

Zum Vorzeichentest Algebraischer Ausdrücke

Burkhard E. Strauß*

A.D. 2022[†]

Zusammenfassung

Der exakte Vergleich algebraischer Zahlen kann verhindern, daß geometrische Algorithmen aufgrund von Rundungsfehlern Fehlentscheidungen mit chaotischen Folgen treffen. Um das Vorzeichen $\text{sgn } \xi_E$ des exakten Wertes $\xi_E \in \mathbb{A}$ eines algebraischen Ausdrucks E mit Operatoren $\in \{+, -, \times, \div, \sqrt[n]{}\}$ und Operanden $\in \mathbb{Q}$ zu bestimmen, berechnen einschlägige Algorithmen eine Nulltrennungsschranke $\text{sep } E$, die es erlaubt, das Vorzeichen an einer hinreichend genauen Näherung $\hat{\xi}_E$ abzulesen. Wir schlagen vor, den Vorzeichentest für E anhand eines Testausdrucks E' mit $\text{sgn } E = \text{sgn } E'$ durchzuführen, der zu einer speziellen Klasse wohlgeratener Ausdrücke gehört, für deren Tests nicht unfaßbar viele Nachkommastellen berechnet werden müssen, so daß auch die Verarbeitung komplexerer Ausdrücke praktikabel wird. Eine Implementation in Java findet sich auf github.com/bestrauss/yaxana.

Abstract

The exact comparison of algebraic numbers can prevent geometric algorithms from taking wrong decisions due to rounding errors leading to chaotic program flow. To compute the sign of the exact value $\xi_E \in \mathbb{A}$ of an algebraic expression E with operators $\in \{+, -, \times, \div, \sqrt[n]{}\}$ and operands $\in \mathbb{Q}$ pertinent algorithms calculate a root separation bound $\text{sep } E$ which permits to read the sign from a sufficiently precise approximation $\hat{\xi}_E$. We propose to perform the sign test of E using a test expression E' with $\text{sgn } \xi_E = \text{sgn } \xi_{E'}$ which belongs to a special class of well worked expressions whose tests do not require the computation of inconceivably many k -ary places. Thus, the processing of more complex expressions becomes feasible. An implementation in Java is available on github.com/bestrauss/yaxana.

*Dipl.-Ing. der Elektrotechnik, RWTH Aachen.

[†]Rev 1.01, 19/07/2022

1 Einleitung

„*Omnia in mensura, et numero et pondere
disposuisti.*“ Vulgata, Liber Sapientiæ 11:21

Gegeben sei ein Ausdruck E , dessen Wert eine reelle algebraische Zahl $\xi_E = \text{val}_E \in \mathbb{A}$ ist. E verknüpft positive rationale Zahlen mittels der Operatoren $\in \{+, -, \times, \div, \sqrt[n]{}\}$ Beispiel:

$$\xi_E = \sqrt{2} + \sqrt{3} - \sqrt{5 + 2 \times \sqrt{6}}. \quad (1)$$

Eine exakte Darstellung des Zahlenwerts $\xi_E = \text{val}(E)$ von E im Binär- oder Dezimalsystem oder dergleichen ist aufgrund endloser Ziffernfolgen i.A. nicht möglich.

Andererseits ist es möglich, fehlerfreie exakte Werte für das Vorzeichen $\text{sgn } \xi_E$ von ξ_E zu bestimmen. Der exakte Vergleich algebraischer Zahlen kann sicherstellen, daß etwa geometrische Algorithmen frei von Rundungsfehlern exakte Entscheidungen treffen und der Programmfluß nicht vom Chaos beherrscht wird.

Mittels der in [1–4] beschriebenen Verfahren läßt sich eine Nulltrennungsschranke $\text{sep } E > 0$ berechnen, so daß entweder $\xi_E = 0$ oder $|\xi_E| \geq \text{sep } E$ gilt. Die Nulltrennungsschranke $\text{sep } E$ garantiert dann, daß der Wert von $\text{sgn } \xi_E$ an einer entsprechend genauen Näherung $\hat{\xi}_E$ für ξ_E abgelesen werden kann. Die Verfahren sind robust, berechnen aber im Fall $\xi_E = 0$ bei Ausdrücken mit mehr als ein paar Wurzeloperationen unfassbar viele Nachkommastellen, deren Anzahl mit dem Produkt der Wurzelexponenten der Wurzeloperationen in E wächst.

