Pfadzerlegung und unberechenbare reelle Funktionen

Ausarbeitung zum Seminar
"Reelle Komplexität"
bei Prof. Dr. Martin Ziegler
und Dr. habil. Ulrike Brandt
von Johanna Sokoli

Inhaltsverzeichnis

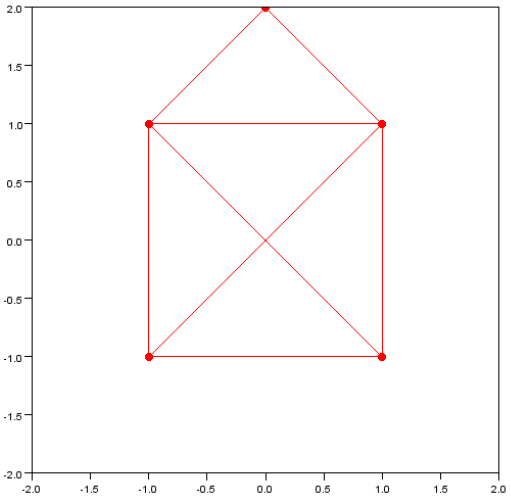
1 Grundlagen aus der Algebra sowie algebraischen Geometrie

Definition 1.1. *Sei R Integritätsbereich und $S \subset R^n$. S heißt* ***elementar semi-algebraisch*** *über R, falls R angeordnet ist und alle $x \in S$ eine endliche Menge von polynomiellen Gleichungen und Ungleichungen über R erfüllen.*
Eine ***semi-algebraische Menge*** *ist endliche Vereinigung von elementar semi-algebraischen Mengen.*
Eine ***abzählbar semi-algebraische Menge*** *ist eine abzählbare Vereinigung von elementar semi-algebraischen Mengen.*
Besitzt R keine Ordnung, so nennt man diese Mengen ***elementar quasi-algebraisch, quasi-algebraisch*** *bzw.* ***abzählbar quasi-algebraisch****.*

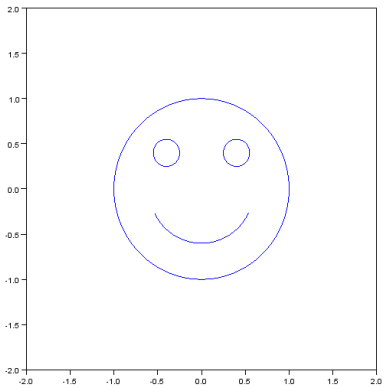
Beispiel 1.2. Die Menge N, das "Haus vom Nikolaus", ist eine semi-algebraische Menge, denn sie wird von den folgenden Mengen von polynomiellen Gleichungen und Ungleichungen beschrieben:

$$\begin{aligned}
S_1 &= \{(x,y) \in \mathbb{R}^2 | x = y,\ -1 \leq x,\ x \leq 1\} \\
S_2 &= \{(x,y) \in \mathbb{R}^2 | x = -y,\ -1 \leq x,\ x \leq 1\} \\
S_3 &= \{(x,y) \in \mathbb{R}^2 | x = -1,\ -1 \leq y,\ y \leq 1\} \\
S_4 &= \{(x,y) \in \mathbb{R}^2 | x = 1,\ -1 \leq y,\ y \leq 1\} \\
S_5 &= \{(x,y) \in \mathbb{R}^2 | y = -1,\ -1 \leq x,\ x \leq 1\} \\
S_6 &= \{(x,y) \in \mathbb{R}^2 | y = 1,\ -1 \leq x,\ x \leq 1\} \\
S_7 &= \{(x,y) \in \mathbb{R}^2 | y = x + 2,\ -1 \leq x,\ x \leq 0\} \\
S_8 &= \{(x,y) \in \mathbb{R}^2 | y = -x + 2,\ 0 \leq x,\ x \leq 1\}
\end{aligned}$$

und es gilt $N = \bigcup_{i=1}^{8} S_i$.



Beispiel 1.3. Auch ein Smiley ist eine semi-algebraische Menge.



