Sei $\mathfrak{C} = (O, M, Q, Z, 0)$ eine Kategorie von Abbildungen:

$$Q : M \longrightarrow O,\ \ Z : M \longrightarrow O.$$

M ist die Menge der Abbildungen oder Morphismen und O die Menge der „Objekte“ der Kategorie. Ist $f \in M$, dann ist $f : Q(f) \longrightarrow z(f)$ eine Abbildung.

Beispiel:

(1) $\begin{array}{rcl} O & := & \{\mathbb{N}^k \mid k = 0, 1, 2, \ldots\} \\ M & = & \mathbb{P}. \end{array}$

(2) $\begin{array}{rcl} O & = & \mathbb{N}^*, \\ M & = & \{f\ \mathbb{P}\text{-berechenbar über } \mathbb{N} \mid f \text{ total}\}. \end{array}$

(3) $\begin{array}{rcl} O & = & \mathbb{N}, \\ M & = & \{f \in \mathbb{P} \mid Z(f) = Q(f) = \mathbb{N}\}. \end{array}$

(4) $\begin{array}{rcl} O & = & \mathbb{B}^*, \\ M & = & \{f : \mathbb{B}^* \to \mathbb{B}^* \mid f \text{ turingberechenbar} \\ & & \ \& \ f \text{ total}\}. \end{array}$

(5) $\begin{array}{rcl} O & = & \mathbb{B}^*, \\ M & = & \{f : \mathbb{B}^* \to \mathbb{B}^* \mid f \text{ turingberechenbar} \\ & & \text{in Zeit } O(n^k) \text{ für ein geeignetes } k\}. \end{array}$

Wir setzen $Pol := (O, M, Q, Z, 0)$. Pol ist die Kategorie der in Polynomialzeit berechenbaren Funktionen.

Definition: Sind $D_i \subset O_i \in O(\mathfrak{C})$ und gibt es $f : O_1 \longrightarrow O_2$ mit $L_1 = f^{-1}(L_2)$, dann schreiben wir

$$L_1 \underset{\mathfrak{C}}{\leq} L_2.$$

Sprechweise: L_1 ist mittels $\mathfrak{C}$ auf L_2 reduzierbar. Genauer:

Das „Wortproblem“:	gilt für $w \in O_1$
	$w \in L_1$?

ist $\mathfrak{C}$ **reduzierbar** auf $f(w) \in L_2$? durch ein geeignetes $f \in \mathfrak{C}$.

Die Sprechweise wird verständlicher durch das

Lemma: $L_1 \underset{\mathfrak{C}}{\leq} L_2 \iff$ Es gibt ein $f \in M(\mathfrak{C})$ mit (1) und (2).

(1) $L_1 \subset Q(f),\ L_2 \subset Z(f)$

(2) $w \in L_1 \iff f(w) \in L_2$.

Lemma: $\underset{\mathfrak{C}}{\leq}$ ist idempotent und transitiv.

Beweis: Sei $L_1 \underset{\mathfrak{C}}{\leq} L_2$, $L_2 \underset{\mathfrak{C}}{\leq} L_3$,
$\Longrightarrow \exists f_1$ und f_2 in $\mathfrak{C}$ mit

$$L_1 = f_1^{-1}(L_2) \text{ und } L_2 = f_2^{-1}(L_3).$$

Hieraus folgt

$$L_1 = f_1^{-1}(f_2^{-1}(L_3)) = (f_2 \circ f_1)^{-1}(L_3).$$

Wegen $f_2 \circ f_1 \in M(\mathfrak{C})$ ist $L_1 \underset{\mathfrak{C}}{\leq} L_3$.

Damit ist der zweite Teil des Lemmas bewiesen. Der erste Teil ergibt sich, da 1_{0_1} definitionsgemäß in $\mathfrak{C}$ liegt.

Definition:

$$L_1 \underset{\mathfrak{C}}{\equiv} L_2 :\Longleftrightarrow L_1 \underset{\mathfrak{C}}{\leq} L_2 \;\&\; L_2 \underset{\mathfrak{C}}{\leq} L_1.$$

Offensichtlich ist $\equiv_{\mathfrak{C}}$ eine Äquivalenzrelation.