Zwecks Verbesserung der Situation wird vorgeschlagen, den Vorzeichentest für E anhand eines mit E verwandten Testausdrucks E' mit $\text{sgn } \xi_E = \text{sgn } \xi_{E'}$ durchzuführen, so daß gewisse Eigenschaften der Nullstellenverteilung des Strukturpolynoms von E' die Verwendung vergleichsweise traumhafter Nulltrennungsschranken erlaubt. Der Rechenaufwand im kritischen Fall $\xi_E = 0$ wird für Ausdrücke mit vielen unterschiedlichen Wurzeloperationen drastisch reduziert bzw. der Test solcher Ausdrücke überhaupt erst praktikabel gemacht.

Es folgen Abschnitte mit Definitionen und mit einer Vorzeichentesttheorie. Danach Fazit sowie im Anhang Beweise zum Strukturpolynom und Literaturverzeichnis.

2 Definitionen

Definition 2.1 (Abstrakter Syntaxbaum, Terminal) Ein Ausdruck E ist ein Baum im Sinne der Graphentheorie. Die Blätter des Baums sind Operanden, die restlichen Knoten unäre oder binäre Operatoren. Im Sinne der Automatentheorie und der Linguistik handelt es sich um einen abstrakten Syntaxbaum, dessen Blätter terminale Symbole bzw. Terminale genannt werden.

Hinweis: Ein Ausdruck kann auch als ein (gegenüber dem Baum allgemeinerer) gerichteter, azyklischer Graph dargestellt werden, indem identische Unterausdrücke im Baum durch nur ein Exemplar ersetzt werden, auf das dann mehr als eine der gerichteten Kanten zeigt. Dies wird in Implementationen genutzt, ist aber im Rahmen dieser Ausführungen nicht weiter von Bedeutung.

Definition 2.2 (Ausdruck) Ein Ausdruck E mit dem Wert ξ_E ist:

- ein Terminal mit dem Wert $c \in \mathbb{Q}, c > 0$,
- die Summe $E_0 + E_1$ zweier Ausdrücke,
- das Produkt $E_0 \times E_1$ zweier Ausdrücke,
- die Negation $-E$ eines Ausdrucks,
- der Kehrwert $1 \div E$ eines Ausdrucks,
- die n -te Wurzel $\sqrt[n]{E}$ eines Ausdrucks,
- der Absolutwert $|E|$ eines Ausdrucks,

sofern

- beim Kehrwert $\xi_E \neq 0$,
- bei der n -ten Wurzel $n \in \mathbb{N} \setminus \{1\}$ und, bei geradem n , $\xi_E \geq 0$.

Unterausdrücke mit verschwindenden Werten werden detektiert und wegoptimiert. Alle Radikanden werden positiv gemacht, $\sqrt[n]{-E} = -\sqrt[n]{E}$, falls ξ_E ungerade.

Hinweis: Die Auswahl der Operatoren dient der Übersichtlichkeit der folgenden Darstellungen und der Beweise. Subtraktion, Division und Potenz mit beliebigen rationalen Exponenten können auf diese Auswahl zurückgeführt werden. Eine andere gebräuchliche Auswahl an Operatoren ist $\in \{+, -, \times, \div, \sqrt[n]{}\}$.

Definition 2.3 (Wert eines Ausdrucks) Der Zahlenwert oder auch einfach Wert $\xi_E = \text{val } E \in \mathbb{A}$ eines Ausdrucks E ist

- $\xi_c = c$
- $\xi_{E_0 + E_1} = \xi_{E_0} + \xi_{E_1}$
- $\xi_{E_0 \times E_1} = \xi_{E_0} \times \xi_{E_1}$
- $\xi_{1 \div E} = 1 \div \xi_E$
- $\xi_{-E} = -\xi_E$
- $\xi_{\sqrt[n]{E}} = \sqrt[n]{\xi_E}$
- $\xi_{|E|} = |\xi_E|$