Bemerkung 1.4. Im 1-dim. Fall sind alle semi-algebraische Mengen eine Vereinigung von Punkten und Intervallen.

Definition 1.5. *Die Abbildung Φ_M wird definiert als*

$$\Phi_M(x) := O(x^T)$$

Hierbei ist T die Zeit, nach der die Maschine hält, O die Ausgabeabbildung der Maschine, und x^T bezeichnet die Berechung der BCSS-Maschine nach T Schritten.

Definition 1.6. *$T_M(x)$ ist die Zeit, welche die BCSS-Maschine M bei Eingabe x benötigt, um zu halten.*
Die Menge

$$\Omega_M := \{x \in \mathcal{I}_M | T_M(x) < \infty\}$$

d.h. die Menge aller möglichen Eingaben x aus der Eingabemenge $\mathcal{I}$, bei deren Eingabe an die Maschine M diese nach endlicher Zeit hält, wird als ***Haltemenge von*** *M bezeichnet.*

Definition 1.7. *Eine Menge $S \subset R^n$ heißt* ***entscheidbar über*** *R^n, wenn die charakteristische Funktion dieser Menge berechenbar ist.*

Definition 1.8. *Der Berechnungspfad der Maschine M bei Eingabe x, d.h. die Menge der Knoten*

$$\eta^0, \ldots, \eta^k, \ldots$$

wird mit γ_x bezeichnet.
Sei weiterhin

$$\nu_{\gamma(k)} := \{x' \in \mathcal{I}_M | \gamma_{x'}(k) = \gamma(k)\}$$

Dies ist die Menge aller Eingaben x, nach deren Eingabe die ersten k Knoten, welche die Maschine M während ihrer Berechungen durchläuft, mit den ersten k Knoten von $\gamma(k)$ übereinstimmen.
Sei

$$\Gamma_T := \{\gamma_x(T) | T_M(x) \leq T,\ x \in \mathcal{I}_M\}$$

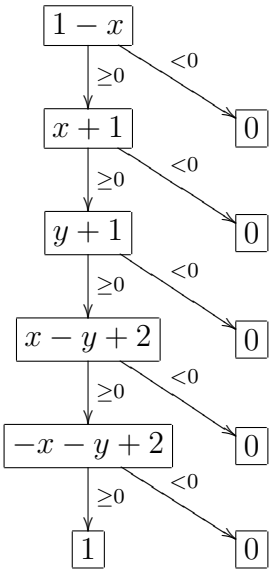
Dies ist die Menge all der Berechnungspfade, welche die Maschine M bei einer Eingabe x durchläuft, sodass sie nach höchstens Zeit T hält.
Außerdem definiert man

$$\Gamma'_M := \{\gamma \in \Gamma_T \text{ für ein } T < \infty, \gamma \notin \Gamma_{T'}\ \forall T' < T\}$$

Dies ist die Menge aller Berechungspfade, welche die Maschine M bei einer Eingabe x durchläuft, sodass sie nach endlicher Zeit hält.

Bemerkung 1.9. Wichtig ist hierbei, dass jeder dieser Pfade nur genau ein mal in Γ'_M hinzugefügt wird, da diese Eigenschaft für einen der Sätze, die weiter unten bewiesen sind, benötigt wird.

Beispiel 1.10. Dies ist die Pfadzerlegung des Algorithmus, der die Punkte innerhalb des Hauses vom Nikolaus entscheidet:



Im 1. Rechenschritt berechnet die BCSS-Maschine $1-x$, und prüft dann anschließend, ob das Ergebnis kleiner als 0 oder größer gleich 0 ist. Im ersten Fall gibt sie direkt 0 aus, da sich der eingegebene Punkt rechts des Hauses vom Nikolaus befindet. Sonst berechnet sie $x+1$, und vergleicht das Ergebnis mit 0. Ist es kleiner, so liegt der eingegebene Punkt links des Hauses vom Nikolaus, und die BCSS-Maschine gibt 0 aus.
Die weiteren Rechenoperationen verlaufen analog. Im letzten Rechenschritt prüft die Maschine dann, ob $-x-y+2<0$ oder $-x-y+2\geq 0$ gilt. Im ersteren Fall gibt sie 0 aus (der eingegebene Punkt befindet sich oberhalb der rechten Dachschräge), sonst sind alle polynomiellen Ungleichungen erfüllt, die Maschine gibt 1 zurück und der Punkt liegt im Haus vom Nikolaus.

