Komplexitätstheoretische Betrachtung Knotentheoretischer Probleme

Zum Hauptseminar zur Knotentheorie von Dr. B. Himpel
Vortrag von Lars A. Wallenborn - lwallenb@uni-bonn.de

06.02.2009

Zusammenfassung

In diesem Seminarvortrag wird die Komplexität und Entscheidbarkeit von einigen knotentheoretischen Problem betrachtet. Dazu werden erstmal Komplexitätstheoretische Grundlagen geschaffen. Besondere Beachtung wird das Entscheidungsproblem ob ein Knoten der Unknoten ist oder nicht erhalten. Der Vortrag ist auf [HLP] aufgebaut.

Inhaltsverzeichnis

1 Formalisierung von Problemen

Definition 1.1 *Für eine endliche Menge A ist*

$$A^* := \{a_1 \dots a_k \mid k \in \mathbb{N}; a_i \in A \ \forall 1 \leq i \leq k\}$$

die Menge aller Wörter in A. Eine Teilmenge von A^* heißt Sprache über A. Für $x = a_1 \dots a_k \in A$ ist $|x| = k$.

Definition 1.2 *Eine Funktion $f : \{0,1\}^* \to \{0,1\}^*$ heißt Problem, eine Funktion $f : \{0,1\}^* \to \{0,1\}$ Entscheidungsproblem.*

Bemerkung 1.3 *Man will natürlich nun alle „intuitiven Problem“ auch als Probleme auffassen können. Dazu ist es notwendig alle Objekte (Zahlen, Vektoren, Graphen etc.), die in intuitiven Problemen vorkommen, in einem Wort aus $\{0,1\}^*$ zu kodieren. Nun gehören aber die meisten praktisch auftauchenden Objekte zu abzählbaren Mengen, es gibt also schon eine bijektive Abbildung, die jedem Objekt genau eine Zahl zuordnet. Natürlich Zahlen lassen sich auf verschiedene Weisen in $\{0,1\}^*$ kodieren (z.B. $n \mapsto \underbrace{1 \cdots 1}_{n\text{-mal}}$ oder Binärdarstellung). Das Abbilden solcher „endlichen Objekte“ auf natürliche Zahlen nennt man „Gödel-Nummerierung“.*

Definition 1.4 *Die von einem Entscheidungsproblem f generierte Sprache ist*

$$L_f := \{x \in \{0,1\}^* \mid f(x) = 1\}$$

Das zu einer Sprache $L \subset \{0,1\}^*$ gehörende Entscheidungsproblem ist

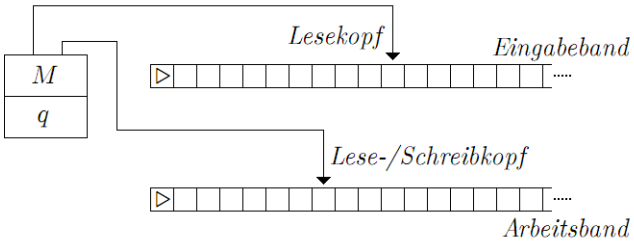
$$f_L(x) = \begin{cases} 1 & \text{für } x \in L \\ 0 & \text{sonst} \end{cases}$$

Also hängen Sprachen und Entscheidungsprobleme ganz eng zusammen.

2 Formalisierung von Maschinen

Definition 2.1 *Eine Turing-Maschine ist ein Tupel $M = (\Gamma, Q, \delta)$ wobei gilt:*

- $\Gamma = \{ \triangleright, \square, 0, 1 \}$ *heißt Alphabet von M*
- *Q heißt die Menge der Zustände von M und ist ebenfalls endlich. Es gibt zwei besondere Zustände:*
  - $q_S \in Q$ *(Startzustand)*
  - $q_E \in Q$ *(Endzustand)*
- *δ ist die sog. Übergangsfunktion:* $\delta : Q \times \Gamma^2 \to Q \times \Gamma \times \{L, R, N\}^2$
- *Weiterhin gibt es zwei (potentiell) unendlich lange Bänder, die in Zellen aufgeteilt sind in denen Elemente aus Γ eingetragen sind. In der ersten Zelle von jedem Band steht $\triangleright$, alle anderen Zellen sind mit $\square$ vorinitialisiert. Über dem ersten Band, dem Eingabeband gibt es einen Lesekopf, der genau eine Zelle auslesen kann. Über dem zweiten Band, dem Arbeitsband befindet sich ein Lese-/Schreibkopf, der genau eine Zelle lesen und wieder (mit Einträgen aus Γ) beschreiben kann. Beide Köpfe sind nach Links und Rechts beweglich.*



