Karlsruhe Institute of Technology

Entscheidungsverfahren mit Anwendungen in der Softwareverifikation

XII: Quantoren-Elimination

Carsten Sinz
Institut für Theoretische Informatik

23.01.2019

Foliensatz basiert z.T. auf Folien von Erika Abraham (RWTH Aachen) und Matthew England (Coventry U)

Einführung

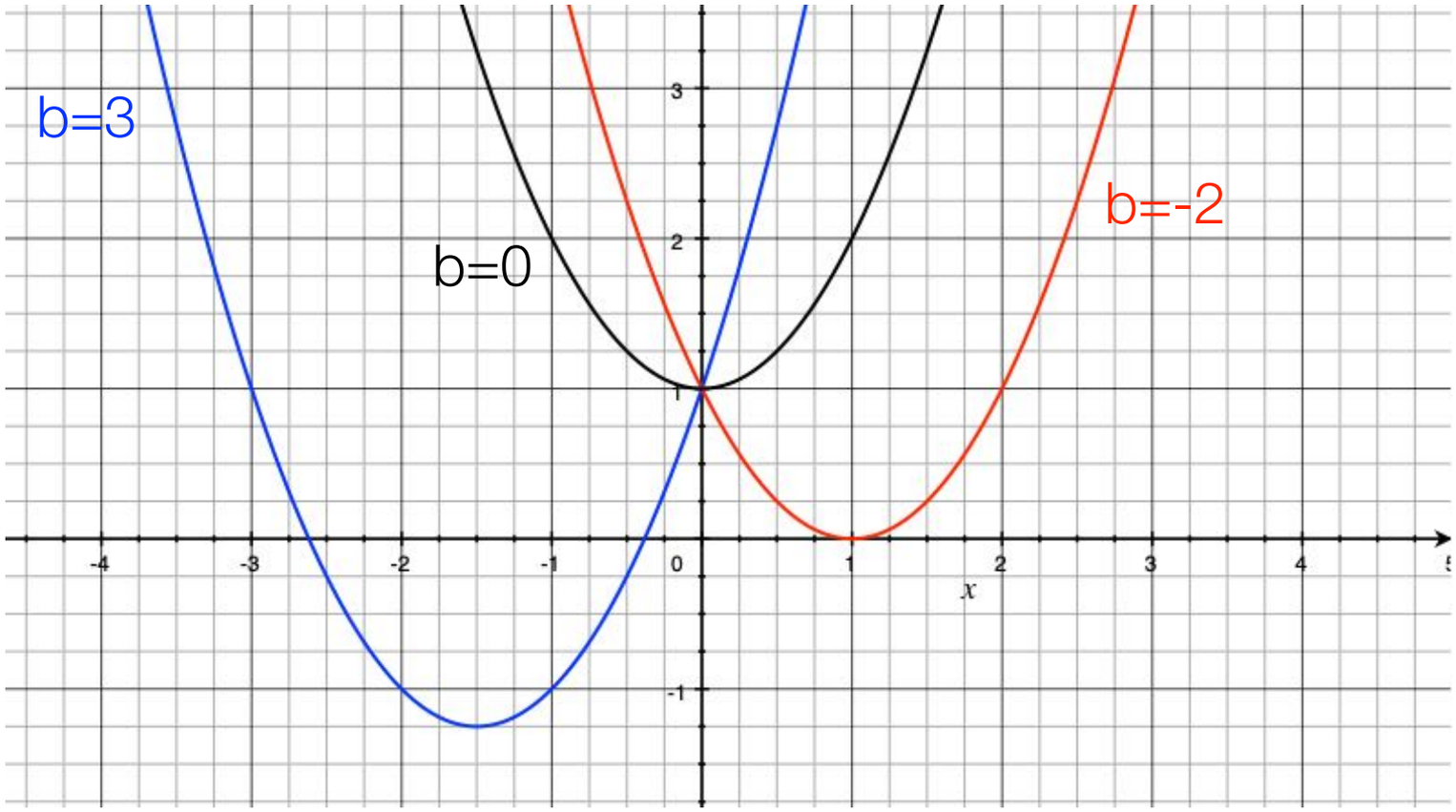
- Formeln dürfen auch Quantoren (∀, ∃) enthalten
- **Fragestellung Quantoren-Elimination (QE):**
  - Können wir eine Formel mit Quantoren in eine äquivalente ohne Quantoren transformieren?
  - Unter welchen Voraussetzungen (und für welche Theorien) ist dies möglich?
- **Häufiger Ansatz für Entscheidungsverfahren für quantifizierte Formeln basierend auf QE:**
  1. Eliminiere Quantoren
  2. Verwende dann Verfahren für quantorenfreies Fragment der Theorie
- Quantoren-Elimination häufig im Zusammenhang mit reeller (linearer und nichtlinearer) Arithmetik