Definition 2.4 (Strukturpolynom) Das Strukturpolynom $p_E(z)$ eines Ausdrucks E mit dem Wert ξ_E ist ein Polynom mit rationalen Koeffizienten, das eine Nullstelle bei $z = |\xi_E|$ hat und das anhand des abstrakten Syntaxbaums von E nach folgenden Bildungsregeln konstruiert wird:

$$\begin{aligned}
p_c(z) &= z - c \\
p_{E_0+E_1}(z) &= z^{-K} \prod_{k_0=0}^{N_0} \prod_{k_1=0}^{N_1} (z - (z_{k_0} + z_{k_1})) \\
p_{E_0 \times E_1}(z) &= \prod_{k_0=0}^{N_0} \prod_{k_1=0}^{N_1} (z - (z_{k_0} \times z_{k_1})) \\
p_{1 \div E}(z) &= \prod_{k=1}^N (z - (1 \div z_k)) \quad , \quad p_{\sqrt[N]{E}}(z) = \prod_{k=1}^N (z^n - z_k) \\
p_{-E}(z) &= p_{|E|}(z) = p_E(z) = \prod_{k=1}^N (z - z_k)
\end{aligned}$$

Dabei

- sind c, z_k, z_{k_0} bzw. z_{k_1} auf der rechten Seite jeweils die Nullstellen von $p_c(z), p_E(z), p_{E_0}(z)$ bzw. $p_{E_1}(z)$, die nicht verschwinden, denn die Bildungsregeln gewährleisten dies.
- haben die gebildeten Polynome rationale Koeffizienten, wie bereits angegeben. Dies wird abgesehen von den trivialen Fällen, in Anhang A auf Seite 11 gezeigt.
- ist K im Term z^{-K} bei der Addition die Anzahl an Nullstellen, die das Polynom ohne den Term z^{-K} hätte. z^{-K} befreit das Polynom von Nullstellen bei $z = 0$.
- verändert der Term z^{-K} die Koeffizienten nicht, sondern tauscht sie nur aus (verschiebt sie), weshalb sie gleich und damit weiterhin rational bleiben.
- liegen vor Einsetzen des Terms z^{-K} niemals sämtliche Nullstellen bei $z = 0$, da per Definition 2.2 auf Seite 4 die Werte von Unterausdrücken nicht verschwinden, außer möglicherweise an der Baumwurzel des abstrakten Syntaxbaums, wo ein solches Ereignis dann $\xi_E = 0$ anzeigt.

Hinweis: Es heißt oben, das (monströse) Strukturpolynom werde konstruiert. Tatsächlich dient das Strukturpolynom nur theoretischen Betrachtungen und kommt in der Praxis, im Algorithmus, nicht vor.

Erörterung 2.1 (Struktur- vs. Minimalpolynom) Im Gegensatz zum Minimalpolynom einer algebraischen Zahl kodiert das Strukturpolynom eines Ausdrucks wesentliche Aspekte der Struktur des Ausdrucks inklusive der Werte seiner Terminale und der Wurzelexponenten. Bildet man aus zwei Ausdrücken mit Werten, deren Minimalpolynome hochgradig sind, einen neuen Ausdruck, dessen Wert rational ist, dann findet ein Kollaps statt und das Minimalpolynom des Wertes des neuen Ausdrucks hat nur noch den Grad 1. Das ist bei Strukturpolynomen nicht der Fall. Unabhängig vom Wert des Ausdrucks reflektiert der Grad des Strukturpolynoms die Komplexität des Ausdrucks. Aus diesem Grund sind Minimalpolynome hier zuwider, von Interesse ist nicht der Begriff „konjugierte algebraische Zahl“ sondern der Begriff „konjugierter Ausdruck“.

Definition 2.5 (Konjugierter Ausdruck) Zwei Ausdrücke E_0 und E_1 heißen *konjugiert*, wenn sie ein und dasselbe Strukturpolynom $p_{E_0}(z) = p_{E_1}(z)$ haben.

Hinweis: Zwei Ausdrücke E_0 und E_1 , die nicht konjugiert sind, können denselben Wert $\xi_{E_0} = \xi_{E_1}$ mit demselben Minimalpolynom haben.