  Zu jedem Zeitpunkt besitzt M genau einen inneren Zustand $q \in Q$.
- *Eine Konfiguration von M ist ein Tupel $(q, e, a) \in Q \times \Gamma^2$. Die Anfangskonfiguration ist beispielsweise $(q_S, \triangleright, \triangleright)$.*
- *In einem Arbeitsschritt wird δ auf die aktuelle Konfiguration angewendet und auf folgende Weise eine neue Konfiguration gewonnen $(q', a', \varepsilon_E, \varepsilon_A) := \delta(q, e, a)$:*
  - *Ändere den inneren Zustand auf q'*
  - *Schreibe a' in die Zelle über der sich der Arbeitskopf gerade befindet, bewege ihn danach, wenn möglich, um ε_A, nenne den neuen Inhalt $\tilde{a}$.*
  - *Bewege den Eingabekopf um ε_E (wenn möglich). Der Inhalt der neuen Zelle sei $\tilde{e}$*
  - *Die neue Konfiguration ist nun $(q', \tilde{e}, \tilde{a})$.*
- *Erreicht M mit Eingabebandinhalt $(\triangleright\ x\ \square) \in \Gamma^*$ (wobei $x \in \{0,1\}^*$) irgendwann den Zustand q_E so sagt man M terminiert auf x und nennt den Inhalt des Arbeitsbandes y von der ersten Zelle bis zum ersten $\square$ die Ausgabe von M auf x. Man schreibt dann auch suggestiv $y = M(x)$.*
- *Eine Turing Maschine $M_{trivial}$, die bei jeder Eingabe sofort in den Endzustand wechselt und dabei $\triangleright$ auf das Ausgabeband schreibt heißt trivial.*

Bemerkung 2.2 *Eine Turing-Maschine kann man sich ganz konkret als C-Programm vorstellen*

#Zustände *entspricht der Größe eines C-Programms*

#Arbeitszellen *entspricht dem verwendeten Arbeitsspeicher eines Programms*

#Anwendungen von δ *entspricht der Zeit, die ein Programm benötigt*

Umgekehrt gibt es auch eine Turing-Maschine, die ein C-Programm ausführt (sie sieht aber sehr unübersichtlich aus).

These: (Church-Turing) Jeder physikalisch realisierbare Computer, sei er mechanisch, auf Silikon-Basis, auf DNA-Basis oder sonstige Alien-Technologie, lässt sich auf einer Turing-Maschine simulieren.

3 Entscheidbarkeit

Definition 3.1 *Ein Problem f heißt entscheidbar, berechenbar oder rekursiv, wenn es eine Turing-Maschine M gibt s.d. für alle $x \in \{0,1\}^*$ gilt $M(x) = f(x)$. Eine Sprache heißt entscheidbar, berechenbar oder rekursiv, wenn f_L entscheidbar ist. Man sagt dann, dass M das Problem bzw. die Sprache entscheidet.*

Beispiel 3.2 $L = \{\underbrace{1\cdots1}_{n-mal} \in \{0,1\}^* \mid n \text{ ist gerade}\}$ *ist entscheidbar.*

Gibt es überhaupt unentscheidbare Sprachen?

Bemerkung 3.3 *Das Tuple (Γ, Q, δ) beschreibt M vollständig und aus diesem Tupel können wir für einen Eingabebandinhalt immer wieder den gleichen Arbeitsbandinhalt erzeugen. Da aber Γ und Q endlich sind, ist auch δ endlich. Somit ist die Menge aller Turing-Maschinen $\mathcal{M}$ abzählbar. Sei F die zugehörige Bijektion $\mathcal{M} \to \mathbb{N}$, verknüpfe sie mit einer Kodierung von natürlichen Zahlen als Elemente in $\{0,1\}^*$ und nenne die resultierende Abbildung $K : \mathcal{M} \to \{0,1\}^*$. K ist bijektiv auf seinem Bild, definiere also eine neue Abbildung*

$$\begin{array}{rcl} K^{-1} : \{0,1\}^* & \to & \mathcal{M} \\ \alpha & \mapsto & \begin{cases} M & \exists M \in \mathcal{M} \text{ mit } K(M) = \alpha \\ M_{trivial} & \text{sonst} \end{cases} \end{array}$$

Definition 3.4

$$HALT := \{(\alpha, x) \in \{0,1\}^* \mid K^{-1}(\alpha) \text{ terminiert auf } x\}$$

Satz 3.5 *$HALT$ ist unentscheidbar.*

Beweis: Sei M_H die Turing-Maschine, die $HALT$ entscheidet. Definiere eine weitere Turing-Maschine M die zur Eingabe $x \in \{0,1\}^*$ folgendes y schreibt und dann in q_E wechselt

$$\begin{array}{rl} \text{Wenn } M_H(x,x) = 0 & y = 1 \\ \text{Sonst} & y = 1 - (K^{-1}(x))_{(x)} \end{array}$$

Was ist $M(x)$ für $x = K(M)$? M terminiert immer nach einem Schritt und kann nur 0 oder 1 ausgeben.
Fall $M(x) = 0$ also ist $(K^{-1}(x))_{(x)} = 1$ dann ist für $x = K(M)$

$$1 = K^{-1}(K(M))_{(K(M))} = M_{(K(M))} = 0 \; \lightning$$

Fall $M(x) = 1$ dann gibt es zwei Möglichkeiten:

Fall $M_H(x,x) = 0$: was falsch ist (auch für $x = K(M)$), da M immer nach einem Schritt terminiert.