Beispiele

Ausgangs-Formel	Quantor eliminiert
$\exists x \;.\; x^2 + 1 > 0$	$\top$
$\forall x \;.\; x^2 + 1 > 0$	$\top$
$\exists x \;.\; x^2 + 3x + 1 > 0$	$\top$
$\forall x \;.\; x^2 + 3x + 1 > 0$	$\bot$

Weiteres Beispiel

- Was ist mit $\forall x \,.\, x^2 + bx + 1 = 0$?
  - Für b=0 haben wir: $\forall x \,.\, x^2 + 1 = 0$, also $\top$ nach QE.
  - Für b=3 haben wir: $\forall x \,.\, x^2 + 3x + 1 = 0$, also $\bot$ nach QE.
  - D.h. die Lösung hängt von b ab.



Theorie der nicht-linearen reellen Arithmetik

- T_{NRA}: Theorie der nicht-linearen reellen Arithmetik
- **Kleines Problem:** Reelle Zahlen lassen sich nicht eindeutig durch eine Axiomatisierung in Prädikatenlogik erster Stufe charakterisieren (Satz von Löwenheim-Skolem)
- **Daher:** Betrachte *reell abgeschlossene Körper (real closed fields)* anstatt der reellen Zahlen
  - $\Sigma = \{ =, <, +, *, 0, 1, \dots \}$
  - Axiome Ax: (Tarski's Axiomatisierung)
    1. $<$ ist asymmetrisch, d.h. falls $x < y$, dann nicht $y < x$
    2. $<$ ist dichte Ordnung, d.h. falls $x<z$, existiert ein y mit $x<y$ und $y<z$
    3. $<$ ist Dedekind-vollständig, d.h. für alle Mengen $X, Y \subseteq \mathbb{R}$ gilt: wenn $x<y$ für alle $x \in X$ und $y \in Y$, dann gibt es ein z, so dass für alle $x \in X$ und $y \in Y$ gilt: falls $z \neq x$ und $z \neq y$, dann ist $x<z$ und $z<y$ (z separiert X und Y)

Theorie der nicht-linearen reellen Arithmetik

- T_{NRA}: Theorie der nicht-linearen reellen Arithmetik
- Axiome Ax: (Tarski's Axiomatisierung, Fortsetzung)
    4. x+(y+z) = (x+y)+z
    5. Für alle x, y existiert ein z mit x+z=y
    6. Falls x+y < z+w, dann x<z oder y<w
    7. 1<1+1
- Aus diesen Axiomen folgt bereits, dass eine eindeutige Operation * existiert mit den Eigenschaften der Multiplikation
- Axiom 3 kann mit einem Trick in Prädikatenlogik erster Stufe formuliert werden: Füge ein einstelliges Prädikat S und ein zweistelliges $\in$ hinzu, sowie die beiden Axiome:
    A. Falls x$\in$y, dann gilt S(y) und ¬S(x)
    B. < darf nur auf Elemente x, für die ¬S(x) gilt, angewendet werden

Weiteres Beispiel

- Betrachte die Formel $\exists x \,.\, x^2 + bx + c = 0$. (Nicht-quantifizierte Variablen können als Konstanten betrachtet werden)
  - Wir wollen ∃x eliminieren und interpretieren die Gleichung über den reellen Zahlen.
  - Wir kennen (aus der Schule) die Lösung(en) der quadratischen Gleichung:

$$x_{1/2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

  - D.h., die Gleichung besitzt eine reelle Lösung, falls $b^2 - 4c \geq 0$.
  - Ergebnis der Quantoren-Elimination wäre also $b^2 - 4c \geq 0$.

Tarski-Formeln

- **Definition:** Eine Tarski-Formel ist eine Formel aus T_{NRA}, bei der die atomaren Formeln die Gestalt p σ 0 besitzen mit $\sigma \in \{ =, <, > \}$ und p ein multivariates Polynom ist (wir können ganzzahlige Koeffizienten annehmen). Eine Tarski-Formel darf am Anfang auch beliebig viele Quantoren (∀,∃) enthalten.
- Formeln mit Quantoren am Beginn der Formel werden auch Formeln in **pränexer Normalform** genannt.
- **Anmerkung:** Tarski-Formeln beschäftigen sich also grob gesagt mit Nullstellen von Polynomen

Umformungen mit Quantoren

- Jede Formel lässt sich in pränexe Normalform (PNF) bringen
- Es gelten die folgenden Äquivalenzen:

$$\begin{aligned}
\forall x \,.\, F(x) &\equiv \neg \exists x \,.\, \neg F(x) \\
\exists x \,.\, F(x) \vee G(x) &\equiv \exists x \,.\, F(x) \vee \exists x \,.\, G(x) \\
\forall x \,.\, F(x) \wedge G(x) &\equiv \forall x \,.\, F(x) \wedge \forall x \,.\, G(x) \\
F \wedge \exists x \,.\, G(x) &\equiv \exists x \,.\, F \wedge G(x) \\
F \vee \forall x \,.\, G(x) &\equiv \forall x \,.\, F \vee G(x)
\end{aligned}$$

