VII. Spektralproblem und Komplexitätstheorie

von Claude-André Christen

1. Einleitung und Uebersicht

Ein Merkmal der modernen Axiomensysteme ist ihre Nicht-Kategorizität, d.h. die Tatsache, dass solche Systeme im allgemeinen nicht eine einzige Struktur, sondern eine ganze Klasse von Strukturen charakterisieren. Obwohl der Zweck eines Systems ausdrücklich darin besteht, die gemeinsamen Eigenschaften ihrer Modelle darzustellen, bleibt das Interesse nach der Klassifizierung dieser Modelle weiterhin bestehen.

Die einfachste Eigenschaft einer Struktur ist wohl ihre Mächtigkeit; die Frage nach den Mächtigkeiten der Modelle einer axiomatischen Theorie liegt also nahe, und lässt sich manchmal genau beantworten. Allgemein bekannt sind die Beispiele der Körper, der Körper einer gegebenen Charakteristik, der Schiefkörper und der Booleschen Algebren: Die Ordnung eines endlichen Körpers ist Potenz einer Primzahl (nämlich der Körper-Charakteristik), und umgekehrt gibt es zu jeder Primzahlpotenz einen Körper dieser Ordnung; weiter gibt es Körper jeder unendlichen Mächtigkeit. Nach dem Satz von Wedderburn gibt es keine endliche, nichtkommutative Schiefkörper; es gibt aber nicht-kommutative Schiefkörper jeder unendlichen Mächtigkeit. Schliesslich sind die Mächtigkeiten der Booleschen Algebren genau die Zweierpotenzen und die unendlichen Mächtigkeiten.

In anderen Fällen ist das Problem ungelöst: Man weiss zum Beispiel heutzutage nicht, für welche Mächtigkeiten es einfache Gruppen dieser Ordnung gibt. Ebenfalls weiss man auch nicht, welche Mächtigkeiten als Ordnung einer nicht-auflösbaren Gruppe auftreten; allein der Nachweis der alten Burnside-Vermutung (laut welcher alle nicht-auflösbaren Gruppen gerade Ordnung haben) braucht ungeheuren Aufwand.

An sich hat die besprochene Mächtigkeitsfrage keine allzu grosse Bedeutung; sie wird deshalb bei einer Theorie auch nur dann in Betracht gezogen, wenn sie in Verbindung mit tiefer liegenden Struktureigenschaften auftritt.

Eine ganz andere Bedeutung hat aber folgendes Problem, wo das Interesse von den einzelnen Theorien zu den dadurch definierbaren Mächtigkeitsklassen verschoben wird: Was sind überhaupt die möglichen Mächtigkeitsklassen der Modelle einer axiomatischen Theorie? Natürlich ist dabei

eine Präzisierung des Wortes "Theorie" notwendig. Erstaunlicherweise wurde dieses Problem erst durch (Scholz 1952) gestellt, und zwar für Theorien, die in der Prädikatenlogik erster Stufe (mit Gleichheit) formulierbar sind.
Besondere Eigenschaften der Prädikatenlogik erster Stufe erlauben übrigens eine engere Formulierung des Problems:
Zunächst ist es klar, dass das Problem trivial wird, falls man das Gleichheitszeichen nicht zulässt: Hat dann eine Theorie überhaupt ein Modell, so auch ein Modell jeder grösseren Mächtigkeit.

Auf Grund des Satzes von Löwenheim-Skolem hat eine abzählbare Theorie erster Stufe entweder keine unendlichen Modelle oder Modelle jeder unendlichen Mächtigkeit. Weiter folgt aus dem Kompaktheitssatz, dass es eine endliche Schranke für die Mächtigkeiten der Modelle einer Theorie gibt, falls diese Theorie kein unendliches Modell besitzt. Es genügt also, die Frage für die endlichen Mächtigkeiten zu stellen.

Lässt man Systeme mit unendlich vielen Axiomen zu, so wird das Problem wiederum trivial: Jede Teilmenge der Menge der positiven ganzen Zahlen ist in dieser Weise darstellbar, denn jede endliche Mächtigkeit ist schon mit einer Gleichheitsformel ohne freie Variable charakterisierbar; die negierte Formel schliesst dann gerade diese Mächtigkeit aus. Werden aber nur endlich viele Axiome zugelassen - oder nur eines, was auf dasselbe herauskommt - so können nur noch abzählbar viele Mengen dargestellt werden.

Auf Grund dieser Reduktionen definiert man das Spektrum einer logischen Formel als die Menge der Mächtigkeiten ihrer endlichen Modelle. Eine Menge heisst dann Spektrum erster Stufe, falls es eine Formel erster Stufe gibt, deren Spektrum sie ist. Das Spektralproblem lautet nun: Welche Mengen sind Spektren erster Stufe? (Zur Abkürzung wird von nun an unter "Spektrum" immer "Spektrum erster Stufe" gemeint.)

Es sei noch ausdrücklich hervorgehoben, dass dieses Problem einen extensionalen Standpunkt voraussetzt: Im Falle der Zweierpotenzen zum Beispiel ist es gleichgültig, ob die Menge als Spektrum eines Axiomensystems für die Booleschen Algebren oder für die Körper der Charakteristik 2 - oder durch irgend ein anderes passendes System - dargestellt wird: Es kommt nur darauf an, dass mindestens eine solche Charakterisierung existiert.

Es stellt sich bald heraus, dass die Spektren schon recht komplizierte

Mengen sein können. Das Spektrum der Theorie der nicht-zyklischen Gruppen besteht zum Beispiel genau aus den Zahlen, welche durch eine von 1 verschiedene Quadratzahl, oder durch zwei Primzahlen teilbar ist, deren eine kongruent 1 modulo die andere ist. Es gibt genau dann eine nicht-abelsche Gruppe der endlichen Ordnung n, wenn n durch eine von 1 verschiedene Kubikzahl oder durch pq^2 teilbar ist, wobei p und q prim sind, und q^2 kongruent 1 modulo p ist (siehe Pazderski 1959, wo noch andere Beispiele behandelt werden).