Fall $(K^{-1}(x))_{(x)} = 0$: und für $x = K(M)$ dann

$$0 = K^{-1}(K(M))_{(K(M))} = M(K(M)) = 1 \; \lightning$$

Also gibt es M_H nicht, und $HALT$ ist nicht entscheidbar. □

Definition 3.6 *Für zwei Entscheidungsprobleme f_1 und f_2 schreibe $f_1 \leq_T f_2$, wenn es ein berechenbares f gibt mit $f_1(x) = f_2(f(x)) \; \forall x \in \{0,1\}^*$. In Worten: „$f_2$ ist mindestens so schwer wie f_1“ oder „f_1 lässt sich durch eine Turing-Maschine auf f_2 zurück führen“ (daher das T).*

Bemerkung 3.7 *Indem man also zeigt, dass für ein Entscheidungsproblem f gilt: $f_{HALT} \leq_T f$, hat man gezeigt, dass f unentscheidbar ist.*

Satz 3.8 *Folgende Probleme sind nicht entscheidbar*

- *Diophantische Gleichung Finde ganzzahlig Nullstelle von $p \in \mathbb{Z}[X_1, \ldots, X_n]$*

  linearer Fall *leicht mit etwas Termumformung*

  quaratischer Fall *clevere Tricks helfen*

  kubischer Fall *Algorithmus noch unbekannt, berühmtestes Beispiel (elliptischen Kurven):*

  $$y^2 = x^3 + ax + b \quad a, b \in \mathbb{Z}$$

  „quadrublischer“ Fall *nachgewiesener weise unentscheidbar*

- *PCP - Post-correspondence-problem Seien $u_1, \ldots, u_N, v_1, \ldots v_N \in \{0,1\}^*$ finde eine Folge von Indices $(i_k)_{1 \leq k \leq K}$ mit $K \geq 1$, $1 \leq i_k \leq N \; \forall k$ und*

  $$u_{i_1} \cdots u_{i_k} = v_{i_1} \cdots v_{i_k}$$

- *Gruppen-Theorie [RAB] Betrachte eine Teilmenge der Menge aller Gruppen, die Menge aller endlich präsentierbarer Gruppen, also alle Gruppen G mit*

  $$G = \langle x_1, \ldots, x_n \mid r_1(x_1, \ldots, x_n), \ldots, r_k(x_1, \ldots x_n) \rangle$$

  Diese Menge decken schon sehr viele (auch unendliche) Gruppen ab, beispielsweise Knotengruppen!

  Sei nun P eine algebraische (d.h. eine unter Gruppenisomorphismus invariante) Eigenschaft einer endlich präsentierten Gruppe. Gelte weiterhin

  - *Es gibt eine Gruppe für die P gilt*
  - *Es gibt eine Gruppe für die nicht P gilt*
  - *Gilt für eine Gruppe P so gilt es auch für jede Untergruppe*

  Dann folgt: Die Sprache

  $$\{G \mid G \text{ ist Präsentation einer endlich präsentierbaren Gruppe und } P(G)\}$$

  ist nicht entscheidbar.

  Beispiele für P: abelsch, einfach, endlich, trivial

  Man kann also im Allgemeinen nicht mal entscheiden ob eine Gruppe trivial ist! Der Weg über die Knotengruppe zu entscheiden, ob ein Knoten der Unknoten ist fällt also aus prinzipieller Betrachtungsweise weg.

4 Komplexitätsklassen

Definition 4.1 *Sei M eine Turing-Maschine*

1. *Für $x \in \{0,1\}^*$ sei $\underline{\text{time}_M(x)}$ die Anzahl der δ-Anwendungen bis M auf x terminiert oder ∞ wenn M auf x nicht terminiert.*

2. *Für $n \in \mathbb{N}$ sei*
$$\underline{\text{time}_M(n)} := \sup_{x \in \{0,1\}^*, |x| \leq n} \{\text{time}_M(x)\}$$

3. *Für $T : \mathbb{N} \to \mathbb{N}$ sei*

   $\underline{\text{Dtime}(T)} := \{L \subseteq \{0,1\}^* \mid \exists M \in \mathcal{M}$ *die L entscheidet und* $\text{time}_M(n) \in O(T(N))\}$

4. $$P := \bigcup_{c \in \mathbb{N}} \text{Dtime}(n^c)$$

   Eine Turing-Maschine, die eine Sprache $L \in P$ entscheidet heißt <u>polynomiell</u>.

Definition 4.2

$$NP := \{ \quad L \subseteq \{0,1\}^* \mid \exists c \in \mathbb{N}, \exists M \in \mathcal{M} \text{ s.d. } \forall x \in \{0,1\}^* \text{ gilt}$$
$$x \in L \Leftrightarrow \exists\ u \in \{0,1\}^{|x|^c} : M(x,u) = 1 \text{ in polynomieller Zeit}\}$$

Das zu einem $x \in L$ gehörende $u \in \{0,1\}^{|x|^c}$ heißt <u>Zertifikat für x unter M</u>.