  (wobei in den letzten beiden Äquivalenzen, x nicht (frei) in F vorkommen darf)

- Mittels dieser Äquivalenzen lässt sich immer eine PNF herstellen

Idee der Quantoren-Elimination

- **Gegeben:** Tarski-Formel F mit n Quantoren
- **Vorgehen:**
  1. Bringe F in pränexe Normalform

$$F \quad \equiv \quad Q_1 x_1 \ldots Q_n x_n \ : \ F_n(x_1, \ldots, x_n)$$

wobei F_n eine quantorenfreie Formel über den Variablen x_1, …, x_n ist.

  2. Eliminiere iterativ (von innen nach außen) Quantoren:

$$\begin{aligned} F \quad &\equiv \quad Q_1 x_1 \ldots Q_n x_n \ : \ F_n(x_1, \ldots, x_n) \\ &\equiv \quad Q_1 x_1 \ldots Q_{n-1} x_{n-1} \ : \ F_{n-1}(x_1, \ldots, x_{n-1}) \\ &\vdots \\ &\equiv \quad Q_1 x_1 \ : \ F_1(x_1) \\ &\equiv \quad F_0 \end{aligned}$$

  3. [Löse F_0 mit einem Entscheidungsverfahren für das quantorenfreie Fragment]

Universelle Quantoren

- **Frage:** Reicht es auch aus, nur ein Verfahren für die Elimination von existentiellen Quantoren zu haben?
- **Ja!** Z.B.:

$$\begin{array}{lllllll} & \exists x_1 & \exists x_2 & \forall x_3 & \exists x_4 & \forall x_5 & : F \\ \equiv & \exists x_1 & \exists x_2 & \neg(\exists x_3 & \neg\exists x_4 & \neg(\exists x_5 & : \neg F)) \end{array}$$

- Außerdem reicht es aus, in der Matrix Konjunktionen von Atomen zu betrachten. (Warum?)
- D.h. wir müssen QE nur für den Fall

$$\exists x \ : \ A_1 \wedge \ldots \wedge A_k$$

formulieren, wobei A_i Atome (ggf. über mehreren Variablen) sind.

Endliche Abstraktion

- **Gegeben:** Tarski-Formel F = ∃x G(x,y_1,…,y_n), wobei G(x,y_1,…,y_n) quantorenfrei.
- **Problem:** Die Menge der reellen Zahlen ist (überabzählbar) unendlich.
- **Idee:** Finde eine endliche Menge T ⊂ $\mathbb{R}$ mit

$$\exists x \ : \ G \quad \equiv \quad \bigvee_{t \in T} G[x/t]$$

- Jedes univariate Polynom p(x) vom Grad d besitzt höchstens d reelle Nullstellen.
- Das Vorzeichen ist zwischen zwei aufeinanderfolgenden Nullstellen invariant.
- $\mathbb{R}$ kann in 2d+1 Vorzeichen-invariante Intervalle, abhängig von p(x), zerlegt werden (Vorzeichen: +, –, 0).
- T besitzt dann einen Test-Punkt für jedes Intervall.
- **Was noch zu tun ist:** Nullstellen von Polynomen bestimmen.

Nullstellen von Polynomen

- Wir beginnen mit univariaten Polynomen
  - Die Quantorenelimination für reelle Polynome arbeitet im letzten Schritt mit einem univariaten Polynom über $\mathbb{R}$.
- Wie bestimmen wir die Nullstellen dieses Polynoms?
- **Problem:** Für Polynome mit Grad ≥5 existieren keine Formeln, um die Nullstellen explizit mit Wurzelausdrücken darzustellen.
- Eine Möglichkeit: Betrachte als Ausgangspunkt $\mathbb{Q}[x_1, \ldots, x_n]$ anstatt $\mathbb{R}[x_1, \ldots, x_n]$.
  - $\mathbb{Q}$ ist zwar nicht algebraisch abgeschlossen, d.h. Nullstellen von Polynomen über $\mathbb{Q}$ müssen nicht in $\mathbb{Q}$ liegen.
    - Beispiel: $f(x) = x^2 - 2$
    - Nullstellen: $\pm\sqrt{2} \notin \mathbb{Q}$
- Aber alle Lösungen lassen sich als Nullstellen von Polynomen über $\mathbb{Q}$ ausdrücken!

