_1'}\in K_v^\times$. Die Restklassen sind paarweise verschieden, denn angenommen es gibt $j\in\{1,\dots,n\}$ mit $j\neq i$, so daß $\overline{c_i'/c_1'}=\overline{c_j'/c_1'}$. Dann ist $v(c_i'/c_1'-c_j'/c_1')>0$, also $v(c_i'-c_j')>v(c_1')=\mu$, ein Widerspruch.

(3) $\Longrightarrow$ (1): Wegen $|K_v^\times|\geqslant n$ gibt es ein $b\in K$ mit $v(b)=0$, so daß $\overline{b}$ von allen $\overline{c_i/c_1}$ für $i\in\{2,\dots,n\}$ verschieden ist, d. h. es gilt $v(c_i/c_1-b)=0$, und mit $a=-c_1b$ folgt $v(a+c_i)=v(c_1)=\mu$. □

Korollar 3.7. *Zu einer gegebenen K-pränexen linearen Formel kann man eine in jedem Körper mit jeder Bewertung äquivalente K-quantorenfreie Formel berechnen.*

Beweis. Wir eliminieren zunächst den innersten K-Quantor. Wegen $\forall X(\varphi)\longleftrightarrow\neg\exists X(\neg\varphi)$ können wir o. B. d. A. annehmen, daß dies ein Existenzquantor ist. Wende zuerst Lemma 3.3 und dann auf die Matrix des Ergebnisses Lemma 3.5 an. Ziehe den Existenzquantor in die Disjunktionen. Nach Proposition 3.6 kann man

$$\exists X\Big(\bigwedge_{l\in L}\big(V(X+c_l)=\gamma_l\wedge\gamma_l=\gamma_m\wedge\gamma_m<\infty\wedge\psi_L\big)\Big)$$

jeweils durch $E_{|L|+1}\wedge\psi_L$ ersetzen. Da die entstandene Matrix linear in allen Variablen ist, in denen die Ausgangsmatrix linear war, läßt sich das Verfahren iterieren. □

Bemerkung 3.8. Alternativ zu den nullstelligen Prädikaten E_n kann man auch die Sprache der Körper um eine Konstante ζ erweitern, die wie im vorigen Kapitel zu interpretieren ist. Vorausgesetzt, daß man beides zur Verfügung hat, gilt nämlich

$$E_n \longleftrightarrow \bigwedge_{i=1}^{n-2} \zeta^i \neq 1$$

für alle $n \in \mathbb{N}$, mit anderen Worten: Man kann die E_n unter Verwendung von ζ quantorenfrei ausdrücken.

KAPITEL 4

Implementierung eines Eliminationsverfahrens für die rationalen Zahlen mit p-adischer Bewertung

Das in Kapitel 2, Abschnitt 2.4 beschriebene Eliminationsverfahren wurde für den Spezialfall des Körpers der rationalen Zahlen implementiert. Die Implementierung im Computeralgebra-System REDUCE baut auf dem Logikpaket REDLOG des Autors auf [Hea93], [Mel94], [Stu95]. Diese Arbeit geht nicht auf die technische Seite der Implementierung ein. Der Abschnitt über Simplifikation schneidet einige mathematische Aspekte an, die für die Implementierung relevant sind, aber nicht unmittelbar mit dem eigentlichen Eliminationsverfahren zusammenhängen. Im zweiten Abschnitt geben wir Beispiele für automatisch durchgeführte Eliminationen.

4.1. Simplifikation

Während der Elimination wird jedes Zwischenergebnis simplifiziert. Dafür steht in REDLOG ein Simplifier für Formeln erster Stufe zur Verfügung. Er erwartet Parameterfunktionen, die theoriespezifische Simplifikationen implementieren. Dies sind das *Zusammenziehen von Relationen* und die *Simplifikation atomarer Formeln.*

Lemma 4.1. Falls $a \longrightarrow b$, so ist $a \wedge b$ äquivalent zu a und $a \vee b$ äquivalent zu b.

Beweis. Gelte $a \longrightarrow b$ und $a \wedge b$, so gilt sicher a. Gelte umgekehrt $a \longrightarrow b$ und a, so gilt b und damit $a \wedge b$. Nun zum disjunktiven Fall. Gelte $a \longrightarrow b$ und $a \vee b$. Falls a gilt, so gilt b wegen der Implikation. Gelte umgekehrt b, so folgt $a \vee b$. $\square$

Lemma 4.2 (Zusammenziehen von Relationen). Für feste Terme s und t betrachten wir Konjunktionen und Disjunktionen von atomaren Formeln, die möglicherweise über verschiedene Relationen aufgebaut sind, aber alle s auf der linken und t auf der rechten Seite haben. Folgende Tabellen geben für verschiedene Wahlen von zwei Relationen ϱ und σ entweder eine Relation τ an, so daß $s\ \varrho\ t \wedge s\ \sigma\ t$ bzw. $s\ \varrho\ t \vee s\ \sigma\ t$ äquivalent zu $s\ \tau\ t$ ist, oder einen äquivalenten Wahrheitswert. Wo ein „–" als Tabelleneintrag steht, ist das nicht möglich.