Beispiel 4.3 *Hier einige Beispiele von Problem, die durch ein Zertifikat leicht zu lösen werden*

- *Seien $\{x_i\}_{i=1}^n$ Boolsche Variablen und $\phi(x)$ eine Disjunktion von Konjunktionen dieser Variable (eine „Veroderung“ von aussagenlogischen „Verundungen“ der x_i bzw. $\neg x_i$) also z.B. für $n = 5$*

  $$\phi(x) = (\neg x_1 \vee x_2 \vee \neg x_5) \wedge (x_3 \vee x_2 \vee \neg x_4) \wedge (x_1 \vee \neg x_2 \vee x_3 \vee \neg x_4 \vee x_5)$$

  Die Menge aller Terme ist abzählbar und damit ist jeder Term als Element aus $\{0,1\}^*$ kodierbar. Sei SAT die Menge aller kodierten erfüllbaren Terme. Es gilt $SAT \in NP$ (Zertifikat ist eine Belegung des Terms). Ob es einen polynomiellen Algoritmus gibt oder nicht ist unbekannt, wenn dem aber so ist folgt (da SAT in gewisser Weise eines der schwersten Probleme in NP ist), dass $P = NP$.

- *Sei G ein endlicher Graph. Ein Hamiltonkreis ist ein geschlossener Weg im Graphen, der jeden Knoten genau ein mal besucht. Sei $HAMILTONIAN$ die Menge aller kodierten endlichen Graphen, in denen es einen Hamiltonkreis gibt. Es gilt: $HAMILTONIAN \in NP$ (Zertifikat ist ein Hamiltonkreis).*

- *Sei $SUBSETSUM = \{S \subseteq \mathbb{Z}$ endlich $\mid \exists S' \subseteq S : \sum_{s \in S'} s = 0\}$.*
  Bsp: $\{-7,-3,-2,5,8\} \in SUBSETSUM$, da $\sum_{s \in \{-3,-2,5\}} s = 0$.

- *$THEOREMS := \{(\phi, n) \mid \phi$ ist math. Satz mit Beweis der Länge $\leq n\}$ Es gilt, dass $THEOREMS \in NP$ (das Zertifikat ist ein Beweis), wenn nun gezeigt würde, dass $P = NP$ ist $THEOREMS \in P$ und Mathematiker werden überflüssig.*

Bemerkung 4.4 *Nach der Definition muss das Zertifikat in seiner Länge polynomiell beschränkt sein. Zahlen $k \in \mathbb{N}$ benötigen als minimale Kodierungsgröße aber $\lceil \log_2(k) \rceil$ Stellen. Man kann also für eine Eingabe $x \in \{0,1\}^*$ mit $n = |x|$ keine Zahl in der Größerordnung von 2^{2^n} als Zertifikat verwenden, denn sie benötigt $\lceil \log_2(2^{2^n}) \rceil = 2^n$ Stellen, was wirklich mehr als n^c Stellen, für ein Konstantes c, sind.*

Man kann sich unter NP auch eine, vielleicht anschaulicherer, Art von Sprachen vorstellen. Nämlich die Menge der Probleme, die von einer sog. „nicht-deterministischen" Turing-Maschine, einem sehr wundersamen Gerät, in polynomieller Zeit gelöst werden können.

Definition 4.5 *Eine nicht-deterministische Turing-Maschine N ist eine Turing-Maschine mit zwei Übergangsfunktionen δ_1 und δ_2, also $N = (\Gamma, Q, \delta_1, \delta_2)$. In jedem Zustand kann N beide Übergangsfunktionen benutzen. Man sagt, dass N auf Eingabe $x \in \{0,1\}^*$ terminiert, wenn es mindestens eine Folge von δ_1-δ_2-Anwendungen gibt, die zu q_E führen. Die Länge des kürzesten solcher Wege heißt* $\mathrm{Ntime}_N(x)$. *Analog zu gerade definiert man nun für $n \in \mathbb{N}$ die Größe* $\mathrm{Ntime}_N(n)$ *und für $T : \mathbb{N} \to \mathbb{N}$ die Menge* $\mathrm{Ntime}(T)$.

Satz 4.6

$$NP = \bigcup_{c \in \mathbb{N}} \mathrm{Ntime}(n^c)$$

Wir können an NP nun also auf zwei Weisen denken: Eine Sprache $L \in NP$ kann

1. von einer nicht-deterministischen Turing-Maschine in polynomieller Zeit gelöst werden
2. von einer deterministischen Turing-Maschine in polynomieller Zeit gelöst werden, wenn man ihr ein Zertifikat (welches polynomiell in der Eingabelänge ist) als Hilfe gibt

Satz 4.7 $P \subseteq NP$

Beweis: Sei $L \in P$, nun gibt es schon ein M, welches auf jeder Eingabe x in polynomieller Zeit ein Ergebnis liefert. Die Wahl von u ist also egal. Somit ist $L \in NP$. □

Offene Frage: $NP \subseteq P$ oder $P \neq NP$

5 Knotentheorie

5.1 Fragestellung

Die Eingabedaten werden ab jetzt immer Verschlingungsdiagramme D einer zahmen Verschlingung L in regulärer Position sein. Die Eingabegröße n ist

$$X(D) := \#\text{Kreuzungen} + \#\,(\text{Knoten in L}) - 1$$

Ist die Verschlingung L eigentlich ein Knoten entspricht n also gerade der Anzahl der Überkreuzungen in D.