2 Die Pfadzerlegung

Lemma 2.1.

a) Sei R Integritätsbereich. Dann ist $\nu_{\gamma(k)}$ elementar semi-algebraisch.

b) Für $\gamma_1(k)\neq\gamma_2(k)$ folgt $\nu_{\gamma_1(k)}\cap\nu_{\gamma_2(k)}=\emptyset$.

Beweis.

b) $\nu_{\gamma_i(k)}$ ist definiert als die Menge aller $x\in\mathcal{I}$, sodass die ersten k während der Berechungen der BCSS-Maschine durchlaufenen Knoten mit $\gamma_i(k)$

übereinstimmen. Sind nun $\gamma_1(k)$ und $\gamma_2(k)$ an mindestens einer Stelle verschieden, so kann für jedes $x' \in \mathcal{I}$ nicht $x' \in \nu_{\gamma_1(k)}$ und $x' \in \nu_{\gamma_2(k)}$ gelten, da es sich bei M um eine deterministische Maschine handelt.

a) **Fall 1:** Die Verzweigungsfunktionen sind Polynome.
Dann ist die Behauptung klar.
Fall 2: Die Verzweigungsfunktionen sind rationale Abbildungen.
Sei die Verzweigungsfunktion $f = \frac{p}{q}$ mit Polynomen p, q.
Sei OBdA $q(x) \neq 0$ (siehe Bemerkung).
Dann gilt

$$\frac{p(x)}{q(x)} = 0 \quad \Leftrightarrow p(x) = 0$$

bzw. im Fall, dass R eine Ordnung besitzt

$$\frac{p(x)}{q(x)} < 0 \quad \Leftrightarrow \quad p(x)q(x) < 0$$

sodass man die Verzweigungsfunktionen in Polynome umformen kann, ohne die Berechnung zu ändern.
Damit folgt die Behauptung.

□

Bemerkung 2.2. $q(x) \neq 0$ kann OBdA angenommen werden:

- Füge vor jeden Berechnungsschritt eine Verzweigungsfunktion ein, die testet, ob der Nenner der im nächsten Schritt zu berechnenden Funktion verschwindet.
- Falls nein, gehe zum nächsten Knoten über.
- Falls ja, gehe in eine Endlosschleife: teste erneut, ob der Nenner verschwindet.

Satz 2.3. Für alle Maschinen M über einem Integritätsbereich R gilt:

1. Sei $T > 0$. $\Omega_T = \bigcup_{\gamma \in \Gamma_T} \nu_\gamma$ ist eine endliche disjunkte Vereinigung von elementar semi-algebraischen Mengen.
2. $\Omega_M = \bigcup_{\gamma \in \Gamma'_M} \nu_\gamma$ ist eine abzählbare disjunkte Vereinigung elementar semi-algebraischer Mengen.
3. Für jedes $\gamma \in \Gamma_M$ ist Φ_M polynomielle oder rationale Abbildung.

Beweis.

1) Nach dem Lemma sind die ν_γ disjunkt und elementar semi-algebraisch. Γ_T hat höchstens 2^T Elemente, denn die Maschine hat in jedem Schritt höchstens 2 mögliche Nachfolgeknoten. Nach T Rechenschritten gibt es also höchstens 2^T mögliche verschiedene Pfade.