$\wedge$	$\neq$	$\parallel$	$\mid$	$\sim$	$=$
$\neq$	$\neq$	$\parallel$	–	–	false
$\parallel$		$\parallel$	$\parallel$	false	false
$\mid$			$\mid$	$\sim$	$=$
$\sim$				$\sim$	$=$
$=$					$=$

$\vee$	$\neq$	$\parallel$	$\mid$	$\sim$	$=$
$\neq$	$\neq$	$\neq$	true	true	true
$\parallel$		$\parallel$	$\mid$	$\mid$	–
$\mid$			$\mid$	$\mid$	$\mid$
$\sim$				$\sim$	$\sim$
$=$					$=$

Beweis. Betrachte zunächst die Tabelle für die Konjunktion. Der jeweils erste Eintrag jeder Zeile folgt aus der Idempotenz von $\wedge$. Die drei false-Einträge sind offensichtliche Widersprüche. Der Rest folgt aus Lemma 4.1. Nun zur Tabelle für die Disjunktion. Wieder folgt der erste Eintrag jeder Zeile aus der Idempotenz von $\vee$. Der jeweils zweite Zeileneintrag folgt aus Lemma 4.1; ebenso der dritte Eintrag der dritten Zeile. Weiter ist $s \neq t \vee s \mid t$ äquivalent zu $s = t \longrightarrow s \mid t$, was offensichtlich ist. Mit derselben Argumentation ist $s \neq t \vee s \sim t$ wahr. Der Zusammenhang zwischen $\neq$ und $=$ ist klar. Die Äquivalenz zwischen $s \parallel t \vee s \sim t$ und $s \mid t$ folgt unmittelbar aus der Definition der drei Relationen. $\square$

Man sieht, daß man, falls eine Vereinfachung möglich ist, entweder einen Wahrheitswert bekommt, der die gesamte betrachtete Disjunktion oder Konjunktion zusammenbrechen läßt, oder eines der Relationssymbole, die schon da waren. Daraus folgt, daß beim Zusammenziehen von mehr als zwei Relationen die Reihenfolge unerheblich für das Endergebnis ist.

Alle Gleichungen und Ungleichungen werden, wie wir später noch sehen, dahingehend simplifiziert, daß ihre rechte Seite 0 ist. Für das Zusammenziehen von diesen Relationen mit $\parallel$, $\mid$ und $\sim$ wird versucht, durch Subtraktion eines Subterms auf die rechte Seite die Terme der anderen atomaren Formel zu matchen.

Wir kommen nun zur Simplifikation atomarer Formeln. In unserer Implementierung sind die Terme in den atomaren Formeln als Polynome über $\mathbb{Z}$ repräsentiert. Bei vorgegebener Bewertung ist π, das Körperelement von minimalem positiven Wert, die entsprechende Primzahl, sonst die Variable p. Im zweiten Fall führen wir folgende p betreffende Simplifikationen durch, wobei die jeweils letzte Komponente einer Äquivalenzkette die gewählte kanonische Form ist.

Lemma 4.3. Gegeben sei eine p-adische Bewertung von $\mathbb{Q}$. Für $a \in \mathbb{Z}[\underline{X}, p]$, $z \in \mathbb{Z}$ mit $z \neq 0$ und $n \in \mathbb{N}$ gelten folgende Äquivalenzen:

$$\begin{aligned} zp^n = 0 &\longleftrightarrow \text{false}, \\ zp^n \neq 0 &\longleftrightarrow \text{true}, \\ ap^n = 0 &\longleftrightarrow a = 0, \\ ap^n \neq 0 &\longleftrightarrow a \neq 0, \\ 1 \mid zp^n \longleftrightarrow 1 \parallel zp^n \longleftrightarrow zp^n \mid 0 \longleftrightarrow zp^n \parallel 0 &\longleftrightarrow \text{true}, \\ 0 \mid zp^n \longleftrightarrow 0 \parallel zp^n \longleftrightarrow zp^n \mid 1 \longleftrightarrow zp^n \parallel 1 &\longleftrightarrow \text{false}, \\ zp^n \sim 0 \longleftrightarrow 0 \sim zp^n \longleftrightarrow zp^n \sim 1 \longleftrightarrow 1 \sim zp^n &\longleftrightarrow \text{false}. \quad \square \end{aligned}$$

Hier liegt ein Ansatzpunkt für zukünftige Verbesserungen; z. B. weiß man, daß $p - 1 \sim 1 \longleftrightarrow \text{true}$. Nach Lemma 1.14 darf man beide Seiten einer atomaren Formel durch ihren ggT über $\mathbb{Z}$ dividieren, wenn man berücksichtigt, daß dieser unter bestimmten Belegungen der Variablen Null sein kann.

Lemma 4.4. Gegeben sei eine p-adische Bewertung von $\mathbb{Q}$. Seien f, $g \in \mathbb{Z}[\underline{X}, p]$ mit f, $g \neq 0$. Setzt man $h = \text{ggT}(f, g)$, $f_h = f/h$ und $g_h = g/h$, so gilt

$$\begin{aligned} f \parallel g &\longleftrightarrow f_h \parallel g_h \wedge h \neq 0, \\ f \mid g &\longleftrightarrow f_h \mid g_h \vee h = 0, \\ f \sim g &\longleftrightarrow f_h \sim g_h \vee h = 0. \quad \square \end{aligned}$$

Die folgenden Vereinfachungen sind Spezialfälle der Anwendung von Lemma 4.4 mit einfachen Weitervereinfachungen:

$$\begin{aligned} 0 \parallel f &\longleftrightarrow \text{false}, \\ f \parallel 0 &\longleftrightarrow f \neq 0, \\ 0 \mid f \longleftrightarrow 0 \sim f \longleftrightarrow f \sim 0 &\longleftrightarrow f = 0, \\ f \mid 0 &\longleftrightarrow \text{true}. \end{aligned}$$

Nach Anwendung von Lemma 4.4 sind insbesondere die Inhalte von f_h und g_h teilerfremd. Es wäre offensichtlich korrekt und auch wünschenswert, diese durch ihre quadratfreien Teile zu ersetzen, aber wir halten den Aufwand der dazu notwendigen Integer-Faktorisierung für nicht angemessen. Wenn die Bewertung bekannt ist, kann man folgende Vereinfachung durchführen.