Bemerkung 5.1

- $X(D) = 0 \Rightarrow D$ *ist ein Diagramm des Unknoten*
- D *ist ein Diagramm des Unknoten genau dann wenn, es einen einen zum Unknoten isotopen Knoten K gibt für den es ein Diagramm D' mit $X(D') = 0$ gibt. (Erinnerung: Eine Isotopie eines topologischen Raumes X ist eine Familie von Homöomorphismen $h_t : X \to X$, $t \in [0,1]$ mit $h_0 = \mathrm{id}$ und $H : [0,1] \times X \to X$ mit $H(t,p) := h_t(p)$ ist stetig)*

- *Knotendiagramme lassen sich, beispielsweise wie Graphen mit Kantemarkierungen für „drunter“ und „drüber“ an jeder Kreuzung, als Element aus* $\{0,1\}^*$ *kodieren, nenne diese Kodierung* F*.*

Definition 5.2 *Definiere folgende Sprachen:*

$$UNKNOT := \{F(D) \mid D \text{ ist Diagramm des Unknoten}\}$$

(Entscheidbarkeit bewiesen von Haken in 1954)

$$SPLITABLE := \{F(D) \mid D \text{ ist Diagramm einer trennbaren Verschlingung}\}$$

(Entscheidbarkeit bewiesen von Schubert in 1961)

Satz 5.3 $UNKNOT \in NP$ *und* $SPLITABLE \in NP$

Beweisskizze: (nur für ersten Teil) Wir wollen zu der Kodierung $F(D) = x \in \{0,1\}^*$ eines Knotendiagramms D eine Konstante $c \in \mathbb{N}$ und ein Zertifikat $u \in \{0,1\}^{|x|^c}$ finden (also ein Zertifikat polynomieller Länge) so, dass es eine Turing-Maschine M gibt, die in polynomieller Zeit (mithilfe von u) prüft, ob x eine Kodierung des Unknotens ist. Wir müssen also Unknoten durch u als solche „zertifizieren“.
Skizze einer Turing-Maschine:

1. Prüfe, ob D ein Knotendiagramm ist: Wandere dazu auf dem Diagramm entlang und markiere besuchte Kanten. Sobald man auf eine markierte Kante trifft prüfe, ob es noch unmarkierte Kanten gibt, wenn nicht, dann ist es ein Knotendiagramm, sonst nur ein Verschlingungsdiagramm.

2. Konstruiere einen „gut triangulierbaren“ stückweise linearen Knoten K in $\mathbb{R}^3$, der D als Projektion hat.

3. Interpretiere u irgendwie als Fläche in $\mathbb{R}^3$ und stelle einige Eigenschaften von ihr sicher (natürlich in polynomieller Zeit). Dann wird folgen, dass sie eine Scheibe (ohne Selbstüberschneidungen) ist die als Rand gerade den Knoten selbst hat. Dies kann (nach vorhergehenden Vorträgen) aber nur der Fall sein, wenn K der Unknoten ist. Somit ist dann D ein Diagramm des Unknoten.

5.2 Triangulierungen

Definition 5.4 *Sei* M *eine kompakte* 3*-Manigfaltigkeit. Eine Triangulierung von* M *ist eine Ausschöpfung* $\mathcal{T} \subseteq \mathcal{P}(M)$ *von* M *durch zu* n*-Simplices (für* $0 \leq n \leq 3$*) homeomorphen Objekten (im Folgenden, der Einfachheit halber, Tetraeder, Dreicke, Kanten und Punkte genannt). Der Schnitt zweier Objekte aus* $\mathcal{T}$ *gehöre immer auch zu* $\mathcal{T}$ *und weiterhin gelte, dass sich zwei Tetraeder nur in einem Dreieck, zwei Dreiecke nur in einer Kante und zwei Kanten nur in einem Punkt schneiden. Die Menge aller Tetraeder heißt* 3*-Skelett, die Menge aller Dreicke* 2*-Skelett, die Menge aller Kanten* 1*-Skelett und die Menge aller Punkte* 0*-Skelett.*
Die Triangulierung heißt regulär, wenn für $1 \leq n \leq 3$ *der Rand des* n*-Skelettes genau das* $n-1$*-Skelett ist. Eine Triangulierung heißt endlich, wenn sie nur aus endlich vielen Tetraedern, Dreiecken, Kanten und Punkten besteht.*
Die baryzentrische Unterteilung einer Triangulierung entsteht indem jeder Simplex s *durch einen* 0*-Simplex (Punkt)* s_0 *im Schwerpunkt von* s *ersetzt wird und* s_0 *dann mit allen* s_1 *verbunden wird, die aus echten Teilmengen von* s *hervogegangen sind. Die baryzentrische Unterteilung überführt endliche Triangulierungen in endliche Triangulierungen und reguläre in reguläre.*