Es ist sogar einfacher, Mengen anzugeben, die Spektren sind, als Mengen, die es nicht sind - eine Berechtigung dieser unmathematischen Behauptung ist die Tatsache, dass alle bekannten Beispiele von Mengen, die keine Spektren sind, mehr oder weniger auf Diagonalisierung beruhen. Wie schlecht die Struktur der Spektren noch verstanden wird, zeigt die einfache, doch ungelöste Frage (Asser 1956): Ist die Klasse der Spektren gegenüber Komplementbildung abgeschlossen? (Es ist dagegen leicht nachzuweisen, dass sie gegenüber Vereinigung und Durchschnitt abgeschlossen ist.)

Im zweiten Paragraphen werden Beispiele angegeben, welche die Kompliziertheit der Spektren veranschaulichen, und zudem einen Vorgeschmack für die später benützte Darstellungsmethode angeben:
Obwohl alle Spektren primitiv rekursiv sind, gibt es ein Spektrum, dessen Aufzählungsfunktion schliesslich stärker als jede primitiv rekursive Funktion wächst. Die Modelle der gewählten zugehörigen Formel stellen Anfangsstücke des Graphen einer Modifikation der Ackermann-Funktion dar.

Es gibt aber sogar zu jeder rekursiven Funktion ein Spektrum, dessen Aufzählungsfunktion stärker als diese Funktion wächst. Diese Behauptung lässt sich aus der Tatsache ableiten, dass die konstruktiv arithmetischen Mengen Spektren sind. Daraus lässt sich ebenfalls beweisen, dass es nicht rekursiv entscheidbar ist, ob ein Spektrum leer ist oder nicht (dies wurde schon von Trachtenbrot 1950 bewiesen); das Problem hat sogar den höchsten Unentscheidbarkeitsgrad unter den rekursiv aufzählbaren Problemen (Büchi 1962). Analog ist das Unendlichkeitsproblem für Spektren $\Pi\Sigma$-vollständig bezüglich Turing-Reduzibilität.

Es ist jedoch klar, dass die Spektren nur eine beschränkte Komplexität aufweisen können, denn es gibt nur 2^{n^r} r-stellige Prädikate auf einem n-elementigen Bereich. Deshalb ist die Zugehörigkeit der Zahl n zu einem

Spektrum für ein geeignetes c in höchstens 2^{n^c} Schritte auf einer Turing-Maschine entscheidbar. Als Folgerung erweist sich die Klasse der Spektren als eine Teilklasse der Klasse der im Kalmárschen Sinne elementaren Funktionen; (Asser 1956) bewies schon, dass die Inklusion echt ist.

Im dritten Paragraphen wird das Hauptergebnis von (Jones & Selman 1974) bewiesen: Die Spektren stimmen mit den Mengen überein, welche durch eine schliesslich exponentiell (d.h. der Form $\lambda x.2^{cx}$ für $c \in \mathbb{N}$) beschränkte nichtdeterministische Turing-Maschine akzeptiert werden. Wird als Input nicht die dyadische Kodierung von n, sondern ein Wort der Länge n (z.B. n mal b_1) gebraucht, so ist die Schranke polynomial. Deshalb ergibt sich ein Zusammenhang mit dem Problem P = NP: Gilt P = NP, so sind auch die Spektren deterministisch mit einer polynomialen Schranke auf einer Turingmaschine zu berechnen (bei Input n mal b_1). Analog: Ist NP gegenüber Komplementbildung abgeschlossen, so auch die Klasse der Spektren. Ein Beweis, dass die Klasse der Spektren gegenüber Komplementbildung nicht abgeschlossen ist, ist also mindestens so schwer, wie ein Beweis, dass NP gegenüber Komplementbildung nicht abgeschlossen ist; und ein Beweis, dass es ein Spektrum gibt, das durch keine deterministische exponentiell-beschränkte Turingmaschine berechenbar ist, mindestens so schwer, wie ein Beweis von $P \neq NP$.

Im vierten Paragraphen werden die Mengen aus NP und die endlich axiomatisierbaren projektiven Klassen von Strukturen von endlichem Typus in Verbindung gebracht. Der gewonnene Satz ist eine Verallgemeinerung des früheren Hauptsatzes, betrifft allerdings nur die endlichen Strukturen einer solchen Klasse: Mittels einer gewissen Kodierung fallen diese Klassen von endlichen Strukturen und die Mengen von NP zusammen. Man achte doch darauf, dass der hier angenommene Standpunkt nicht derjenige der Modelltheorie ist, sondern eher derjenige der finiten Mathematik (mit einem naiven Begriff des Endlichen).

Es gibt zum Beispiel ein nicht-deterministisches polynomiales Verfahren, welches die endlichen zyklischen Gruppen akzeptiert und die endlichen nicht-zyklischen Gruppen verwirft. Dies entspricht hier der Tatsache, dass es eine endlich axiomatisierbare projektive Klasse gibt, deren endliche Strukturen genau die endlichen zyklischen Gruppen sind, obwohl weder die Klasse der endlichen zyklischen Gruppen noch die ganze Klasse der zyklischen Gruppen eine projektive Klasse bilden.

Endlich werden noch am Schluss der Arbeit Ergebnisse über Spektren

höherer Stufe aufgezählt; für Beweise wird auf die zitierte Literatur hingewiesen.

2. Beispiele von Spektren

Zunächst wird kurz die Sprache der Prädikatenlogik erster Stufe beschrieben, sowie die Begriffe "Interpretation" und "Modell" erläutert.

Die Grundzeichen der Prädikatenlogik erster Stufe sind die (logischen) Zeichen $\vee$, $\wedge$, $\neg$, $\exists$, $\forall$, (,), =
und die (nicht-logischen) Zeichen aus $Z = V \cup FZ \cup PZ$:

$V = \{v_i \mid i \in \mathbb{N}\}$ ist die Menge der Individuenvariablen;

$FZ = \{f_i^j \mid i,j \in \mathbb{N}\}$ ist die Menge der Funktionszeichen;

$PZ = \{p_i^j \mid i,j \in \mathbb{N}\}$ ist die Menge der Prädikatszeichen.