Satz: Ist $\mathfrak{C} = (M, O)$ mit $O = \{\mathbb{N}^k \mid k = 0, 1, 2, \ldots\}$ und $M \subset \mu\mathbb{P}$, dann folgt aus $L' \underset{L}{\leq}$ und $\chi_{L'} \notin \mu\mathbb{P}$, daß $\chi_L \notin \mu\mathbb{P}$ gilt.

Beweis: Aus $\chi_L \in \mu\mathbb{P}$ und $f \in \mathfrak{C}$ folgt $\chi_{L'} = \chi_L \circ f \in \mu\mathbb{P}$. Widerspruch zur Voraussetzung.

Wir werden diesen Satz verwenden um für eine Reihe von Problemen zu zeigen, daß sie nicht entscheidbar sind.

Erläuterung des Konzeptes:
Die Reduktionstheorie hat sich aus der Geometrie entwickelt. Die Kategorie $\mathfrak{C}$ ist dort eine Gruppe von Bewegungen.

Sei $G = \mathfrak{C}$ die Gruppe der Bewegungen im euklidischen Raum und $L_1 = \{P_1, P_2, P_3\}, L'_1 = \{P'_1, P'_2, P'_3\}$ seien Punktetripel aus dem $\mathbb{R}^3$. Es gilt dann

$$L_1 \leq L_2 \iff \text{Es gibt } f \in G \text{ mit } L_1 = f^{-1}(L_2).$$

Da G eine Gruppe ist, gilt auch $f^{-1} \in G$, so daß wegen $L_2 = (f^{-1})^{-1}(L_1) = f(L_1)$ auch $L_2 \underset{G}{\leq} L_2$.

In anderen Worten: Aus $L_2 \underset{G}{\leq} L_1$ folgt, daß die beiden Dreiecke P_1, P_2, P_3 und $P'_1 P'_2 P'_3$ kongruent sind.

Aus der Schule kennt man Kongruenzsätze, wie

> Zwei Dreiecke sind genau dann kongruent, wenn sie in drei Seiten übereinstimmen.

Von kongruenten Dreiecken weiß man z. B., daß sie den gleichen **Flächeninhalt** haben. In der Reduktionstheorie versucht man, Probleme hinsichtlich ihrer **Komplexität** zu klassifizieren.

Man sucht Invarianten unter Reduktionen, wie es z.B. der Flächeninhalt für Bewegungen darstellt, um die Inäquivalenz von Sprachen relativ zu Kategorien $\mathfrak{C}$ zu zeigen.

Die gröbste Klassifikation liefert die Kategorie $\mathfrak{C}\mu$ der totalen μ-rekursiven Funktionen. man kann mit den in der Vorlesung vorgestellten Konstruktionen Mengen L definieren, so daß weder L und $\overline{L}$ aufzählbar sind. Die Kategorie erlaubt eine Klassifikation dieser Mengen. Für die Informatik interessanter sind Klassifikationen, die sich durch kleinere Reduktionskategorien ergeben. Am bekanntesten ist hier die oben definierte Kategorie Pol.

Um das mit dieser Kategorie verknüpfte berühmte Problem $\underline{P} = \underline{NP}$? zu verstehen, bedarf es noch einer Ergänzung.

Sei $\mathfrak{C}$ eine Reduktionskategorie und

$$\mathfrak{T} = \{L_1, L_2, \dots\}$$

eine Menge von Sprachen aus den Objekten von $\mathfrak{C}$.

Definition: Ist $L \subset O_i$ und $O_i \in O(\mathfrak{C})$, dann heißt L $\mathfrak{T}$-hart bezüglich $\mathfrak{C} :\iff \mathfrak{T} \subset \{f^{-1}(L) \mid f \in M(\mathfrak{C})\}$.

Erläuterung: Die Anwendung der auf den Teilmengen der Objekte von $\mathfrak{C}$ definierten Abbildungen f^{-1} mit $f \in M(\mathfrak{C})$ erzeugt ganz $\mathfrak{T}$ und eventuell noch mehr. Wir schreiben dafür $\mathfrak{T} \subset \mathfrak{C}^{-1}(L)$.