Lemma 4.5. Gegeben sei eine p-adische Bewertung von $\mathbb{Q}$. Seien $f,\, g \in \mathbb{Z}[\underline{X}]$ mit $f,\, g \neq 0$. Wir faktorisieren f und g in Inhalt und primitiven Teil: $f = c_f \cdot f^*$ und $g = c_g \cdot g^*$. Für $\varrho \in \{|, \|, \sim\}$ gilt mit $\delta = |v(c_f) - v(c_g)|$ im Fall $v(c_f) \leqslant v(c_g)$, daß

$$f \;\varrho\; g \longleftrightarrow f^* \;\varrho\; p^\delta g^*.$$

Entsprechend gilt im Fall $v(c_f) > v(c_g)$, daß $f \;\varrho\; g \longleftrightarrow p^\delta f^* \;\varrho\; g^*$. □

Zwar schließt obiges Lemma auch den Fall $f,\, g \in \mathbb{Z}$ ein, aber in diesem Fall können wir sofort zu true oder false evaluieren. Auf Seite 34 haben wir algorithmisch zusammengefaßt, wie die Simplifikation atomarer Formeln im einzelnen abläuft.

4.2. Beispiele für automatisch durchgeführte Eliminationen

In Bezug auf die Uniformität des Eliminationsergebnisses bietet die Implementierung drei Wahlmöglichkeiten:

(1) Vollkommen uniforme Elimination unter Verwendung von Korollar 2.35.
(2) Elimination für p-adische Bewertungen bis zu einem zu wählenden p nach Korollar 2.37.
(3) Wie in (2), aber p wird auf die entsprechende Primzahl gesetzt. Wie wir im letzten Abschnitt gesehen haben, lassen sich atomare Formeln dadurch besser simplifizieren. Das Ergebnis ist allerdings nur für das gewählte p korrekt.

In den Beispielformeln bindet $\wedge$ stärker als $\vee$. Die Zeitangaben beziehen sich auf eine SUN SPARC-10. Wo nicht ausdrücklich auf etwas anderes hingewiesen wird, haben wir vollkommen uniform eliminiert. Eliminationen vom Typ (2) kommen in den Beispielen nicht vor. Sie verliefen bei den gewählten Beispielformeln was Zeit und Ergebnisgröße angeht in etwa wie die vollkommen uniformen. Bei den Eliminationen vom Typ (3), also mit konretem p, hingegen macht sich die bessere Simplifikation deutlich bemerkbar.

4.2.1. Unendlichkeit des Wertes von 0.

Wir suchen eine quantorenfreie Beschreibung aller Elemente a, die irgendein Element strikt teilen. Die Eingabe ist $\exists x(a \parallel x)$. Die Ausgabe $a \neq 0$ erhält man nach 0 ms.

Algorithmus 4.6 (Simplifikation atomarer Formeln). *Eingabe:* Eine atomare Formel $f \varrho g$, wobei $f, g \in \mathbb{Z}[\underline{X}, p]$ und $\varrho \in \{=, \neq, \|, |, \sim\}$. *Ausgabe:* Eine äquivalente Formel α'. *Methode:*

$\langle$*Simplifiziere die atomare Formel* $f \varrho g\rangle \equiv$
    if $\varrho \in \{=, \neq\}$ **then**
        $\langle$*Körpertheoretische Vereinfachung von* $f \varrho g$ s. u.$\rangle$
    else
        $\langle$*Bewertungstheoretische Vereinfachung von* $f \varrho g$ s. u.$\rangle$
    fi
$\langle$*Körpertheoretische Vereinfachung von* $f \varrho g\rangle \equiv$
    $h :=$ Der primitive Teil von $f - g$ mit $\mathrm{HC}(h)$ positiv
    if $h = zp^n$ für $0 \neq z \in \mathbb{Z}$ **then**
        Evaluiere zu $\alpha' \in \{\text{true}, \text{false}\}$
    else if $h = ap^n$ für beliebiges Polynom a **then**
        $\alpha' := a \varrho 0$
    else
        $\alpha' := h \varrho 0$
    fi
$\langle$*Bewertungstheoretische Vereinfachung von* $f \varrho g\rangle \equiv$
    Mache $\mathrm{HC}(f)$ und $\mathrm{HC}(g)$ positiv
    if $f = g$ **then**
        if $\varrho = \|$ **then** $\alpha' :=$ false **else** $\alpha' :=$ true **fi**
        exit
    fi
    Berechne $f_h \varrho g_h \omega h \sigma 0$ nach Lemma 4.4
    $\alpha'_1 := f_h \varrho g_h$
    $\langle$*Körpertheoretische Vereinfachung von* $h \sigma 0$ s. o.$\rangle$ zu α'_2
    if p bekannt **then**
        if $f_h \in \mathbb{Z} \wedge g_h \in \mathbb{Z}$ **then**
            Evaluiere zu $\alpha'_1 \in \{\text{true}, \text{false}\}$
        else
            $\alpha'_1 := f^*_h \varrho p^\delta g^*_h$ oder $p^\delta f^*_h \varrho g^*_h$ wie in Lemma 4.5
        fi
    else
        if α'_1 setzt 0 oder 1 in Relation zu zp^n für $0 \neq z \in \mathbb{Z}$ **then**
            Evaluiere zu $\alpha'_1 \in \{\text{true}, \text{false}\}$
        fi
    fi
    if α'_1 von der Form $a \sim b$ **then**
        if $a \preccurlyeq b$ wobei $\preccurlyeq$ Totalordnung auf $\mathbb{Z}[\underline{X}, p]$ **then**
            Vertausche a und b
        fi
    fi
    $\alpha' := \alpha'_1 \omega \alpha'_2$ mit Simplifikation von Wahrheitswerten