Aus diesen Grundzeichen werden Ausdrücke - d.h. Folgen von Zeichen - gebildet. Die Concatenation von Folgen wird einfach durch Hintereinanderschreiben der Folgen bezeichnet. Bedeutung wird nur den folgenden drei Klassen T, A und F von Ausdrücken zuerkannt:

Die Menge T der Terme ist die kleinste Menge, welche die Folgen der Länge 1, bestehend aus einem Zeichen aus V, enthält, und welche für $i,j \in \mathbb{N}$ die Concatenation von f_i^j mit den j Termen $t_1,\ldots,t_j$ enthält. Die Zeichen f_i^j heissen deshalb "j-stellige" Zeichen; der Lesbarkeit halber wird - auch im Falle j=o - die Folge $f_i^j\, t_1 \ldots t_j$ mit $f_i^j(t_1,\ldots,t_j)$ bezeichnet.

Die Menge A der Atomformeln ist die Menge der Ausdrücke der Form $t_1 = t_2$ und $p_i^j(t_1,\ldots,t_j)$ für $i,j \in \mathbb{N}$ und $t_1,\ldots,t_j \in T$ (mit derselben Bezeichnungskonvention wie oben; die p_i^j heissen auch j-stellig).

Die Menge F der Formeln ist die kleinste Menge, welche A enthält und mit $f_1, f_2 \in F$ und $v \in V$ auch die Ausdrücke
$(f_1 \vee f_2)$, $(f_1 \wedge f_2)$, $\neg f_1$, $(\exists v) f_1$, $(\forall v) f_1$ enthält.

Es lässt sich beweisen, dass jeder Term (sowie jede Formel) gemäss diesen Regeln auf eine einzige Weise gebildet ist.

-Formeln der Form $(Q_1 v_{i_1}) \ldots (Q_k v_{i_k}) f$, wobei jedes Q_j ein Quantorzeichen $\forall$ oder $\exists$ bezeichnet und f keine Quantorzeichen enthält, heissen pränex. f ist die Matrix der Formel und $(Q_1 v_{i_1}) \ldots (Q_k v_{i_k})$ ihr Präfix. Bekanntlich gibt es zu jeder Formel eine dazu äquivalente pränexe Formel.

Eine Formel heisst abgeschlossen, wenn jede Okkurenz einer Individuenvariablen v auch Okkurenz einer Teilformel von f der Form $(\exists v) f'$ oder

$(\forall v)f'$ ist.

Eine Struktur für eine Formel f der Prädikatenlogik erster Stufe ist ein Paar <M,I>, wobei M eine nicht-leere Menge ist, und I eine für die in f vorkommenden Zeichen aus Z definierte Funktion ist, welche folgende Eigenschaften besitzt:

(a) für $i \in \mathbb{N}$ ist $I(v_i)$ eine Funktion von $M^{\mathbb{N}}$ nach M; dabei ist $[I(v_i)](c) = c_i$ für $c \in M^{\mathbb{N}}$;

(b) für $i,j \in \mathbb{N}$ ist $I(f_i^j)$ eine Funktion von M^j nach M;

(c) für $i,j \in \mathbb{N}$ ist $I(p_i^j)$ eine Funktion von M^j nach $2 = \{0,1\}$.
Bemerkung: M^0 ist $\{\emptyset\}$.

Aus I wird induktiv eine Interpretation J der Terme und Formeln, die aus diesen Zeichen gebildet werden, wie folgt eindeutig definiert:

(1) für $i,j \in \mathbb{N}$, $t_1,\ldots,t_j \in T$ und $c \in M^{\mathbb{N}}$ ist $J(f_i^0)(c) = I(f_i^0)(\emptyset)$ und
$J(f_i^{j+1}(t_1,\ldots,t_{j+1}))(c) = I(f_i^{j+1})(J(t_1)(c),\ldots,J(t_{j+1})(c))$;

(2) für $i,j \in \mathbb{N}$, $t_1,\ldots,t_j \in T$ und $c \in M^{\mathbb{N}}$ ist
$J(p_i^0)(c) = I(p_i^0)(\emptyset)$ und
$J(p_i^{j+1}(t_1,\ldots,t_{j+1}))(c) = I(p_i^{j+1})(J(t_1)(c),\ldots,J(t_{j+1})(c))$;

(3) für $t,t' \in T$ und $c \in M^{\mathbb{N}}$ ist

$$J(t=t')(c) = \begin{cases} 1 \text{ falls } J(t)(c) = J(t')(c) \\ 0 \text{ sonst} \end{cases};$$

für $f,f' \in F$, $i \in \mathbb{N}$ und $c \in M^{\mathbb{N}}$ ist:

(4) $J(f \vee f')(c) = \max(J(f)(c), J(f')(c))$

(5) $J(f \wedge f')(c) = \min(J(f)(c), J(f')(c))$

(6) $J(\neg f)(c) = 1 - J(f)(c)$

(7) $J((\exists v_i)f)(c) = \max\limits_{m \in M} J(f)(c|_m^{c_i})$

(8) $J((\forall v_i)f)(c) = \min\limits_{m \in M} J(f)(c|_m^{c_i})$

$$\left(\text{dabei ist } c|_m^{c_i}(k) = \begin{cases} c_k \text{ falls } k \neq i \\ m \text{ sonst} \end{cases}\right)$$

Eine Struktur <M,I> ist ein Modell von f, falls es für die von I erzeugte Interpretation ein $c \in M^{\mathbb{N}}$ gibt, mit $J(f)(c) = 1$. Eine Formel heisst k-elementig erfüllbar, falls sie ein Modell <M,I> mit $\bar{M} = k$ besitzt.