2) Wie oben sind die ν_γ elementar semi-algebraisch.
Die Vereinigung ist

   - disjunkt, da die ν_γ disjunkt sind (wie oben), und mit $\gamma \in \Gamma'_M$ sichergestellt wird, dass der Pfad einer nach Zeit T haltenden Berechnung nicht für ein $T' > T$ noch einmal ausgewählt wird.
   - abzählbar, da Γ_T maximal 2^T, d.h. abzählbar viele, Elemente hat (wie oben), und $T \in \mathbb{N}\backslash\{0\}$ abzählbar ist.

3) Φ ist definiert als die Verknüpfung der Berechnungen, alle Berechungen sind Polynome oder rationale Abbildungen.

□

3 Anwendungsbeispiele des Satzes zur Pfadzerlegung

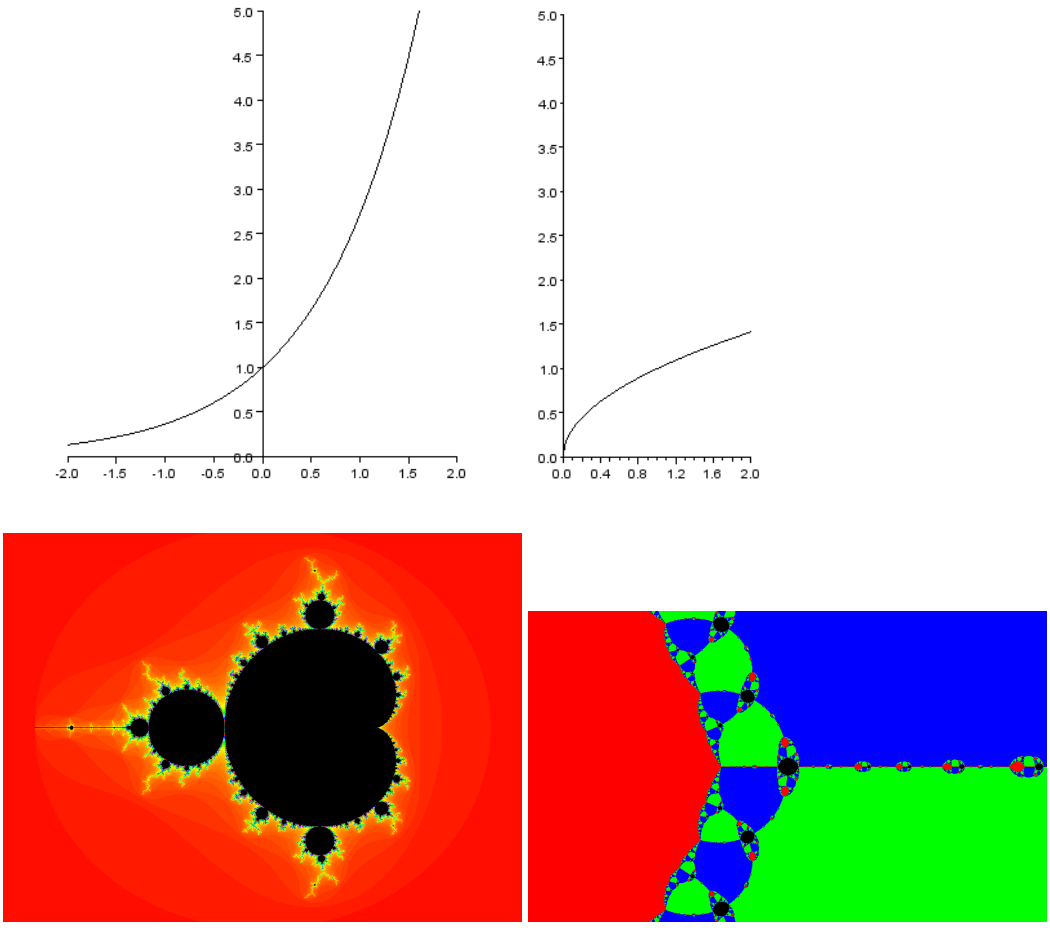
Satz 3.1. Die folgenden Mengen sind BCSS-unentscheidbar / die Funktionen sind BCSS-unberechenbar:

a) $\mathbb{Q}$

b) ILP, d.h. die Existenz einer ganzzahligen Lösung eines Systems linearer Ungleichungen mit reellen Koeffizienten

c) $f : \mathbb{R}_+ \to \mathbb{R}_+,\ x \mapsto \sqrt{x}$ und $g : \mathbb{R} \to \mathbb{R},\ x \mapsto exp(x)$

d) Die Mandelbrotmenge sowie die Menge der Startpunkte, sodass die Newtonmethode für die Funktion $f(x) = x^3 - 2x + 2$ konvergiert