4.2.2. Dichte Wertegruppe. Folgende Formel besagt, daß die Wertegruppe dicht ist, was für $(\mathbb{Z}, +)$ nicht zutrifft:

$$\forall x \forall y \bigl(x \parallel y \longrightarrow \exists z(x \parallel z \wedge z \parallel y)\bigr).$$

Das Problem wird zunächst automatisch pränex und dann unter Verwendung von Lemma 2.39 positiv gemacht. Beim Positivmachen entsteht aus $x \parallel y$ in der Prämisse der Implikation die atomare Formel $y \mid x$. Bei der Elimination von $\exists z$ muß also Lemma 2.43 angewandt werden, um stattdessen eine strikte Teilbarkeit und eine Gleichung zu erhalten. Nach 170 ms erhält man die Antwort false.

4.2.3. Dreiecksungleichung. In den Eingabeformeln in diesem Beispiel kommt eine quantifizierte Variable auf beiden Seiten einer Relation vor. Im Verlauf der Elimination wird Korollar 2.12 angewendet. Wir codieren zunächst die Dreiecksungleichung in unserer Sprache: $\forall x \forall y(x \mid x + y \vee y \mid x + y)$. Das Eliminationsergebnis nach 34 ms ist

$$(p \mid p-1 \vee 1 \mid p-1) \wedge (p \mid p+1 \vee 1 \mid p+1) \wedge 1 \mid 2 \wedge \\ (1 \mid p+1 \vee p \mid p+1) \wedge (1 \mid p-1 \vee p \mid p-1).$$

Das sind 9 atomare Formeln. Man sieht leicht, daß jedes Konjunktionsglied wahr ist. Wenn $v(x) < v(y)$, so wissen wir $v(x+y) = v(x)$. Wir eliminieren

$$\forall x \forall y(x \parallel y \longrightarrow x + y \sim x)$$

und erhalten nach 34 ms folgendes Ergebnis mit 12 atomaren Formeln, das ebenfalls äquivalent zu true ist:

$$p-1 \sim 1 \wedge p+1 \sim 1 \wedge (1 \mid 2 \vee 2 \sim 1) \wedge (1 \mid 3 \vee 3 \sim 2) \wedge \\ (1 \mid p+1 \vee p+1 \sim p) \wedge (1 \mid p-1 \vee p-1 \sim p) \wedge (1 \mid 2 \vee 3 \sim 2).$$

Atomare Formeln wie $1 \mid 2$ im dritten Konjunktionsglied könnte man automatisch zu true vereinfachen: alle ganzen Zahlen werden von der 1 geteilt. Faßt man die beiden obigen Aussagen in der Formel $\forall x \forall y(x \sim y \vee x + y \sim x \vee x + y \sim y)$ zusammen, so erhält man nach 68 ms folgendes Eliminationsergebnis, das aus 20 atomaren Formeln besteht:

$$(2 \sim 1 \vee 3 \sim 1 \vee 3 \sim 2) \wedge (3 \sim 1 \vee 2 \sim 1 \vee 3 \sim 2) \wedge \\ (2 \sim 1 \vee 3 \sim 2 \vee 3 \sim 1) \wedge (p+1 \sim p \vee p+1 \sim 1) \wedge \\ (p-1 \sim p \vee p-1 \sim 1) \wedge (3 \sim 1 \vee 3 \sim 2 \vee 2 \sim 1) \wedge \\ (p+1 \sim 1 \vee p+1 \sim p) \wedge (p-1 \sim 1 \vee p-1 \sim p).$$

Auch hier sieht man, daß alle Konjunktionsglieder wahr sind. Betrachten wir das erste Konjunktionsglied: Nur eine Primzahl, nämlich p ist nicht zu 1 assoziiert. Auch in dieser Richtung wären automatische Simplifikationen denkbar.

4.2.4. Größe des Restklassenkörpers (1). Die folgende Formel beschreibt, daß der Restklassenkörper außer der 0 noch mindestens 4 verschiedene Elemente besitzt:

$$\exists x(x \sim 1 \wedge x \sim 2 \wedge x \sim 3 \wedge x \neq 1 \wedge x \neq 2 \wedge x \neq 3).$$