Sei S^3 die Ein-Punkt-Kompaktifizierung von R^3 (man stelle sich das Vorgehen analog zur Kompaktifizierung von R^2 zur S^2 vor). Weiter sei K ein stückweise linearer Knoten in $\mathbb{R}^3$ (zu jedem zahmen Knoten finden wir einen isotopen solchen Knoten) und $\mathcal{T}$ eine Triangulierung von $\mathbb{S}^3$ mit K in ihrem 1-Skelett und dem „unendlich ferne Punkt“ als einen Punkt der Triangulierung.
Unterteile die Triangulierung $\mathcal{T}$ zwei mal baryzentrisch und erhalte so $\mathcal{T}''$, eine Triangulierung dieser Art nennen wir gut. Sei R_K eine Umgebung des Knotens K, die aus den Simplices in $\mathcal{T}$ besteht, die nicht-leeren Schnitt mit K haben. Betrachte nun die kompakte 3-Mannigfaltigkeit $M_K := \mathbb{S}^3 - \mathring{R}_K$ mit Rand ∂M_K wobei $\mathring{R}_K$ das Innere von R_K bezeichne. Der Rand ∂R_K von R_K und damit auch der Rand ∂M_K von M_K ist ein Torus und wird von Punkten, Kanten und Dreiecken in $\mathcal{T}''$ trianguliert.

Definition 5.5 *Sei M eine kompakten 3-Mannigfaltigkeit mit Rand ∂M. Eine Fläche S heißt echt eingebettet, wenn sie sich nicht selbst überschneidet und $S \cap \partial M = \partial S$. S heißt essentiell, wenn gilt:*

- *S ist echt eingebettet in M*
- *es gibt keinen Homeomorphismus von S nach ∂M, der die Identität auf ∂S ist*
- *es gibt eine injektive Abbildung $i : \pi_1(S) \to \pi_1(M)$*

Bemerkung 5.6 *Seifertflächen sind ein Beispiel für essentielle Flächen.*

Lemma 5.7 *Sei K ein polygonaler Knoten und M_K wie oben gut trianguliert:*

$$K \text{ ist der Unknoten} \Leftrightarrow \exists \text{essentielle Scheibe in } M_K$$

Existiert die Scheibe, dann gilt, dass

- *∂S ist trennbar von K (im Sinne von Verschlingungen)*
- *∂S durchsticht eine essentielle Scheibe in R_K maximal einmal*

(was man auch ausdrücken kann als $[\partial S] = (0, \pm 1)$ in $H_1(\partial M_K, \mathbb{Z})$ wobei $H_1(\partial M_K, \mathbb{Z}) \cong \mathbb{Z} \oplus \mathbb{Z}$ von $(1, 0)$, der Homologieklasse des Randes eine essentiellen Scheibe in R_K (einem Meridian), und von $(0, 1)$, der Homologieklasse eines Longitude in ∂M_K, erzeugt wird) dann ist S essentiell und 5.7 impliziert dann, dass K der Unknoten ist.

Grob gesagt muss man nach diesem Lemma nun keine aufspannende Scheibe für K mehr finden sondern nur noch für eine Longitude und wenn wir so eine Scheibe gefunden haben darf sie mit einem Meridian nur ein mal verknotet sein.

Lemma 5.8 *Sei S zusammenhängende in $\mathbb{R}^3$ eingebettette, triangulierbare Fläche, mit Euler-Charakteristik $\chi(S) = 1$ dann, ist S eine Scheibe.*

Beweis: $\chi(S) = (\#\text{Flächen}) - (\#\text{Kanten}) + (\#\text{Ecken})$, da S eine Fläche ist und $\chi(S) = 1$ vorausgesetzt wird, dann folgt, dass $\#\text{Flächen} = \#\text{Kanten}$. Dies ist nur bei einer Scheibe oder der projektiven Ebene der Fall. Die projektive Ebene lässt sich aber nicht in $\mathbb{R}^3$ einbetten. □

5.3 Normalflächen

Definition 5.9 *Sei t im Folgenden die Anzahl der Tetraeder $\{T_i\}_{i=1}^{t}$ in einer guten Triangulierung $\mathcal{T}$ von M_K. Eine Fläche $S \subseteq M_K$ heißt Normalfläche, wenn sie echt eingebettet ist und ihr Schnitt mit jedem Tetraeder von $\mathcal{T}$ aus nur endlich vielen Drei- und Vierecken besteht, deren Ecken auf verschiedenen Kanten des entsprechenden Tetraeders liegen.*

Bemerkung 5.10 *Eine Normalfläche ist nicht notwendigerweise zusammenhängend (in mancher Literatur wird das hier definierte als „System von Normalflächen" bezeichnet und Normalflächen sind dort zusammehängend)*

Eine Normalfläche kann ein Tetraeder nur auf sieben verschiedene Weisen schneiden. Die ersten vier (im Folgenden Schnitttyp 1, 2, 3 oder 4 genannt) entstehen dadurch, dass eine Ecke des Tetraeders jeweils von den anderen drei getrennt wird und die die letzten drei (im Folgenden Schnitttyp 5, 6 oder 7 genannt) trennen zwei Eckpunkte des Tetraeders jeweils von den beiden anderen.
Jeder Schnitttyp kann mehrmals vorkommen, wir wollen Flächen nun anhand der Anzahl der auftrettenden Schnitttypen charakterisieren:

Definition 5.11 *Sei*

$$\begin{array}{rccl} v: & \{S \mid S \text{ Normalfläche}\} & \to & (\mathbb{Z}^7)^t = \mathbb{Z}^{7t} \\ & S & \mapsto & v(S) = (v_1, \ldots, v_t) \end{array}$$

hierbei ist $v_t = (v_{t1}, \ldots, v_{t7})$ und v_{ij} die Anzahl der Schnitte vom Typ j im Tetraeder T_i. Für eine Normalfläche S heißt $v(S)$ Normalkoordinaten von S.