Definition: L heißt **$\mathfrak{F}$-vollständig** (complete) bezüglich $\mathfrak{C}$, falls $L \in \mathfrak{T}$ gilt und L $\mathfrak{T}$-hart ist.

In den interessanten Fällen gilt dann auch $\mathfrak{C}^{-1}(L) = \mathfrak{T}$.

Wir wählen nun $\mathfrak{C} = Pol$ und

$\mathfrak{T} := \underline{NP}$:= {L | L läßt sich durch eine nichtdeterministische Turingmaschine in polynomieller Zeit entscheiden.}

In diesem Fall gilt offensichtlich:

Ist $L \in \underline{NP}$, dann gilt $Pol^{-1}(L) \subset \underline{NP}$.

L ist also NP-vollständig genau dann, wenn $Pol^{-1}(L) = NP$ gilt.

Das Problem

$$\underline{P} = \underline{NP}?$$

ist die Frage, ob die Menge der in polynomieller Zeit entscheidbarer Probleme $\underline{P}$ gleich der Menge der **nicht**deterministisch in polynomieller Zeit entscheidbarer Probleme ist. Das ist ein schönes Problem.

Die Beantwortung dieser Frage hat für sich allein genommen wohl keine praktische Bedeutung. Die Frage ist aber wichtig, da sie zeigt, daß wir ein fundamentales Problem, nämlich ob richtig Raten „hilft“, noch nicht verstanden haben. Die Arbeiten zur Klärung dieser Frage berühren damit auch Probleme großer praktischer Relevanz. Aus diesem Grund ist es zu erwarten, daß bei der Suche nach einer Lösung dieses Problems Entdeckungen gemacht werden, die auch von großer praktischer Bedeutung sind.

Diese und verwandte Fragestellungen werden in der Vorlesung „Komplexitätstheorie“ ausführlich behandelt. Hier müssen wir uns mit dieser Skizze begnügen. Es sei nur noch hinzugefügt, daß die Frage, ob ein vorgegebener Schaltkreis der Größe n auf irgendeine mögliche Eingabe mit einer Ausgabe $= 1$ reagiert, ein NP-vollständiges Problem ist, wenn n als Maß für die Problemgröße dient. Das Testproblem für Schaltkreise ist also ein NP-vollständiges Problem.

Semi-Thue-Systeme

Sei A ein Alphabet und $P \subset A^* \times A^*$ eine endliche Menge. Wir betrachten nun Ableitungen von Wörtern, indem wir Substitutionen von Teilwörtern $u_1 \longrightarrow v_1$ zulassen, falls $(u_1, v_1) \in P$ ist. Wir definieren im folgenden die Relation $(u \xrightarrow{P})$ für $(u, v) \in A^* \times A^*$.

$$\begin{aligned} u &\xrightarrow{P} u \text{ für } u \in A^*, \\ w_1 u w_2 &\xrightarrow{P} w_1 v w_2 \text{ für } (u,v) \in P, \\ w_1 \xrightarrow{P} w_2,\ w_2 &\xrightarrow{P} w_3 \Rightarrow w_1 \xrightarrow{P} w_3. \end{aligned}$$

Definition: Das Tupel $\mathfrak{S} := (A^*, P, \rightarrow)$ heißt **Semi-Thue-System**.

Thue war ein norwegischer Mathematiker, der sich mit dem Wortproblem von Gruppen auseinandergesetzt hat. Ein $\mathfrak{S}$ heißt **Thue-System** $:\iff$ Aus $(u,v) \in P$ folgt $(v,u) \in P$.

Definition: Das Problem : „Gilt für $u, v \in A^*$ die Relation $u \xrightarrow{P} v$?“ heißt das Wortproblem für Semi-Thue-Systeme.

Gesucht ist also ein Algorithmus, der für gegebene P, u, v entscheidet, ob $u \xrightarrow{P} v$ gilt.

Satz: Das Wortproblem für Semi-Thue-Systeme ist nicht generell entscheidbar.