3 Eine Vorzeichentesttheorie

Erörterung 3.1 (Aufgabenstellung) Sei der reelle Wert ξ_E eines Ausdrucks E ganzalgebraisch (der allgemeine Fall läßt sich darauf zurückführen, [2,3]). Seien z_k die $N \in \mathbb{N}$ Nullstellen des Strukturpolynoms $p_E(z)$ von E , die entweder reell sind oder in konjugiert komplexen Paaren auftreten, dann gilt für das Produkt der Nullstellen

$$\prod_{k=1}^N z_k = c_0 \in \mathbb{Z}$$

und somit insbesondere auch

$$\xi_E \neq 0 \quad \Rightarrow \quad \prod_{k=1}^N |z_k| \geq 1.$$

Nun ist der Wert ξ_E des Ausdrucks E eine der Nullstellen z_k . Sei o.B.d.A. $\xi_E = z_1$. Dann ergibt sich

$$\xi_E \neq 0 \quad \Rightarrow \quad |\xi_E| \geq \frac{1}{\prod_{k=2}^N |z_k|} \geq \frac{1}{(\max_k |z_k|)^{N-1}}.$$

Der Term $(\max_k |z_k|)^{-(N-1)}$ wird als Nulltrennungsschranke für ganzalgebraische Werte verwendet [2].

Es handelt sich bei dieser Ungleichung in der typischen Praxis um eine unglaublich miserable Abschätzung, aber im schlimmsten Fall könnten ja tatsächlich alle Nullstellen mehr oder weniger genau auf einem riesigen Kreis um den Ursprung der komplexen z -Ebene mit dem Radius $\max_k |z_k|$ liegen, während nur eine einzige Nullstelle in der Gegend von $|c_0|(\max_k |z_k|)^{-(N-1)}$ all diese Nullstellen kompensiert.

Was man viel lieber hätte, wären hingegen Nullstellenpaare mit $|z_{k_0} \cdot z_{k_1}| = 1$, so wie das bei gewissen zeitdiskreten Systemen in der Nachrichtentechnik vorkommt; man denke an die Übertragungsfunktionen der Analyse-Resynthese-Kanäle in perfekt rekonstruierenden Polyphasen- oder Quadraturspiegelfilterbänken; ähnlich auch den Polstellen-Nullstellen-Paaren von Allpaßfiltern. Unter solch himmlisch geordneten Umständen könnte man die Abschätzung

$$\xi_E \neq 0 \quad \Rightarrow \quad |\xi_E| \geq \frac{1}{\max_k |z_k|}$$

verwenden, in der der monströse Exponent $N - 1$ fehlt. N ist das Produkt der Wurzelexponenten der unterschiedlichen Wurzelunterausdrücke in E , und daher der Grund, weshalb sich bisher die Behandlung von Ausdrücken mit bereits moderat vielen solchen in der Praxis verboten hat. Weiterhin wäre zusätzlich auch fest $c_0 = 1$, so daß nicht ein womöglich sehr viel größerer Koeffizient mit bloß 1 nach unten abgeschätzt würde.

Definition 3.1 (Wohlgeratener Ausdruck) Wir nennen einen Ausdruck E mit dem nicht-verschwindenden Wert ξ_E *wohlgeraten*, wenn in der Menge der Nullstellen seines Strukturpolynoms $p_E(z)$ in der komplexen z -Ebene neben Nullstellenpaaren, deren Produkte jeweils den Betrag 1 haben, nur solche nicht-paarigen Nullstellen vorkommen, deren Wert selbst den Betrag 1 hat.

Satz 3.1 (Hauptsatz) Seien E_0 und E_1 zwei (gemäß Definition 2.5 auf Seite 6) konjugierte Ausdrücke, deren Werte nicht verschwinden, dann ist der Ausdruck $E_0 \div E_1$ (lies: $E_0 \times (1 \div E_1)$) wohlgeraten.

Beweis 3.1 Das Strukturpolynom $p_{E_0 \div E_1}(z)$ des Ausdrucks $E_0 \div E_1$ wird (gemäß Definition 2.4 auf Seite 5) gebildet, indem [da die Ausdrücke konjugiert sind und daher $p_{E_0}(z) = p_{E_1}(z)$ gilt] jede Nullstelle von $p_{E_0}(z)$ durch sich selbst und durch jede andere Nullstelle von $p_{E_0}(z)$ geteilt wird. Man erhält einerseits Nullstellen $\frac{z_k}{z_k} = 1$ und andererseits Nullstellenpaare $\frac{z_k}{z_m}$ und $\frac{z_m}{z_k}$ mit $\frac{z_k}{z_m} \frac{z_m}{z_k} = 1$. \square

Definition 3.2 (Testausdruck) Sei ξ_E der Wert eines Ausdrucks E . Wir bezeichnen den Ausdruck E' mit dem Wert $\xi_{E'}$ als einen *Testausdruck für E* , wenn $\text{sgn } \xi_E = \text{sgn } \xi_{E'}$.