Wann entspricht ein $v \in \mathbb{Z}^{7t}$ nun einer Normalfläche? Dazu betrachten wir einige Eigenschaften, die $v(s)$ haben muss:

Nicht-Negativitäts-Eigenschaft $v_{ij} \geq 0 \ \forall i \{1, \ldots, t\}, j \in \{1, \ldots, 7\}$

Verklebe-Eigenschaft Betrachte zwei Indices $i, j \in \{1, \ldots, t\}$ s.d. $T_i, T_j \in \mathcal{T}$ Tetraeder mit einer gemeinsamen Fläche sind. Für jedes Paar von Seiten in diesem Schnittdreieck kann es in beiden Tetraedern maximal jeweils einen Schnitt vom Typ 1, 2, 3 oder 4 und einen vom Typ 5, 6 oder 7 geben. Seien $k_1 \in \{1, 2, 3, 4\}$ und $l_1 \in \{5, 6, 7\}$ die vorkommenden Schnitttypen in T_i und k_2 und l_2 die entsprechenden in T_2, dann gilt:

$$v_{ik_1} + v_{il_1} = v_{jk_2} + v_{jl_2}$$

da jede auftretende Schnittkante von Schnitten in beiden Tetraedern herrühren muss.

Vierecks-Eigenschaft Kommt in einem Tetraeder ein Schnitt vom Typ $k \in \{5, 6, 7\}$ vor, so kommt kein Schnitt vom Typ $l \in \{5, 6, 7\} - \{k\}$ vor, sonst wäre s nicht echt eingebettet (würde sich selbst überschneiden).

[HAK] zeigte, dass alle $v \in \mathbb{Z}^{7t}$, die obige Eigenschaften erfüllen eine Normalfläche S mit $v(S) = v$ bis auf Isotopie von $\mathbb{R}^3$ eindeutig fest legen.

Definition 5.12 *Eine Menge $C \subseteq \mathbb{R}^n$ heißt Kegel, wenn $\lambda x \in C$ für alle $\lambda \geq 0$ und $x \in C$. Für $A \in \mathbb{R}^{n \times n}$ heißt eine Menge $\{x \in \mathbb{R}^n \mid Ax \geq 0\}$ polyedrischer Kegel. Eine Hilbertbasis eines Kegels $C \subseteq \mathbb{R}^n$ ist eine minimale Menge $B \subset \mathbb{Z}^n$ s.d.*

$$C = \{\lambda_1 x_1 + \ldots + \lambda_n x_n \mid x_i \in B, \lambda_i \in \mathbb{Z}_{\geq 0}\}$$

Definition 5.13 *Alle Punkte $v \in \mathbb{Z}^{7t}$ mit der Nicht-Negativitäts-Eignschaft sind enthalten im polyedrischen Kegel*

$$\mathbb{R}^{7t,+} := \left\{x = (x_1, \ldots, x_{7t}) \in \mathbb{R}^{7t} \mid x_i \geq 0 \ \forall i\right\}$$

Die Punkte aus $\mathbb{Z}^{7t} \subseteq \mathbb{R}^{7t,+}$ mit der Verklebe-Eigenschaft nennt man Haken-Normal-Kegel $\mathcal{C}_{M_K}$ und die Menge der Punkte in $\mathcal{C}_{M_K}$ mit der Rechtsecks-Eigenschaft heißt $\mathcal{W}_{M_K}$. Eine Fläche S heißt zusammengesetzt, wenn es Flächen S' und S'' gibt s.d. $v(S) = v(S') + v(S')$. Nicht-zusammengesetzte Flächen heißen Fundamentalflächen.

Fundamentalflächen sind zusammenhängend. Sonst wären ihre Normalkoordinaten die Summe der Normalkoordinaten ihrer Zusammenhangskomponten. Die Normalkoordinaten einer Fundamentalfläche liegt in der minimalen Hilbert Basis des Kegels $\mathcal{C}_M$ (welche endlich ist). Liegt die Normalkoordinaten auf einer Extremallinie von $\mathcal{C}_M$ so heißt sie Vertex-Fläche und $v(S)$ heißt Vertex-Lösung. Eine Vertex-Fläche heißt minimal, wenn sie Fundamentalfläche ist.