Bemerkung 3.2. In den oberen 2 Grafiken sind die exp- bzw. Wurzelfunktion zu sehen.
Unten links befindet sich ein Bild der Mandelbrotmenge. Die schwarzen Bereiche markieren Konvergenzbereiche, alle anderen Farben geben die Divergenzgeschwindigkeit an.
Unten rechts sieht man eine Veranschaulichung des Konvergenzverhaltens des Newtonverfahrens für die Funktion $f(x) = x^3 - 2x + 2$. Hierbei sind die Bereiche, für die das Newtonverfahren gegen die Nullstelle $x_1 \approx -1,769292354$ konvergiert, rot gefärbt, für $x_2 \approx 0,884646177 + i \cdot 0,589742805$ blau und für $x_3 \approx 0,884646177 - i \cdot 0,589742805$ grün. Die schwarzen Bereiche des Bildes kennzeichnen die Startpunkte, für die auch nach 50000 Schritten des Newtonverfahrens noch unklar ist, ob bzw. gegen welche Nullstelle das Verfahren konvergiert.

Definition 3.3.

a) Eine ***Topologie*** τ *ist ein Mengensystem, welches aus Teilmengen einer Menge X besteht, sodass die folgenden Eigenschaften erfüllt sind:*

- $X \in \tau$
- $\emptyset \in \tau$
- *Für* $t_i \in \tau$, $i \in \{1, \ldots, n\}$ *folgt* $(\cap_{i=1}^{n} t_i) \in \tau$
- *Für* $t_i \in \tau$, $i \in I$, *wobei I eine beliebige Indexmenge ist, folgt* $(\cup_{i=1}^{\infty} t_i) \in \tau$

Solche Mengen $t \in \tau$ werden ***offene Mengen*** *genannt.*

b) Eine Menge X zusammen mit einer Topologie τ auf X nennt man einen ***topologischen Raum****.*

c) Ein topologischer Raum heißt ***zusammenhängend****, wenn man ihn nicht in zwei disjunkte, nichtleere, offene Teilmengen zerlegen kann.*

Beispiel 3.4. $\mathbb{R}$ mit der euklidischen Topologie ist zusammenhängend.

Satz 3.5. Jede semi-algebraische Menge hat nur endlich viele Zusammenhangskomponenten.

Beweis. des Satzes 3.6:

a) Wie wir schon gesehen haben, sind alle von BCSS-Maschinen entscheidbaren Mengen abzählbar semi-algebraisch.
Angenommen, $\mathbb{Q}$ ist entscheidbar.
$\Rightarrow \mathbb{R}\backslash\mathbb{Q}$ ist entscheidbar
$\Rightarrow \mathbb{R}\backslash\mathbb{Q}$ hat nur abzählbar viele Zusammenhangskomponenten.
Aber $\mathbb{R}\backslash\mathbb{Q}$ hat überabzählbar unendlich viele isolierte Punkte, also überabzählbar unendlich viele Zusammenhangskomponenten.
Widerspruch.

d) **i)** Auch die Mandelbrotmenge ist keine abzählbare Vereinigung semi-algebraischer Mengen.

ii) Die Menge der Startpunkte, sodass die Newtonmethode für die Funktion $f(x) = x^3 - 2x + 2$ nicht konvergiert, ist eine Cantormenge.
Eine Cantormenge ist ebenfalls keine abzählbare Vereinigung semi-algebraischer Mengen, da sie aus überabzählbar vielen einzelnen Punkten besteht.

b) Betrachte folgendes Gleichungssystem:

$$ax \leq y \quad ax \geq y \quad x \geq 1$$

Für die Lösung (x, y) gilt:
$(x, y) \in \mathbb{Z}^2 \quad \Leftrightarrow \quad a \in \mathbb{Q}$, denn

" $\Rightarrow$ "

Sei $(x, y) \in \mathbb{Z}^2$ eine Lösung des obigen Gleichungssystems.
Mit den ersten beiden Gleichungen folgt $ax = y$, sodass $a = \frac{y}{x} \in \mathbb{Q}$ gilt.