Definition 3.3 (Wohlgeratener Testausdruck) Sei E' ein Testausdruck für E und sei E' für den Fall $\xi_E \neq 0$ wohlgeraten, dann nennen wir E' einen wohlgeratenen Testausdruck für E .

Satz 3.2 (Ein wohlgeratener Testausdruck) Seien Ausdrücke E_0 , E_1 und $E = E_0 - E_1$ und gelte für die Werte $\xi_{E_0} \neq 0$ und $\xi_{E_1} \neq 0$, dann ist

$$E' = \frac{E_0 - E_1}{|E_0| + |E_1|}.$$

ein wohlgeratener Testausdruck für E .

Beweis 3.2 Da der Wert des Nenners aufgrund der Voraussetzungen inklusive der Absolutwertbildungen positiv ist, gilt $\text{sgn } E' = \text{sgn } E$ weshalb E' nach Definition 3.2 auf Seite 8 ein Testausdruck für E ist. Weiterhin sind im Fall $\xi_{E_0} \neq \xi_{E_1}$ bzw. $\xi_E \neq 0$, Zähler und Nenner konjugierte Ausdrücke gemäß Definition 2.5 auf Seite 6, d.h. Zähler und Nenner haben dasselbe Strukturpolynom, denn laut Definition 2.4 auf Seite 5 gilt bei der Bildung des Strukturpolynoms

$$p_{-E}(z) = p_{|E|}(z) = p_E(z),$$

weshalb der Bildungsvorgang beider Strukturpolynom in jedem Zwischenschritt für Zähler und Nenner dasselbe Ergebnis liefert. Laut Hauptsatz 3.1 auf Seite 8 ist damit der Ausdruck E' wohlgeraten. \square

Algorithmus 3.1 (ZVAA Vorzeichentest) Bestimmung des Vorzeichens des Wertes ξ_E eines Ausdrucks $E = E_0 - E_1$.

1. Bilde den wohlgeratenen Testausdruck E' nach Satz 3.2 auf Seite 9.
2. Berechne $\text{sgn } \xi_{E'}$ per BFMSS[2] wie in [3, 4] beschrieben, wobei allerdings in dem Term für die Nulltrennungsschranke der Exponent $N_{E'} - 1$ (der dort $D(E') - 1$ genannt wird) durch 1 ersetzt wird.
3. **return** $\text{sgn } \xi_{E'}$.

Erörterung 3.2 Im Fall von Ausdrücken mit wenigen Wurzeloperationen berechnet der ZVAA-Vorzeichentest nach Algorithmus 3.1 auf Seite 10 zwei nennenswerte zusätzliche Operationen und ist deshalb etwas langsamer als BFMSS[2]. Bei wachsender Anzahl an unterschiedlichen Wurzeloperationen nähern sich beide im Fall $\xi_E \neq 0$ aneinander an, und im Fall $\xi_E = 0$ wird ZVAA drastisch schneller. Es empfiehlt sich, unter entsprechenden Umständen ZVAA einzusetzen.

4 Fazit

Ein neuer Algorithmus zum Vorzeichentest algebraischer Ausdrücke E wurde vorgestellt, der anstelle des gefragten Vorzeichentests für einen Ausdruck E einen Vorzeichentest für einen Testausdruck E' mit $\text{sgn } \xi_E = \text{sgn } \xi_{E'}$ durchführt, wobei E' zu einer speziellen Klasse wohlgeratener Ausdrücke gehört. Der Rechenaufwand im kritischen Fall $\text{val } E = 0$ ist damit für Ausdrücke mit vielen unterschiedlichen Wurzeloperationen drastisch reduziert bzw. derartige Tests sind überhaupt erst praktikabel.

$$E' = \frac{E_0 - E_1}{|E_0| + |E_1|}$$

A Beweise zum Strukturpolynom

Satz A.1 (Strukturpolynom von Multiplikation und Addition)