Satz 5.14 *Sei M eine kompakte 3-Manigfaltigkeit mit Rand $\partial M \neq \varnothing$. M enthalte eine essentielle Scheibe, dann enthält M auch eine essentielle Scheibe, die minimale Vertex-Fläche ist.*

Lemma 5.15 *Sei $v \in \mathbb{Z}^{7t}$ minimale Vertex-Lösung, dann gilt:*

$$\max v_i \leq 2^{7t-1}$$

Für jedes Element v einer Hilbert Basis von $\mathcal{C}_{\mathcal{M}}$ gilt:

$$\max v_i \leq t2^{7t+2} - 1$$

Lemma 5.16 *Der Haken-Normal-Kegel $\mathcal{C}_M$ hat maximal 2^{2t} minimale Vertex-Lösungen und er hat maximal $t^{7t}2^{49t^2+14t}$ Elemente in einer Hilbert-Basis.*

Lemma 5.17 *Sei D ein Knotentdiagramm mit n Kreuzungen. Dann kann man in der Zeit $O(n\log(n))$ Knoten K in $\mathbb{R}^3$ konstruieren, der in regulärer Position ist und D als Diagramm hat. Weiterhin erhält man eine kompakte triangulierte 3-Manigfaltigkeit $M_K = \mathbb{S}^3 - R_K$, deren Triangulierung gut ist und $O(n)$ Tetraeder enthält. In der Triangulierung ist ein Meridian auf dem Torus ∂M_K markiert.*

5.4 Zertifikat für den Unknoten

Wir wollen ein Element $v \in \mathcal{W}_{\mathcal{M}_\mathcal{K}}$ (dessen Normalenfläche S eine essentielle Scheibe eines Knotens K ist, den wir aus einem Diagramm D konstruiert haben) nun als Zertifikat für $UNKNOT$ verwenden. Dafür muss folgender Satz gelten:

Satz 5.18 *Es gilt:*

1. *Man kann dafür sorgen, dass t polynomiell in der Eingabegröße ist*
2. *die Elemente aus $\mathcal{W}_{\mathcal{M}_\mathcal{K}}$ sind nicht zu groß: es sollte wegen 4.4 eine Konstante c geben so dass für die einzelnen Eintrag gilt $v_i \in O(2^{cn})$*
3. *es ist in polynomieller Zeit nachvollziehbar, ob $v \in \mathcal{W}_{M_K}$ (also, ob v alle drei Eigenschaften aus 5.3 hat)*

Damit erhalten wir dann eine Normalfläche S mit $v(S) = v$ für diese ist nun noch in polynomieller Zeit nachvollziehbar:

4. *S ist zusammenhängend*

5. *S ist Scheibe*

6. *S ist essentiell*

Beweis:

1. Es lässt sich nach 5.17 eine Knoten finden dessen Triangulierung $t \in O(n)$ Tetraeder hat.

2. Die in 5.15 gegebnen Schranken sichern, dass es eine Konstante c gibt und somit auch eine durch $t = c'n$ definierte Konstant c' so dass $v_i \in O(2^{ct}) = O(2^{c'n})$. (beispielsweise genügt $c = 8$)

3. **Nicht-Negativitäts-Eigenschaft** Es muss für alle $i \in \{1, \ldots, t\}$ und $j \in \{1, \ldots, 7\}$ gelten, dass $v_{ij} \geq 0$. Dies kann also in $O(7t) = O(n)$ geprüft werden

   Verklebe-Eigenschaft Hier müssen Bedingungen der Form $v_{a_i} + v_{b_i} = v_{c_i} + v_{d_i}$ geprüft werde. Die Anzahl dieser Bedingungen ist im schlimmsten Fall die maximale Anzahl der Verklebungen von t Tetraedern multipliziert mit 3 (da es in jedem Schnittdreieck 3 mögliche Paare von Seiten gibt). Geht man also davon aus, dass jedes Tetraeder auf allen vier Seiten verklebt ist ergibt sich
   $$3 \cdot \frac{4t}{2} = 6t$$
   als Anzahl von Bedingungen. Die Prüfung ist also auch in $O(6t) = O(n)$ möglich

   Rechtecks-Eigenschaft Hier muss geprüft werden, ob für $i \in 1, \ldots, t$ und $j \in \{5, 6, 7\}$ maximal ein v_{ij} ungleich 0 ist. Also genügt auch hier $O(3t) = O(n)$.

4. S ist zusammenhängend, dies läßt sich zeigen indem man zeigt, dass v Minimal-Lösung ist

5. S ist nun also zusammenhängend und trianguliert. $\chi(S)$ lässt sich durch eine passende Linear-Kombination von Komponenten von v berechnen. Und somit folgt nach 5.8, dass S eine Scheibe ist

6. Nach 5.7 genügt es zu prüfen, ob ∂S und K nicht verknotet sind und ob ∂S die vom durch 5.17 markierten Meridian berandete Fläche einmal durchsticht.

□

Literatur

[HLP] Joel Hass, Jeffry C. Lagarias, Nicholas Pippenger, „The Computational Complexity of Knot and Link Problems“, http://1kh.de/311552

[RAB] Michael O. Rabin, „Recursive Unsolvability of Group-Theoretic Problems“, Annales of Mathematics, 67 (1985) S. 172-194

[HAK] W. Haken, „Theorie der Normalflächen: Ein Isotopiekriterium für den Kreisknoten“, Acta Math., Hauptsatz 2, 105 (1961) 245-375