Das Spektrum einer Formel f ist die Menge der positiven Zahlen n, für welche f n-elementig erfüllbar ist.
Als erstes Beispiel werden die Spektren von Gleichheitsformeln untersucht - das sind die Formeln, die weder Funktions- noch Prädikatszeichen enthalten. Wie man leicht aus den angegebenen Definitionen ableiten kann, ist $\mathbb{N}$ das Spektrum der Formel $v_0=v_0$ und die leere Menge das Spektrum der Formel $\neg\, v_0=v_0$ (die kurz $v_0\neq v_0$ geschrieben wird). Das Spektrum der Formel $(\exists v_0)(\exists v_1)\ v_0\neq v_1$ (oder von $v_0\neq v_1$, was für die Erfüllbarkeit auf dasselbe herauskommt) besteht aus allen ganzen Zahlen, die grösser als 1 sind; dasjenige von $(\forall v_0)(\forall v_1)\ v_1 = v_0$ oder dasjenige von $(\exists v_0)(\forall v_1)\ v_1 = v_0$ dagegen aus der einzigen Zahl 1. Allgemeiner besteht das Spektrum der Formel

$$(\exists v_0)\ldots(\exists v_k)(\ldots((v_0\neq v_1 \wedge v_0\neq v_2)\wedge v_0\neq v_3)\ldots\wedge v_{k-1}\neq v_k),$$

welche durch $(\exists v_0)..(\exists v_k)\bigwedge_{0\leq i<j\leq k} v_i\neq v_j$ abgekürzt wird, aus den Zahlen, die grösser als k sind, und das Spektrum der Formel

$$(\forall v_0)\ldots(\forall v_{k+1})(\ldots((v_0=v_1 \vee v_0=v_2)\vee v_0=v_3)\ldots\vee v_k=v_{k+1}),$$

welche durch $(\forall v_0)\ldots(\forall v_{k+1})\bigvee_{0\leq i<j\leq k+1} v_i=v_j$ abgekürzt wird, aus den Zahlen, die kleiner als k+2 sind; dasselbe Spektrum hat die Formel

$$(\exists v_0)\ldots(\exists v_k)(\forall v_{k+1})\bigvee_{0\leq i\leq k} v_{k+1} = v_i.$$

Folglich besteht das Spektrum von

$$(\exists v_0)\ldots(\exists v_k)(\forall v_{k+1})\Big(\bigwedge_{0\leq i<j\leq k} v_i\neq v_j \wedge \bigvee_{0\leq i\leq k} v_{k+1}=v_i\Big)$$

aus der einzigen Zahl k+1.
Eine beliebige endliche Menge ist also Spektrum einer Gleichheitsformel: Nämlich Spektrum der Disjunktion von Formeln der zuletzt erwähnten Form, die die Elemente der Menge charakterisieren. Das Spektrum der Negation dieser Formel ist die komplementäre Menge; folglich ist auch jede koendliche Menge Spektrum einer Gleichheitsformel.
Umgekehrt gilt aber auch, dass die Spektren der Gleichheitsformeln genau die endlichen und koendlichen Mengen sind: Da diese Formeln weder Funktions- noch Prädikatszeichen enthalten, sind die Klassen der Mächtigkeiten der Modelle einer abgeschlossenen Formel und ihrer Negation komplementär. Nach dem Satz von Löwenheim hat also genau eine davon unendliche Modelle; nach dem Kompaktheitssatz hat aber dann die andere Formel ein endliches Spektrum.
Dieser Beweis lässt sich nicht auf den allgemeinen Fall erweitern, denn die Formeln $(\exists v_0)p_0^1(v_0)$ und $\neg\,(\exists v_0)p_0^1(v_0)$ sind schon beide in beliebi-

gen Bereichen erfüllbar. Trotzdem sind die Spektren der monadischen Formeln (d.h. der Formeln, die keine Funktionszeichen und keine mehrstellige Prädikatszeichen enthalten) wieder genau die endlichen und die koendlichen Mengen - ein Resultat, das auch auf (Löwenheim 1915) zurückgeht. Der Beweis dieser Behauptung beruht auf einem sogenannten Quantoreneliminationsverfahren und kann z.B. in (Ackermann 1954) gefunden werden. Gewisse Spektren können aber mit monadischen Formeln dargestellt werden, die viel kürzer als jede zugehörige Gleichheitsformel sind: Das Spektrum der Formel f_k:

$$(\forall v_o)(\forall v_1)(v_o=v_1 \vee (\bigvee_{o\leq i<k}(p_i^1(v_o)\wedge\neg p_i^1(v_1))\vee\bigvee_{o\leq i<k}(\neg p_i^1(v_o)\wedge p_i^1(v_1))))$$

besteht aus allen Zahlen, die kleiner oder gleich 2^k sind; eine Gleichheitsformel mit diesem Spektrum hat aber eine Länge grösser als 2^k; die Länge der Formeln f_k wächst dagegen nur linear mit k.

Sobald ein einziges 1-stelliges Funktionszeichen oder ein einziges 2-stelliges Prädikatszeichen in einer Formel enthalten ist, so kann das Spektrum der Formel schon unendlich sein und unendliches Komplement haben. Das Spektrum von

$$(\forall v_o)(f_o^1(v_o)\neq v_o\wedge f_o^1(f_o^1(v_o))=v_o)$$

besteht genau aus den geraden Zahlen. Nun kann eine Funktion immer durch ihren Graphen dargestellt werden: So hat zum Beispiel die Konjunktion der drei Formeln

$$(\forall v_o)(\exists v_1)p_o^2(v_o,v_1)$$

$$(\forall v_o)(\forall v_1)(\forall v_2)(\neg(p_o^2(v_o,v_1)\wedge p_o^2(v_o,v_2))\vee v_1=v_2)$$

$$(\forall v_o)(\neg p_o^2(v_o,v_o)\wedge(\exists v_1)(p_o^2(v_o,v_1)\wedge p_o^2(v_1,v_o)))$$

dasselbe Spektrum wie die obige Formel. In dieser Weise kann man übrigens jeder Formel eine neue Formel mit demselben Spektrum zuordnen, welche keine Funktionszeichen enthält.