Sie ist in $\mathbb{Q}$ für p-adische Bewertungen mit $p \geqslant 5$ wahr. Nach etwa 153 ms erhält man folgendes Ergebnis mit 81 atomaren Formeln:

$$\begin{gathered}
p+3 \sim 3 \wedge p+3 \sim 2 \wedge p+3 \sim 1 \wedge p+2 \neq 0 \wedge p+1 \neq 0 \vee \\
11 \sim 3 \wedge 11 \sim 2 \wedge 11 \sim 1 \vee \\
2p+3 \sim 3 \wedge 2p+3 \sim 2 \wedge 2p+3 \sim 1 \wedge p+1 \neq 0 \wedge 2p+1 \neq 0 \vee \\
5 \sim 1 \wedge 15 \sim 2 \wedge 15 \sim 1 \vee \\
p+1 \sim 1 \wedge 3p+3 \sim 2 \wedge 3p+3 \sim 1 \wedge 3p+2 \neq 0 \wedge 3p+1 \neq 0 \vee \\
3 \sim 1 \wedge 2 \sim 1 \vee 3 \sim 2 \wedge 2 \sim 1 \vee \\
p-2 \sim 3 \wedge p-2 \sim 2 \wedge p-2 \sim 1 \wedge p-1 \neq 0 \wedge p+1 \neq 0 \vee \\
p+2 \sim 3 \wedge p+2 \sim 2 \wedge p+2 \sim 1 \wedge p+1 \neq 0 \wedge p-1 \neq 0 \vee \\
10 \sim 3 \wedge 5 \sim 1 \wedge 10 \sim 1 \vee \\
2p+2 \sim 3 \wedge p+1 \sim 1 \wedge 2p+2 \sim 1 \wedge 2p+1 \neq 0 \wedge 2p-1 \neq 0 \vee \\
3 \sim 2 \wedge 3 \sim 1 \vee 5 \sim 3 \wedge 5 \sim 2 \wedge 5 \sim 1 \vee 7 \sim 3 \wedge 7 \sim 2 \wedge 7 \sim 1 \vee \\
2p-1 \sim 3 \wedge 2p-1 \sim 2 \wedge 2p-1 \sim 1 \wedge 2p+1 \neq 0 \wedge p+1 \neq 0 \vee \\
p-1 \sim 3 \wedge p-1 \sim 2 \wedge p-1 \sim 1 \wedge p+1 \neq 0 \wedge p+2 \neq 0 \vee \\
p+1 \sim 3 \wedge p+1 \sim 2 \wedge p+1 \sim 1 \wedge p-1 \neq 0 \wedge p-2 \neq 0 \vee \\
2 \sim 1 \wedge 3 \sim 1 \wedge 6 \sim 1 \vee 3 \sim 1 \wedge 9 \sim 2 \wedge 9 \sim 1 \vee \\
4 \sim 1 \wedge 6 \sim 1 \wedge 12 \sim 1 \vee 4 \sim 3 \wedge 2 \sim 1 \wedge 4 \sim 1 \vee 8 \sim 3 \wedge 4 \sim 1 \wedge 8 \sim 1.
\end{gathered}$$

Wählt man vor der Elimination $p = 3$ fest, so erhält man nach 17 ms die Antwort false, und für $p = 5$ und $p = 100003$ nach 17 ms die Antwort true.

4.2.5. Größe des Restklassenkörpers (2). Wir wissen, daß für eine p-adische Bewertung $K_v = \mathbb{Z}/p$ ist, also ist stets $|K_v^\times| = p-1$ für p prim. Da 4 keine Primzahl ist, ist $|K_v^\times| = 3$ unmöglich. Die Formel

$$\forall x(x \sim 1 \wedge x \sim 2 \wedge x \sim 3 \longrightarrow x \sim 4)$$

ist genau dann wahr, wenn aus der Existenz von drei verschiedenen Elementen in $K_v^\times$ folgt, daß es auch noch ein viertes gibt. Nach etwa 17 ms erhalten wir das Eliminationsergebnis

$$\begin{aligned}
(4 \sim 1 \vee 2 \parallel 1 \vee 1 \parallel 2 \vee 3 \parallel 1 \vee 1 \parallel 3) \wedge (2 \mid 1 \vee 1 \parallel 2 \vee 3 \parallel 2 \vee 2 \parallel 3) \wedge \\
(4 \sim 3 \vee 1 \parallel 3 \vee 3 \parallel 1 \vee 2 \parallel 3 \vee 3 \parallel 2) \wedge \\
(p \parallel 4 \vee 4 \parallel p \vee p \parallel 2 \vee 2 \parallel p \vee 3p \parallel 4 \vee 4 \parallel 3p).
\end{aligned}$$

Das sind 20 atomare Formeln Für konkrete Wahlen $p = 2, 3, 5, 100003$ erhalten wir nach jeweils 17 ms true.

4.2.6. Erfüllbarkeit parametrischer Formeln. Man sieht leicht, daß die atomare Formel $ax + b \mid c$ bezüglich x genau dann erfüllbar ist, wenn $a \neq 0 \vee b \mid c$ gilt. Wir eliminieren $\exists x(ax + b \mid c)$ und erhalten nach 17 ms das Ergebnis

$$a+b \mid c \vee b \mid c \wedge a = 0 \vee a \neq 0 \wedge (bp+b \mid cp \vee a = 0) \vee a \neq 0 \wedge (b+c \mid c \vee a = 0).$$