" $\Leftarrow$ "

Sei nun $a \in \mathbb{Q}$, d.h. es existieren $b, c \in \mathbb{Z}$, sodass $a = \frac{b}{c}$.
Damit lassen sich die ersten beiden Gleichungen zu $bx = cy$ umformen, sodass $\frac{b}{c} = \frac{y}{x}$ gilt. Ist nun $c > 0$, wählt man $x = c$ und $y = b$, im Fall $c < 0$ wählt man $x = -c$ und $y = -b$. In beiden Fällen ist $(x, y) \in \mathbb{Z}^2$ und löst das obige Gleichungssystem.

Könnte man also ILP entscheiden, so auch $\mathbb{Q}$.
Widerspruch.

c) Nach dem Satz zur Pfadzerlegung kann eine BCSS-Maschine nur rationale Abbildungen bzw. stückweise rationale Abbildungen berechnen. Es gilt jedoch, dass weder $\sqrt{x}$ noch $exp(x)$ rationale Abbildungen sind, und man kann sie auch nicht stückweise rational darstellen:

- Annahme: $exp(x) = \sum_{i=1}^{\infty} \frac{p_i(x)}{q_i(x)} \cdot \chi_{[a_i,b_i]}(x)$ für Polynome mit Grad $\leq d_i$ und $[a_i, b_i]$ Intervalle, die eine Partition von $\mathbb{R}$ bilden.

$$\Leftrightarrow \quad \sum_{i=1}^{\infty} q_i(x) \cdot \chi_{[a_i,b_i]}(x) \cdot \exp(x) = \sum_{i=1}^{\infty} p_i(x) \cdot \chi_{[a_i,b_i]}(x)$$

  Nach $\max_{i \in \mathbb{N}} d_i + 1$-fachem Ableiten verschwindet die rechte Seite, während die linke Seite aus $\sum_{i=1}^{\infty} exp(x) \cdot \widetilde{q_i}(x) \cdot \chi_{[a_i,b_i]}(x)$ mit $deg(\widetilde{q_i}(x)) = deg(q_i(x)) \; \forall i \in \mathbb{N}$ besteht. Dies widerspricht der Annahme.

- Definiere

$$\begin{aligned} deg\left(\sum_{i=1}^{\infty} \frac{p_i(x)}{q_i(x)}\right) &= \max_{i \in \mathbb{N}} deg\left(\frac{p_i(x)}{q_i(x)}\right) \\ &= \max_{i \in \mathbb{N}} (deg(p_i(x)) - deg(q_i(x))) \end{aligned}$$

  Annahme: $\sqrt{x} = \sum_{i=1}^{\infty} \frac{p_i(x)}{q_i(x)} \cdot \chi_{[a_i,b_i]}(x)$ mit $[a_i, b_i]$ wie oben.
  Es folgt

$$1 = deg(id) = deg((\sqrt{x})^2) = 2deg(\sqrt{x})$$

sodass $deg(\sqrt{x}) \notin \mathbb{Z}\ \forall x \in \mathbb{R}$.
Dies widerspricht der Annahme, da das Maximum einer Differenz zweier natürlicher Zahlen eine ganze Zahl ist.

□

Satz 3.6. $\mathbb{Q}$ ist semi-entscheidbar.