Nebenbei sei auch bemerkt, dass es Formeln mit einem einzigen 1-stelligen Funktionszeichen bzw. 2-stelligen Prädikatszeichen gibt, die erst abzählbar erfüllbar sind - was bei monadischen Formeln nicht der Fall ist. Solche sind zum Beispiel

$$(\exists v_o)(\forall v_1)(\forall v_2)((f_o^1(v_1)\neq v_o\wedge f_o^1(v_1)\neq v_1)\wedge(f_o^1(v_1)\neq f_o^1(v_2)\vee v_1=v_2))$$

und

$$(\forall v_o)(\exists v_1)(\forall v_2)((\neg p_o^2(v_o,v_o)\wedge p_o^2(v_o,v_1))\wedge(\neg p_o^2(v_1,v_2)\vee p_o^2(v_o,v_2)))$$

Wie leicht einzusehen ist, sind die Spektren von existentiellen (bzw. abgeschlossenen universellen) pränexen Formeln, die keine Funktions-

zeichen enthalten, Reststücke (bzw. Anfangsstücke) der Menge der positiven Zahlen; die angegebenen Beispiele von Gleichheitsformeln zeigen, dass alle Rest- und Anfangsstücke vorkommen. Ebenfalls sind die Spektren von pränexen Formeln ohne Funktionszeichen, in welchen die Existentialquantoren sämtlichen Universalquantoren vorangehen (wie in $(\exists v_0)(\forall v_1)v_1=v_0$) genau die endlichen und koendlichen Mengen.
Dagegen lässt sich aber beweisen, dass jedes Spektrum das Spektrum einer pränexen Formel (erster Stufe) ohne Funktionszeichen ist, in welcher die Universalquantoren sämtlichen Existentialquantoren vorangehen (Skolemsche Normalform bez. Erfüllbarkeit). Dies entspricht der aussagenlogischen Reduktion auf die konjunktive Normalform in II: Jedes Modell der Formel

$$(\forall v_0)(\exists v_1)(\forall v_2)p_0^3(v_0,v_1,v_2)$$

lässt sich zu einem Modell der Formel

$$(\forall v_0)(\forall v_1)(\forall v_2)(\exists v_3)((\neg p_1^2(v_0,v_1)\vee p_0^3(v_0,v_1,v_2))\wedge p_1^2(v_0,v_3))$$

erweitern, und jedes Modell der zweiten Formel induziert ein Modell der ersten Formel. Sind Funktionszeichen zugelassen, so darf man sich entsprechend auf universelle pränexe Formeln einschränken: Das Spektrum von

$$(\forall v_0)(\forall v_1)\ p_0^3(v_0,f_0^1(v_0),v_1)$$

ist dasselbe wie dasjenige der obigen Formel.

In den nachfolgenden Beispielen werden Anfangsstücke von arithmetischen Relationen in einem gewissen Sinne durch Formeln dargestellt. Um die Formulierung zu vereinfachen, werden jetzt sogenannte geordnete Modelle betrachtet: Ein geordnetes Modell von f ist ein Modell, dessen Trägermenge ein Anfangsstück von $\mathbb{N}$ - d.h. eine Menge $\{0,1,\ldots,n\}$ - ist und bei dem das Prädikatszeichen p_0^2 durch $<$ interpretiert wird.
Falls das Zeichen p_0^2 nicht in f vorkommt, so ist die letztere Bedingung leer. Somit gibt es zu jedem Spektrum S eine Formel, welche genau dann ein n-zahliges geordnetes Modell besitzt, wenn n zu S gehört.
Hiervon gilt auch die Umkehrung: Sei f eine Formel und T die Menge derjenigen n, zu denen es ein n-zahliges geordnetes Modell gibt; dann ist T ein Spektrum.
Es sei nämlich f' die Konjunktion von f und einer Formel, welche ausdrückt, dass p_0^2 eine Ordnungsrelation ist. Dann ist einmal jedes geordnete Modell von f auch ein Modell von f'; umgekehrt ist jedes endliche Modell von f' isomorph einem endlichen geordneten Modell von f' und

somit auch einem endlichen Modell von f.

Definition Die arithmetische Relation R wird durch die Formel f dargestellt, wenn folgende Bedingungen erfüllt sind:

(1) Zu jeder positiven ganzen Zahl n gibt es ein n-zahliges geordnetes Modell von f.

(2) Es gibt ein Prädikatszeichen p_i^s, dessen Interpretation in jedem endlichen geordneten Modell $\langle M,I\rangle$ von f mit der Einschränkung von R auf M übereinstimmt.

Lemma Der Graph der Funktion a, welche durch das Rekursionsschema

$$\begin{cases} a(o,y,z) = z+1 \\ a(x+1,y,o) = y \\ a(x+1,y,z+1) = a(x,y,a(x+1,y,z)) \end{cases}$$

definiert wird, wird durch eine Formel erster Stufe dargestellt.

Beweis f sei die Konjunktion folgender Formeln (dabei ist $(f_1 \leftrightarrow f_2)$ eine Abkürzung von $(\neg f_1 \vee f_2) \wedge (f_1 \vee \neg f_2)$):

(1) $(\forall v_o) \neg p_o^2(v_o,v_o)$

(2) $(\forall v_o)(\forall v_1)(v_o = v_1 \vee (p_o^2(v_o,v_1) \vee p_o^2(v_1,v_o)))$

(3) $(\forall v_o)(\forall v_1)(\forall v_2)(\neg (p_o^2(v_o,v_1) \wedge p_o^2(v_1,v_2)) \vee p_o^2(v_o,v_2))$

(4) $(\exists v_o) p_1^1(v_o)$

(5) $(\forall v_o)(\forall v_1)(\neg p_1^1(v_o) \vee \neg p_o^2(v_1,v_o))$

(6) $(\forall v_o)(\forall v_1)(\neg p_2^2(v_o,v_1) \vee p_o^2(v_o,v_1))$

(7) $(\forall v_o)(\forall v_1)(\forall v_2)(\neg p_2^2(v_o,v_1) \vee (\neg p_o^2(v_o,v_2) \vee \neg p_o^2(v_2,v_1)))$