Es enthält 9 atomare Formeln. Eliminiert man $\exists x(a_1x + b_1 \mid a_2x + b_2)$, so erhält man nach 34 ms folgendes Ergebnis mit 23 atomaren Formeln:

$$\begin{aligned} &a_1 + b_1 \mid a_2 + b_2 \vee a_2 \neq 0 \vee b_1 \mid b_2 \wedge a_1 = 0 \vee \\ &\qquad a_1b_1p + a_1b_1 \mid a_1b_2p + a_2b_1 \wedge a_1 \neq 0 \vee b_1 \mid b_2 \wedge a_1a_2^2 = 0 \vee \\ &\quad a_1a_2^2 \neq 0 \wedge (a_1^2 \mid a_1a_2 + a_2^2 \vee a_1b_2 - a_2b_1 = 0) \vee b_1 \mid b_2 \wedge a_1a_2 = 0 \vee \\ &\quad a_1^2b_1 \mid a_1a_2b_1 + a_1a_2b_2 - a_2^2b_1 \wedge a_1a_2 \neq 0 \vee b_1 \mid b_2 \wedge a_2 = 0 \vee \\ &b_1 \mid b_2 \wedge a_1^2 = 0 \vee a_1^2b_1 + a_1^2b_2 - a_1a_2b_1 \mid a_1^2b_2 + a_1a_2b_2 - a_2^2b_1 \wedge a_1^2 \neq 0 \vee \\ &\qquad\qquad a_1b_1 + a_1b_2 \mid a_1b_2 + a_2b_2 \wedge a_1 \neq 0. \end{aligned}$$

Wir möchten einen Eindruck von der Komplexität des Verfahrens bezüglich verschiedener Relationen bei wachsender Anzahl atomarer Formeln vermitteln. Dazu fassen wir Ergebnisgrößen und Rechenzeiten für die Elimination von

$$\varphi_n = \exists x\Big(\bigwedge_{i=1}^{n} a_ix + b_i \mid c_i\Big) \quad \text{und} \quad \psi_n = \exists x\Big(\bigwedge_{i=1}^{n} a_ix + b_i \sim c_i\Big)$$

für wachsendes n in folgender Tabelle zusammen. Man weiß, daß im Fall der φ_n die Größe der Eliminationsmenge linear in n ist; im Fall der ψ_n hingegen ist sie quadratisch.

n	φ_n		ψ_n	
	Größe	Zeit (ms)	Größe	Zeit (ms)
1	9	0	12	17
2	38	17	148	119
3	81	68	570	578
4	140	68	1560	2686
5	215	187	3490	10081
6	306	306	6828	33048
7	413	493	12138	97104
8	536	612	20080	249968
9	675	918	31410	570044
10	830	1207	46980	1174683

4.2.7. Kreise bezüglich des p-adischen Absolutbetrags. Zu jeder p-adischen Bewertung v_p kann man durch $|x|_p = p^{-v_p(x)} \in \mathbb{R}$ einen Absolutbetrag definieren. Mit der Definition $p^{-\infty} = 0$ erfüllt er offenbar

$$\begin{aligned} |x|_p &\geqslant 0 \quad \text{und} \quad |x|_p = 0 \longleftrightarrow x = 0, \\ |xy|_p &= |x|_p|y|_p, \\ |x + y|_p &\leqslant \max\big\{|x|_p, |y|_p\big\} \leqslant |x|_p + |y|_p. \end{aligned}$$

Damit kann man durch $\big\{\, x \in \mathbb{Q} \;\big|\; |x - a|_p \leqslant r \,\big\}$ einen *geschlossenen Kreis* und entsprechend durch $\big\{\, x \in \mathbb{Q} \;\big|\; |x - a|_p < r \,\big\}$ einen *offenen Kreis* um a mit Radius r definieren. Aus der starken Dreiecksungleichung folgt, daß für festes p je zwei Kreise, die nicht disjunkt sind, ineinander enthalten sind. Das wollen wir automatisch beweisen. Die Eingabeformel für den geschlossenen Kreis lautet

$$\forall r_1 \forall r_2 \forall a \forall b\big(\exists x(r_1 \mid x - a \wedge r_2 \mid x - b \wedge r_1 \mid r_2) \longrightarrow \forall y(r_2 \mid y - b \longrightarrow r_1 \mid y - a)\big).$$

Nach 901 ms erhält man folgende Formel, die aus 49 atomaren Formeln besteht. Sie ist äquivalent zu true:

$$\begin{gathered}(p^2 \mid p+1 \vee p+1 \neq 0) \wedge (1 \parallel p-1 \vee p-1 \mid 1) \wedge (3 \parallel 2p \vee 2p \mid 3) \wedge \\ (p-1 \parallel p^2 \vee p^2 \mid p-1) \wedge (2 \parallel 3p \vee 3p \mid 2) \wedge (1 \parallel p+1 \vee p+1 \mid 1) \wedge \\ (p+1 \parallel p^2 \vee p^2 \mid p+1) \wedge (p^2 \mid p+1 \vee p+1 = 0 \vee p+1 \parallel p^2 \wedge p+1 \neq 0) \wedge \\ (2 \parallel p \vee p \mid 2) \wedge (p \mid p-1 \vee p-1 \neq 0) \wedge (p \mid p+1 \vee p+1 \neq 0) \wedge \\ (p-1 \parallel p \vee p \mid p-1) \wedge (p+1 \parallel p \vee p \mid p+1) \wedge (1 \parallel p+1 \vee p+1 \parallel p \vee p+1 = 0) \wedge \\ (3p \mid 2 \vee 2 \parallel 3p) \wedge (p+1 \mid 1 \vee 1 \parallel p+1) \wedge (p \mid 2 \vee 2 \parallel p) \wedge \\ (2p \mid 3 \vee 3 \parallel 2p) \wedge (p^2 \mid p+1 \vee p+1 \parallel p^2) \wedge (p^2 \mid p-1 \vee p-1 \parallel p^2) \wedge \\ (p \mid p-1 \vee p-1 \parallel p) \wedge (p \mid p+1 \vee p+1 \parallel p) \wedge (1 \parallel p^2+p \vee p+1 \mid 1).\end{gathered}$$