Beweis. Für ein gegebenes $z \in \mathbb{R}$ können systematisch alle Paare $(x, y) \in \mathbb{Z}^2$ durchprobiert werden, da $\mathbb{Z}$ und damit auch $\mathbb{Z}^2$ abzählbar ist.
Gilt $z = \frac{x}{y}$, so akzeptiere, sonst teste das nächste Paar. □

Satz 3.7.

$$f :\subseteq \mathbb{R} \to \mathbb{R}, \quad x \mapsto \begin{cases} 1 & : \quad x \in \mathbb{Q} \\ 0 & : \quad x \notin \mathbb{Q} \wedge x^2 \in \mathbb{Q} \\ \perp & : \quad x^2 \notin \mathbb{Q} \end{cases}$$

ist BCSS-berechenbar.

Beweis. Teste wie im Beweis von Satz 3.6, ob $x^2 \in \mathbb{Q}$ gilt.
Ist dies nicht der Fall, so hält die BCSS-Maschine nicht, dies ist wegen $x \mapsto \perp$ für $x^2 \notin \mathbb{Q}$ aber auch nicht notwendig.
Gilt $x^2 \in \mathbb{Q}$, so wurde $(a, b) \in \mathbb{Z}^2$ gefunden, sodass $x^2 = \frac{a}{b}$ gilt. Nun wird der gefundene Bruch wie folgt gekürzt:
Prüfe, ob a durch 2 teilbar ist.

- Falls nein, prüfe, ob a durch 3 teilbar ist. Ist die Antwort wieder nein, fahre mit 4 fort, etc., so lange, bis geprüft wird, ob a durch a teilbar ist. Dann ist der Bruch vollständig gekürzt.
- Falls ja, prüfe, ob auch b durch 2 teilbar ist.
  - Falls nein, prüfe, ob a durch die nächste folgende Zahl teilbar ist.
  - Falls ja, ist der Bruch kürzbar. Ersetze a und b durch die Zahlen $\frac{a}{t}$ und $\frac{b}{t}$, wobei t die Zahl ist, von der die Maschine soeben festgestellt hat, dass sowohl a als auch b durch sie teilbar sind. (Dies "weiß" die BCSS-Maschine, da dies nur vom Berechnungspfad abhängig ist.) Beginne nun erneut mit dem Kürzen.

Dieses Teilprogramm kann in keine Endlosschleife geraten, da jeder Bruch nur endlich oft gekürzt werden kann, bis Zähler und Nenner koprim sind.
Teste nun für den gekürzten Bruch $\frac{a'}{b'}$, ob a' und b' Quadratzahlen sind:
Teste dazu, ob $1^2 = a'$ gilt.

- Falls ja, ist a' eine Quadratzahl. Teste nun analog, ob b' eine Quadratzahl ist.
- Falls nein, fahre mit 2^2, 3^2 etc. analog fort, bis entweder $n^2 = a'$ gilt, teste dann analog, ob auch b' eine Quadratzahl ist, oder n^2 größer als a' ist.

(Auch hier ist das Nicht-Halten der BCSS-Maschine nicht möglich, da irgendwann der Fall $a' > n^2$ bzw. $b' > n^2$ eintritt und die BCSS-Maschine "weiß", dass a' bzw. b' keine Quadratzahl ist.)
Sind nun a' und b' Quadratzahlen, so ist $x \in \mathbb{Q}$, und die BCSS-Maschine gibt 1 aus. Sonst ist zwar $x^2 \in \mathbb{Q}$, aber $x \notin \mathbb{Q}$, und die BCSS-Maschine gibt 0 aus. □

Satz 3.8. Jedes diskrete Problem ist entscheidbar.

Beweis. Eine BCSS-Maschine kann sich reelle Konstanten exakt merken, und diese in weiteren Berechnungen nutzen.
Um ein diskretes Problem zu entscheiden, benötigt die BCSS-Maschine also nur die richtige Konstante $c \in \mathbb{R}$, aus der sie dann die richtige Antwort "ablesen" kann. □

Quellenangaben

Complexity and real Computation, Blum, Cucker, Shub, Smale, Springer 1998
Real Computability and Hypercomputation, Martin Ziegler, 2007