(8) $(\forall v_o)(\exists v_1)(p_1^1(v_o) \vee p_2^2(v_1,v_o))$

(9) $(\forall v_o)(\forall v_1)(\forall v_2)(\forall v_3)(\neg p_1^1(v_o) \vee (p_2^2(v_2,v_3) \longleftrightarrow p_3^4(v_o,v_1,v_2,v_3)))$

(10) $(\forall v_o)(\forall v_1)(\forall v_2)(\forall v_3)((\neg p_1^1(v_2) \vee p_1^1(v_o)) \vee (p_3^4(v_o,v_1,v_2,v_3) \longleftrightarrow v_3 = v_1))$

(11) $(\forall v_o)(\forall v_1)(\forall v_2)(\forall v_3)(\forall v_4)(\forall v_5)((\neg p_2^2(v_4,v_2) \vee \neg p_2^2(v_5,v_o)) \vee$
$(p_3^4(v_o,v_1,v_2,v_3) \longleftrightarrow (\exists v_6)(p_3^4(v_o,v_1,v_4,v_6) \wedge p_3^4(v_5,v_1,v_6,v_3))))$

Es lässt sich sofort prüfen, dass für jedes $n \in \mathbb{N}$ die Formel f erfüllt wird, falls die Zeichen p_o^2, p_1^1, p_2^2 und p_3^4 durch die Einschränkungen der Kleinerrelation, der charakteristischen Relation von 0, der Nachfolgerrelation und des Graphen der Funktion a auf $n+1 = \{0,1,\ldots,n\}$ interpre-

tiert werden.
Sei weiter <M,I> ein geordnetes endliches Modell von f, d.h. M ist ein Anfangsstück von $\mathbb{N}$, und $I(p_o^2)$ stimmt mit der Einschränkung von < auf M überein. Mit Induktion lässt sich dann aus (4) und (5), bzw. (6)-(8), (9)-(11) beweisen, dass $I(p_1^1)$ mit der Relation $\lambda x \cdot x=o$ auf M, bzw. $I(p_2^2)$ mit der Einschränkung der Nachfolgerrelation $\lambda xy \cdot y=x+1$ auf M und (da a monoton ist im 3. Argument) $I(p_3^4)$ mit der Einschränkung des Graphen der Funktion a auf M übereinstimmt.
Mit dem Graphen der Funktion a wird auch der Graph der Funktion $\lambda x \cdot a(x,x,x)$ durch eine Formel dargestellt. Um dies zu sehen, fügen wir ein Prädikatszeichen p_3^2 und das weitere Konjunktionsglied

$$p_3^2(x_o,x_1) \longleftrightarrow p_3^4(x_o,x_o,x_o,x_1)$$

hinzu.

Hilfssatz Der Graph der Funktion d werde durch eine Formel f dargestellt; dann bilden die Werte von d+1 ein Spektrum.

Beweis Die Funktion d sei etwa zweistellig und es sei p_3^3 das Prädikatszeichen der Darstellung. Es sei dann f' die Konjunktion von f und der Formel

$$(\exists v_o)(\exists v_1)\,(\exists v_2)(p_3^3(v_o,v_1,v_2) \wedge \neg\,(\exists v_3)\; p_o^2(v_2,v_3)).$$

Ist dann M ein geordnetes Modell von f' mit der Trägermenge {0,...,n}, so ist n ein Funktionswert von d und (n+1) ist die Mächtigkeit von M. Umgekehrt gibt es zu jedem n, das Funktionswert von d ist, auch ein geordnetes Modell mit der Trägermenge {0,...,n}. Da, wie gezeigt, die Menge der Zahlen m, zu denen es ein geordnetes Modell mit m Elementen gibt, ein Spektrum ist, so folgt die Behauptung.

Aus Lemma und Hilfssatz folgt nun unmittelbar
Satz 1 Die Werte der Funktion $\lambda x \cdot a(x,x,x)+1$ bilden ein Spektrum.

Korollar Es gibt ein Spektrum, dessen Aufzählungsfunktion schliesslich stärker als jede primitiv-rekursive Funktion wächst.

Beweis Das lässt sich wie in (Ackermann 1928) beweisen.

Das nächste Beispiel ist allgemeiner Natur:
Definition Die Klasse der konstruktiv-arithmetischen Relationen ist die kleinste Klasse, welche die Additions- und die Multiplikationsrela-

tion enthält, und welche gegenüber Booleschen Operationen, beschränkten Quantifikationen und expliziten Transformationen (d.h. Variablenidentifikation und -vertauschung, sowie Substitution von Konstanten) abgeschlossen ist.
(Diese Definition stammt aus (Smullyan 1961). Für Beispiele sei auf diese Arbeit verwiesen.)

Satz 2 Jede konstruktiv-arithmetische Relation ist durch eine Formel erster Stufe darstellbar.

Beweis Dem induktiven Charakter der obigen Definition entsprechend wird der Beweis durch Induktion über den Aufbau der Relationen geführt.
(1) Die Relationen $\lambda x \cdot x=o$ und $\lambda xy \cdot y=x+1$ werden durch die Formeln (1)-(8) des früheren Lemmas dargestellt. Folglich wird die Additionsrelation dargestellt durch die Konjunktion von (1)-(8) und der beiden Formeln:

*) $(\forall v_o)(\forall v_1)(\forall v_2)(\neg p_1^1(v_1) \vee (p_3^3(v_o,v_1,v_2) \longleftrightarrow v_o=v_2))$

**) $(\forall v_o)(\forall v_1)(\forall v_2)(\forall v_3)(\neg p_2^2(v_3,v_1) \vee$
$(p_3^3(v_o,v_1,v_2) \longleftrightarrow (\exists v_4)(p_3^3(v_o,v_3,v_4) \wedge p_2^2(v_4,v_2))))$.