Für $p = 100003$ erhält man nach 459 ms true. Das Eliminationsergebnis für offene Kreise ist mehr als doppelt so groß. Für die Eingabeformel

$$\forall r_1 \forall r_2 \forall a \forall b \bigl(\exists x(r_1 \parallel x-a \wedge r_2 \parallel x-b \wedge r_1 \mid r_2) \longrightarrow \forall y(r_2 \parallel y-b \longrightarrow r_1 \parallel y-a)\bigr).$$

erhält man nach 1496 ms folgende Formel, die aus 116 atomaren Formeln besteht:

$$\begin{gathered}(p{+}1 \neq 0 \wedge p^2{+}p = 0 \vee p{+}1 = 0 \vee p{+}1 \parallel p^2 \wedge p{+}1 \neq 0 \vee p \parallel p{+}1 \wedge p{+}1 \neq 0) \wedge \\ (3 \mid 2 \vee 2 \parallel 3) \wedge (2 \mid 3 \vee 3 \parallel 2) \wedge (p \mid p+1 \vee p+1 \parallel p \vee p+1 = 0) \wedge \\ (p \mid p-1 \vee p-1 \parallel p \vee p-1 = 0) \wedge (1 \parallel 2 \vee 3 \mid 2 \vee 2 \parallel 3) \wedge \\ (p+1 \mid 1 \vee 1 \parallel p+1) \wedge (1 \mid 2 \vee 2 \parallel 1) \wedge (1 \parallel 3 \vee 2 \mid 3 \vee 3 \parallel 2) \wedge \\ (1 \parallel p+1 \vee p \mid p+1 \vee p+1 \parallel p) \wedge (1 \parallel p-1 \vee p \mid p-1 \vee p-1 \parallel p) \wedge \\ (1 \parallel p-1 \vee p-1 \parallel p) \wedge (p \parallel p+1 \vee p+1 \parallel p^2 \vee p^2+p = 0 \vee p+1 = 0) \wedge \\ (1 \parallel 2 \vee 2 \parallel p) \wedge (p+1 = 0 \vee p+1 \neq 0 \wedge p^2+p \neq 0 \vee p+1 \neq 0 \wedge p^2+p = 0) \wedge \\ (p+1 \mid p \vee p \parallel p+1) \wedge (2 \parallel p \vee 1 \parallel 2) \wedge (3 \parallel 2p \vee 2 \parallel 3) \wedge \\ (p+1 \parallel p^2 \vee p \parallel p+1 \vee p+1 = 0) \wedge (p+1 \parallel p \vee 1 \parallel p+1 \vee p+1 = 0) \wedge \\ (2 \parallel 3p \vee 3 \parallel 2) \wedge (1 \parallel p+1 \vee p+1 \parallel p \vee p+1 = 0) \wedge \\ (1 \parallel p-1 \vee p-1 \parallel p \vee p-1 = 0) \wedge (2 \mid 1 \vee 1 \parallel 2) \wedge (1 \parallel 2 \vee 3 \mid 1 \vee 2 \parallel 3) \wedge \\ (p+1 \mid p \vee 1 \parallel p+1) \wedge (1 \parallel 3 \vee 2 \mid 1 \vee 3 \parallel 2) \wedge \\ (p+1 \neq 0 \wedge p^2+p = 0 \vee p+1 = 0 \vee p+1 \neq 0 \wedge p^2+p \neq 0) \wedge \\ (p \parallel p+1 \vee p+1 \mid p \vee p+1 = 0) \wedge (1 \parallel p+1 \vee p+1 \mid 1) \wedge (2 \parallel 1 \vee 1 \mid 2) \wedge \\ (3 \parallel 2 \vee 2 \mid 3) \wedge (p{+}1 \parallel p \vee p \mid p{+}1 \vee p{+}1 = 0) \wedge (p{-}1 \parallel p \vee p \mid p{-}1 \vee p{-}1 = 0) \wedge \\ (2 \parallel 3 \vee 3 \mid 2) \wedge (p \parallel p+1 \vee p+1 \mid p) \wedge (1 \parallel 2 \vee 2 \mid 1) \wedge (1 \parallel 2 \vee 2 \parallel 3 \vee 3 \mid 1) \wedge \\ (1 \parallel p+1 \vee p+1 \mid p) \wedge (1 \parallel 3 \vee 3 \parallel 2 \vee 2 \mid 1) \wedge (1 \parallel p+1 \vee p+1 \parallel p) \wedge \\ (p+1 \parallel p^2 \vee p \parallel p+1 \vee p^2+p = 0 \vee p+1 = 0).\end{gathered}$$

Auch diese Formel ist äquivalent zu true. Für $p = 100003$ erhält man nach 816 ms das Ergebnis true.

Zusammenfassung der Ergebnisse

Das erste Kapitel faßt grundlegende Eigenschaften von exponentiell bewerteten Körpern zusammen. Wir haben versucht, eine Intuition von den algebraischen Eigenschaften dieser Strukturen zu vermitteln, und einige Beispiele angegeben. Dabei haben wir das allgemeinere Konzept der Absolutbeträge, die oft als Bewertungen bezeichnet werden, außer Acht gelassen. Ihr Zusammenhang mit Bewertungen wird lediglich in einem Beispiel am Ende von Kapitel 4 angedeutet. Besonders intensiv haben wir uns mit den p-adischen Bewertungen der rationalen Zahlen beschäftigt.