Beweis: Zum Beweis reduzieren wir das Halteproblem von Turingmaschinen auf das Wortproblem für Semi-Thue-Systeme. Hieraus folgt, wie wir gezeigt haben, die Nichtentscheidbarkeit des Wortproblems für Semi-Thue-Systeme.

Als Alphabet A wählen wir die Vereinigung des Bandalphabetes der TM mit dem Zustandsalphabet. P ist durch die Turingtafel gegeben.

Die Turingtafel hat die Form

$$\begin{array}{ccc} aqb & \longrightarrow & \left\{ \begin{array}{cccc} a & q_1 & b' & \\ c & q_1 & a & b' \\ a & b' & q_1 & c \end{array} \right. \\ \vdots & & \end{array}$$

Hierin tritt bei deterministischen TM höchstens eine der drei möglichen Formen auf.

Wir wählen

$$w = q_a u \text{ als Anfangskonfiguration}$$

und ergänzen die Turingtafel durch Terminalproduktionen

$$q_e a \longrightarrow q_e.$$

Das Halteproblem der TM reduziert sich auf das Problem

$$q_a u \longrightarrow q_e.$$

Man kann den Satz noch verschärfen zu dem

Satz: Es gibt ein spezielles Semi-Thue-System für das das Wortproblem nicht entscheidbar ist.

Beweis: Wie vorher: Man geht dabei von einer universellen TM aus, für die, wie wir gezeigt haben, das Halteproblem nicht entscheidbar ist.

Satz: Das Wortproblem für Thue-Systeme ist nicht generell entscheidbar.

Beweis: Sei $\mathfrak{S}$ ein deterministisches Semi-Thue-System, wie wir es aus einer Turingtafel erhalten, und $\mathfrak{T}$ gehe aus $\mathfrak{S}$ durch Symmetrischmachen hervor.

Wir zeigen

$$u \xrightarrow{\mathfrak{T}} v \iff u \xrightarrow{\mathfrak{S}} v \text{ oder } v \xrightarrow{\mathfrak{S}} u.$$

Sei $w_0 = q_0 w \in K_a$ und $w_P = q_e$ Endzustand der TM von der wir ausgehen. Wir betrachten eine reguläre oder kanonische Berechnung

$$w_0 \xrightarrow{\mathfrak{S}} w_1 \xrightarrow{\mathfrak{S}^{-1}} w_2 \xrightarrow{\mathfrak{S}} \ldots \xrightarrow{\mathfrak{S}} w_P.$$

Die Ableitung beginnt mit $\mathfrak{S}$, wenn wir die TM so normieren, daß ein Anfangszustand nicht mehr angenommen wird. Sie endet mit $\mathfrak{S}$, da der Endzustand in $\mathfrak{S}^{-1}$ nicht auf der rechten Seite vorkommt.

Nun betrachten wir die Situation

$$w' \xrightarrow{\mathfrak{S}^{-1}} w'' \xrightarrow{\mathfrak{S}} w'''.$$

Da die Turingmaschine, von der wir $\mathfrak{S}$ abgeleitet haben, deterministisch ist, sind durch die Umkehrungen der Maschine keine Verzweigungen möglich.

Hieraus ergibt sich, daß wir in der Ableitung den Abschnitt

$$w_{p-2} \xrightarrow{\mathfrak{S}^{-1}} w_{p-1} \xrightarrow{\mathfrak{S}} w_p$$

durch

$$w_{p-2} \xrightarrow{\mathfrak{S}} w_p$$

ersetzen dürfen (w_p kommt in keiner Regel von $\mathfrak{S}^{-1}$ auf der rechten Seite vor). Durch Iteration des Schlusses erhalten wir

$$w_0 \xrightarrow{\mathfrak{S}} w_p.$$

Damit haben wir die Ableitungen über $\mathfrak{S}$ durch Ableitungen über $\mathfrak{T}$ simuliert. Die Simulation ist treu, da die Anfangs- und Endkonfigurationen identisch sind. Also haben wir das Wortprobelm von $\mathfrak{S}$ auf das Wortproblem von $\mathfrak{T}$ reduziert.