Algebraische Zahlen

- Die Menge $\mathbb{A}$ der **reellen algebraischen Zahlen** umfasst alle Nullstellen von Polynomen aus $\mathbb{Q}[x]$.
- Reelle algebraische Zahlen haben für unseren Zweck viele Vorteile:
  - Endliche Repräsentation
  - Addition und Multiplikation lässt sich in polynomieller Zeit berechnen
  - Konvertierung zwischen verschiedenen Darstellungen in poly. Zeit
- **Definition (Körpererweiterung)**: K ist Unterkörper eines Körpers L, wenn $K \subseteq L$, $0,1 \in K$ und die auf K eingeschränkten Verknüpfungen bilden auch wieder einen Körper. Das Paar aus L und K bezeichnet man als **Körpererweiterung** und schreibt L/K**.**
  - Beispiel: $\mathbb{C}/\mathbb{R}$ ist eine Körpererweiterung
- **Definition (algebraische Körpererweiterung)**: Eine Körpererweiterung L/K heißt **algebraisch**, falls jedes Element von L **algebraisch** über K ist, d.h. jedes Element aus L Nullstelle eines Polynoms mit Koeffizienten aus K ist.

Algebraische Zahlen

- Beispiele algebraischer Körpererweiterungen:
  - $\mathbb{C}/\mathbb{R}$ ist algebraisch
  - $\mathbb{Q}(\sqrt{2})$ ist algebraisch
  - $\mathbb{R}/\mathbb{Q}$ ist nicht algebraisch (transzendent)
- Sei α eine Nullstelle des Polynoms $f(x) = a_n x^n + \ldots + a_1 x + a_0$ mit Koeffizienten $a_i \in \mathbb{Q}$. Dann bezeichnen wir mit $\mathbb{Q}(\alpha)$ den kleinsten Erweiterungskörper von $\mathbb{Q}$, der α enthält.
- Das normierte (d.h. a_n=1) Polynom f(x) kleinsten Grades, mit f(α)=0 heißt **Minimalpolynom** von α. Wir bezeichnen es auch mit m_α.

Algebraische Zahlen

- Für eine Körpererweiterung L/K ist L ein K-Vektorraum.
- Eine algebraische Erweiterung ℚ(α) mit Minimalpolynom
  $$m_\alpha(x) = x^n + \ldots + a_1 x + a_0$$
  ergibt einen Vektorraum der Dimension n über ℚ mit Basis $\{1, \alpha, \alpha^2, \ldots \alpha^{n-1}\}$.
- Somit lassen sich die Elemente aus ℚ(α) als $k = k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1}$ mit $k_i \in \mathbb{Q}$ darstellen. Dies entspricht einem Polynom $p_k(\alpha)$.
- **Theorem**: $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(m_\alpha(x))$
  - (f) bezeichnet das Polynomideal ℚ[x]·f, d.h. alle Polynom-Vielfachen von f.
- Dieses Theorem erlaubt uns, Berechnungen im Körper ℚ(α) mittels Berechnungen im Polynom-Restklassenring durchzuführen.
- Für $p_k(x) \in \mathbb{Q}[x]/m_a(x)$ können wir die Elemente aus ℚ(α) mit $p_k(\alpha)$ identifizieren, d.h. wir können die Elemente aus ℚ(α) als Polynome über α darstellen.

Algebraische Zahlen

- **Beispiel:** $\alpha = \sqrt{2}, \quad m_\alpha(x) = x^2 - 2$
  - Wir rechnen in $\mathbb{Q}[x]/(x^2-2)$. Alle Elemente des Erweiterungskörpers $\mathbb{Q}(\alpha)$ haben die Form $k_0 + k_1\alpha$ mit $k_0, k_1 \in \mathbb{Q}$. Mit diesen können wir als Polynom mit Unbestimmter α im Restklassenkörper arbeiten.
  - Damit gilt z.B. $\alpha^2 \equiv 2 \pmod{\alpha^2 - 2}$.
- **Beispiel 2**: $\beta = \sqrt{2} + \sqrt{3}, \quad m_\beta(x) = x^4 - 10x^2 + 1$
  - Es gilt: $\beta^3 = (\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$ und damit $\beta^3 - 9\beta = 11\sqrt{2} + 9\sqrt{3} - 9(\sqrt{2} + \sqrt{3}) = 2\sqrt{2}$, also $(\beta^3 - 9\beta)^2 = (2\sqrt{2})^2 = 8$.
  - Rechnen in $\mathbb{Q}(\beta)$ bzw. $\mathbb{Q}[x]/(x^4-10x^2+1)$ liefert:

$$\begin{aligned}(x^3 - 9x)^2 &= x^6 - 18x^4 + 81x^2 \\ &\equiv 8 \pmod{x^4 - 10x^2 + 1}\end{aligned}$$

  d.h. Rechnen im Restklassenring liefert das gleiche Ergebnis.