(2) Analog wird die Multiplikationsrelation dargestellt durch die Konjunktion von (1)-(8), *), **) und der beiden Formeln:

$(\forall v_o)(\forall v_1)(\forall v_2)(\neg p_1^1(v_1) \vee (p_4^3(v_o,v_1,v_2) \longleftrightarrow p_1^1(v_2)))$

$(\forall v_o)(\forall v_1)(\forall v_2)(\forall v_3)(\neg p_2^2(v_3,v_1) \vee$
$(p_4^3(v_o,v_1,v_2) \longleftrightarrow (\exists v_4)(p_4^3(v_o,v_3,v_4) \wedge p_3^3(v_o,v_4,v_2))))$

(3) R entstehe aus R' durch Variablenvertauschung und Variablenidentifikation:
$R = \lambda x_o \ldots x_{s-1} \cdot R'(x_{\pi(o)},\ldots,x_{\pi(s'-1)})$, wobei π eine Abbildung von s' in s ist. R' sei durch f mit $p_k^{s'}$ dargestellt, und f enthalte das Zeichen p_k^s nicht. Dann wird R durch die Konjunktion von f mit
$(\forall v_o)\ldots(\forall v_{s-1})(p_k^s(v_o,\ldots,v_{s-1}) \longleftrightarrow p_k^{s'}(v_{\pi(o)},\ldots,v_{\pi(s'-1)})$ dargestellt.

(4) Da die Relation $\lambda x \cdot x=o$ und die Nachfolgerrelation darstellbar sind, so auch für jedes $n \in \mathbb{N}$ die Relation $\lambda x \cdot x=n$. Sei diese Relation durch die Formel f_1 (mit $p_{k'}^1$) dargestellt, und sei R' durch f_2 (mit $p_{k''}^{s+1}$) dargestellt; weiter sei das Zeichen p_k^s weder in f_1 noch in f_2 enthalten. Dann wird die Relation
$R = \lambda x_o \ldots x_{s-1} \cdot R'(x_o,\ldots,x_{s-1},n)$ durch die Konjunktion von f_1, f_2 und

$(\forall v_0)\ldots(\forall v_{s-1})(p^s_k(v_0,\ldots,v_{s-1}) \longleftrightarrow (\exists v_s)(p^{s+1}_{k''}(v_0,\ldots,v_s) \wedge p^1_{k'}(v_s)))$

dargestellt, sofern nur Modelle der Mächtigkeit grösser als n betrachtet werden. Die endlich vielen anderen Fälle lassen sich aber gesondert behandeln.

(5) Ist R eine Boolesche Verknüpfung darstellbarer Formeln, so ist sie klarerweise auch darstellbar.

(6) R' sei durch f (mit $p^s_{k'}$) dargestellt, und f enthalte das Zeichen p^s_k nicht. Die Relation $R_1 = \lambda x_0\ldots x_{s-1}\cdot(\exists x_s<x_{s-1})R'(x_0,\ldots,x_{s-2},x_s)$ wird durch die Konjunktion von f und
$(\forall v_0)\ldots(\forall v_{s-1})(p^s_k(v_0,\ldots,v_{s-1}) \longleftrightarrow (\exists v_s)(p^2_0(v_s,v_{s-1}) \wedge p^s_{k'}(v_0,\ldots,v_{s-2},v_s)))$ dargestellt, und die Relation
$R_2 = \lambda x_0\ldots x_{s-1}\cdot(\forall x_s<x_{s-1})R'(x_0,\ldots,x_{s-2},x_s)$ analog durch die Konjunktion von f und
$(\forall v_0)\ldots(\forall v_{s-1})(p^s_k(v_0,\ldots,v_{s-1}) \longleftrightarrow (\forall v_s)(\neg p^2_0(v_s,v_{s-1}) \vee p^s_{k'}(v_0,\ldots,v_{s-2},v_s)))$.

Korollar 2.1 Jede konstruktiv arithmetische Menge von positiven Zahlen ist ein Spektrum.

Beweis Die Menge $M' = \{n \mid n+1 \in M\}$ ist genau dann konstruktiv arithmetisch, wenn M konstruktiv arithmetisch ist. M' sei durch f mit p^1_k dargestellt. Das Spektrum von
$(f \wedge (\exists v_0)(p^1_k(v_0) \wedge (\forall v_1)\neg p^2_0(v_0,v_1)))$ ist dann M.

Korollar 2.2 $\{f \mid$ Spektrum $(f) \neq \emptyset\}$ hat den maximalen Unentscheidbarkeitsgrad unter den rekursiv aufzählbaren Mengen.

Beweis Nach (Smullyan 1961, Theorem 8, Seite 89) gibt es eine konstruktiv arithmetische Relation M derart, dass es für jede rekursiv aufzählbare Menge E ein $i \in \mathbb{N}$ gibt mit $E = E_i$, wobei

$$x \in E_i \iff (\exists y)M(i,x,y);$$

weiter gilt $$M(i,x,y) \Longrightarrow i<y \wedge x<y.$$

f' stelle M mit p^3_k dar, und f'_i stelle $\lambda x\cdot x=i$ mit $p^1_{k'}$ dar. Sei f_i die Formel

$$(\exists v_0)(\exists v_1)(\exists v_2)(((f'_i \wedge p^1_{k'}(v_0)) \wedge (f' \wedge p^3_k(v_0,v_1,v_2))) \wedge ((\forall v_3)\neg p^2_0(v_2,v_3) \wedge p^1_1(v_1))).$$

Die Menge $\{i|\ 0\in E_i\}$, welche maximalen Unentscheidbarkeitsgrad unter den rekursiv aufzählbaren Mengen hat, ist dann auf Grund der Zuordnung $i \mapsto f_i$ 1-1 reduzibel auf $\{f|\ \text{Spektrum}(f) \neq \emptyset\}$. Da die Relation $\lambda x f \cdot x \in \text{Spektrum}(f)$ rekursiv ist, so ist die erwähnte Menge rekursiv aufzählbar, und damit ist alles bewiesen.

Korollar 2.3 $\{f|\ \text{Spektrum}(f)$ unendlich$\}$ hat den maximalen Unentscheidbarkeitsgrad unter den $\Pi\Sigma$-Mengen.

Beweis Analog; $p_1^1(v_1)$ durch $(\forall v_3)(\neg p_o^2(v_3,v_2) \vee \neg p_k^3(v_o,v_1,v_3))$ ersetzen.