Seien E_0 und E_1 Ausdrücke, sei \circ eine Operation $\in \{+, \times\}$ und seien

$$p_{E_0}(z) = \prod_{k=1}^{N_0} (z - z_{0,k}) = \sum_{k=0}^{N_0} c_{0,k} z^k, \quad z \in \mathbb{C}, z_{0,k} \in \mathbb{A}, c_{0,k} \in \mathbb{Q}$$

bzw.

$$p_{E_1}(z) = \prod_{k=1}^{N_1} (z - z_{1,k}) = \sum_{k=0}^{N_1} c_{1,k} z^k, \quad z \in \mathbb{C}, z_{1,k} \in \mathbb{A}, c_{1,k} \in \mathbb{Q}$$

die zugehörigen Strukturpolynome mit algebraischen Nullstellen $z_{0,k}$ bzw. $z_{1,k}$ und rationalen Koeffizienten $c_{0,k}$ bzw. $c_{1,k}$. Dann hat das Strukturpolynom

$$p_{E_0 \circ E_1}(z) = \prod_{k_0=1}^{N_0} \prod_{k_1=1}^{N_1} (z - (z_{0,k_0} \circ z_{1,k_1})) = \sum_{k=0}^{N_0 N_1} c_{\circ,k} z^k$$

des Ausdrucks $E_0 \circ E_1$ ebenfalls rationale Koeffizienten $c_{\circ,k} \in \mathbb{Q}$.

Beweis A.1 [2] enthält einen Beweis für den Fall ganzzahliger Koeffizienten, der auf rationale Koeffizienten übertragen werden kann. \square

Satz A.2 (Strukturpolynom des Kehrwerts) Sei E ein Ausdruck und sei

$$p_E(z) = \prod_{k=1}^N (z - z_k) = \sum_{k=0}^N c_k z^k, \quad z \in \mathbb{C}, z_k \in \mathbb{A}, c_k \in \mathbb{Q}$$

das Strukturpolynom des Ausdrucks E mit rationalen Koeffizienten c_k . Dann hat das Strukturpolynom

$$p_{1 \div E}(z) = \prod_{k=1}^N (z - (1 \div z_k)) = \sum_{k=0}^N c_{\div,k} z^k, \quad c_{\div,k} \in \mathbb{Q}$$

des Ausdrucks $1 \div E$ ebenfalls rationale Koeffizienten $c_{\div,k}$.

Beweis A.2 Das Polynom

$$z^N p_E(z^{-1}) = z^N \sum_{k=0}^N c_k z^{-k} = \sum_{k=0}^N c_k z^{N-k} = \sum_{k=0}^N c_{N-k} z^k$$

hat dieselben Koeffizienten wie $p_E(z)$, nur in umgekehrter Reihenfolge. Daher sind die Koeffizienten des Polynoms $z^N p_E(z^{-1})$ rational. Nun gilt für dasselbe Polynom auch

$$z^N p_E(z^{-1}) = z^N \prod_{k=1}^N (z^{-1} - z_k) = \frac{(-1)^N}{c_0} \prod_{k=1}^N (z - z_k^{-1}),$$

weshalb die Koeffizienten $c_{\div, k}$ des Polynoms

$$p_{1 \div E}(z) = \prod_{k=1}^N (z - (1 \div z_k)) = \sum_{k=0}^N c_{\div, k} z^k$$

ebenfalls rational sind. □

Literatur

- [1] M. Mignotte “*Identification of Algebraic Numbers*” *Journal of Algorithms*, 3(3), September 1982
- [2] C. Burnikel, R. Fleischer, K. Mehlhorn, and S. Schirra: “*A Strong and Easily Computable Separation Bound for Arithmetic Expressions Involving Radicals*” *Algorithmica*, v. 27: S. 87–99, Springer, May 2000
- [3] C. Burnikel, S. Funke, K. Mehlhorn, S. Schirra, and S. Schmitt: “*A separation bound for real algebraic expressions*” *Lecture Notes in Computer Science*, 9th ESA, volume 2161, S. 254–265, Springer, 2001
- [4] Pion, Sylvain and Yap, Chee “*Constructive root bound for k -ary rational input numbers*” *Theoretical Computer Science*, v. 369, n. 1-3, pp. 361–376, Elsevier, 2006 <https://hal.inria.fr/inria-00344349>