Das zweite Kapitel gibt zunächst eine kurze Einführung in die Elimination durch Eliminationsmengen. Beim Beweis des in [Wei88] publizierten Eliminationsverfahrens haben wir das Problem in zwei Teile aufgespalten: Der eine ist unabhängig vom Restklassenkörper der Bewertung, der andere läßt sich auf das Vermeiden von Restklassen reduzieren. Es ist uns gelungen, das Problem des Vermeidens von Restklassen mit Hilfe eine Konstante ζ uniform, also unabhängig von der (diskreten) Bewertung zu lösen. Dazu ist anzumerken, daß man diese Konstante auch bei der bereits bekannten nicht uniformen Methode benötigt. Wir haben unsere Aufmerksamkeit wieder besonders auf die p-adischen Bewertungen von $\mathbb{Q}$ gerichtet und festgestellt, daß man in diesem Fall die Konstante ζ nicht benötigt. Anschließend haben wir in [LW93] publizierte Ideen für lineare Elimination in angeordneten Körpern auf unsere Situation übertragen. Wir konnten Eliminationsmengen angeben, die zwar kleiner sind als die bisher bekannten Skolemmengen, aber dieselbe Größenordnung haben. Aus der Existenz der uniformen Eliminationsmengen folgt ein modelltheoretischer Sachverhalt über elementare Erweiterungen bezüglich linearer Formeln.

Das dritte Kapitel beschreibt das in [Wei84] publizierte Verfahren zur linearen Quantorenelimination. Es trennt bewertungstheoretische Probleme in einen gruppentheoretischen Teil und Fragen über den Restklassenkörper auf. Dies ähnelt in gewisser Weise unserem Vorgehen im zweiten Kapitel. Bei dem Verfahren wird die zugrundeliegende Sprache um nullstellige Prädikate erweitert. Wir zeigen, daß ein Zusammenhang zwischen diesen Prädikaten und der Konstante ζ aus dem zweiten Kapitel besteht.

Das vierte Kapitel geht auf Methoden zur Simplifikation von Formeln in der Bewertungstheorie ein. Erfahrungen mit linearer reeller Quantorenelimination haben gezeigt, daß gute Vereinfachungsstrategien für eine brauchbare Implementierung unerläßlich sind. Man vergleiche dazu etwa [Bur90]. Einige Beispiele für automatisch durchgeführte Eliminationen sollen die Arbeit abrunden. Anhand der Beispiele haben wir mögliche Weiterentwicklungen des Simplifiers angedeutet.

Literaturverzeichnis

[Bur90] Klaus-Dieter Burhenne. Implementierung eines Algorithmus zur Quantorenelimination für lineare reelle Probleme. Diplomarbeit, Lehrstuhl Prof. Dr. V. Weispfenning, Universität Passau, 1990.

[BWK93] Thomas Becker, Volker Weispfenning, and Heinz Kredel. *Gröbner Bases, a Computational Approach to Commutative Algebra*, volume 141 of *Graduate Texts in Mathematics*. Springer, New York, 1993.

[End72] Otto Endler. *Valuation Theory*. Universitext. Springer, Berlin, Heidelberg, 1972.

[Hea93] Anthony C. Hearn. *Reduce User's Manual for Version 3.5*. RAND, Santa Monica, CA 90407-2138, October 1993.

[Knu68] Donald E. Knuth. *Fundamental Algorithms*, volume 1 of *The Art of Computer Programming*. Addison-Wesley, Reading, Massachusetts, second edition, 1968.

[LW93] Rüdiger Loos and Volker Weispfenning. Applying linear quantifier elimination. *The Computer Journal*, 36(5):450–462, 1993. Special issue on computational quantifier elimination.

[Mah81] Kurt Mahler. *P-adic Numbers and their Properties*. Cambridge University Press, Melbourne, second edition, 1981.

[Mel94] Herbert Melenk. *Reduce Symbolic Mode Primer*. Konrad-Zuse-Zentrum für Informationstechnik, Berlin, 1994. Available via anonymous ftp at `serv03.zib-berlin.de`, path `/pub/redlib/documents/symbolic.tex`.

[Stu95] Thomas Sturm. *Redlog, a Reduce Library of Algorithms for the Manipulation of First-Order Formulas*. Universität Passau, 1995. To appear.

[vdW93a] Bartel Leendert van der Waerden. *Algebra I*. Springer, Berlin, Heidelberg, ninth edition, 1993.

[vdW93b] Bartel Leendert van der Waerden. *Algebra II*. Springer, Berlin, Heidelberg, sixth edition, 1993.

[Wei84] Volker Weispfenning. Quantifier elimination and decision procedures for valued fields. In *Models and sets (Aachen, 1983)*, volume 1103 of *Lecture Notes in Mathematics*, pages 419–472. Springer, Berlin, New York, 1984.

[Wei86] Volker Weispfenning. Quantifier eliminable ordered Abelian groups. In S. Wolfenstein, editor, *Procedings of the First International Symposium on Ordered Algebraic Structures (Luminy-Marseilles, 1984)*, pages 113–126. Heldermann, Berlin, 1986.

[Wei88] Volker Weispfenning. The complexity of linear problems in fields. *Journal of Symbolic Computation*, 5(1):3–27, February 1988.

Verzeichnis der Definitionen

Eidesstattliche Erklärung

Ich versichere, daß ich diese Arbeit selbständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt habe. Alle Ausführungen, die wörtlich oder sinngemäß übernommen wurden, sind als solche gekennzeichnet. Diese Arbeit habe ich in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Passau, 19. Februar 1995

Thomas Sturm