Korollar 2.4 Für jede rekursive Funktion gibt es ein Spektrum, dessen Aufzählungsfunktion stärker als diese Funktion wächst.

Beweis Nach (Smullyan 1961, Theorem 9, Seite 91) gibt es konstruktiv arithmetische Relationen T und U derart, dass es für jede rekursive Funktion f ein $i\in\mathbb{N}$ gibt mit $z = f(x) \Longleftrightarrow U(\mu y T(i,x,y),z)$; weiter gelten $U(y,z) \Longrightarrow y>z$ und $T(i,x,y) \Longrightarrow y>i \wedge y>x$. Der Rest verläuft analog.

3. Spektren und Turingmaschinen

Durch die dyadische Kodierung - welche der Zahl 0 das leere Wort $\emptyset$ und der Zahl $n = \sum_{j=o}^{m} n_j 2^j$ $(n_j \in \{1,2\})$ das Wort $\overline{n} = b_{n_o} \ldots b_{n_m}$ zuordnet, und somit eine bijektive Abbildung von $\mathbb{N}$ auf $\{b_1,b_2\}^*$ ist - lässt sich jede Klassifizierung der Teilmengen von $\{b_1,b_2\}^*$ auf die Teilmengen von $\mathbb{N}$ kanonisch erweitern. Insbesondere wird schlechthin gesagt, eine Teilmenge M von $\mathbb{N}$ liege in P, falls die Menge $\overline{M} = \{\overline{n}|\ n\in M\}$ in P liegt.

Wie in der Einführung angekündigt, wird in diesem Paragraphen bewiesen, dass die Spektren erster Stufe mit denjenigen Mengen M von positiven Zahlen übereinstimmen, welche schliesslich exponentiell berechenbar sind, d.h. für welche es ein $c\in\mathbb{N}$ und eine schliesslich $\lambda x \cdot 2^{cx}$-beschränkte nicht -deterministische NTM gibt, welche M akzeptiert. Dieser Satz ist aequivalent mit dem Satz - welcher etwas einfacher zu beweisen ist -, dass die Spektren genau diejenigen Mengen M sind, für welche die Menge $M_1 = \{b_1^{(n+1)}|\ n+1\in M\}$ in NP liegt, (wobei $b_1^{(n+1)} = \underbrace{b_1 \ldots b_1}_{n+1}$).

Zunächst wird der Beweis der trivialeren Richtung skizziert:

Satz 3 Für jedes Spektrum erster Stufe M liegt die Menge M_1 in NP.

Beweis M sei das Spektrum der (o.E.d.A.) pränexen Formel f, welche p Prädikatszeichen mit Stellenzahl kleiner oder gleich r enthält. Die Zugehörigkeit von n+1 zu M wird am direktesten mit einer NTM T auf $\sum_o = \{b_o, b_1, b_2\}$ mit mehreren r-dimensionalen Bändern getestet, welche folgendermassen operiert:
Der Input befinde sich auf dem nullten Band. T bewertet zuerst nichtdeterministisch auf den Bändern 1 bis p die p Prädikatszeichen von f in einem (n+1)-elementigen Bereich. Dies erfordert natürlich nur eine polynomiale Schrittzahl.
T bewertet dann die Formel, indem sie sukzessiv alle Bewertungsmöglichkeiten der Variablen probiert und ihrer Quantifikation entsprechend reagiert; die Bewertung einer Variablen kann in der Form eines Wortes der Länge kleiner als n+1 auf einem weiteren Band memoriert werden. Für die Auswertung einer Atomformel werden somit für ein passendes c_1 höchstens $c_1 \cdot (n+2)$ Schritte benötigt, und für die Auswertung der Matrix von f also höchstens $c_2 \cdot (n+2)$ Schritte für ein passendes c_2. Besteht das Präfix von f aus q Variablen, so sind höchstens $(n+2)^q$ Bewertungsversuche nötig. Die Schrittzahl von T ist also polynomial beschränkt.

Nach den Reduktionssätzen des ersten Vortrags hängt aber NP nicht vom benützten Maschinentypus ab: Somit ist der Satz bewiesen.

Die im Beweis der anderen Richtung benützte Methode ist derjenigen vom vorigen Paragraphen sehr ähnlich: Die Berechnungen einer NTM werden in einem endlichen - jetzt $(n+1)^k$-elementigen - Bereich dargestellt. Der Leser wird wohl auch einen Zusammenhang mit dem Beweis des Satzes von Cook (im zweiten Vortrag) erkennen: Die dort angegebenen aussagenlogischen Formeln sind (im wesentlichen!) die (n+1)-Redukte der jetzt angegebenen Formel.

Satz 4 Für jede Menge M_1 aus NP ist die Menge $M = \{n+1 \mid b_1^{(n+1)} \in M_1\}$ ein Spektrum erster Stufe.

Beweis M_1 liege in NP. Nach Voraussetzung wird M_1 durch eine schliesslich polynomial-beschränkte NTM T akzeptiert. O.E.d.A. sei $T = \langle S, s_o, s_1, R\rangle$ mit $S = \{s_o, s_1, \ldots, s_{q-1}\}$ eine NTM auf $\sum_o$, welche schliesslich $\lambda x \cdot (x+1)^r - (x+1)$-beschränkt ist. Weiter sei
$\overline{R} = R \cup \{\langle b, s_i, b, s_i\rangle \mid \neg (\exists a)(\exists j)\ (\langle b, s_i, a, s_j\rangle \in R)\}$ und
$\overline{T} = \langle S, s_o, s_1, \overline{R}\rangle$.

Der Lesbarkeit halber wurden in den folgenden Formeln die Prädikatszeichen mit K, A, N, F, L, B_j $(0\leq j\leq 2)$ und $S_j (0\leq j<q)$ bezeichnet; t, u, v, w bezeichnen r-Tupel von Variablen. $(f_1 \wedge f_2 \wedge \ldots \wedge f_k)$ ist eine Abkürzung von $((\ldots(f_1 \wedge f_2)\wedge\ldots)\wedge f_k)$, $(f_1 \vee f_2 \vee \ldots \vee f_k)$ eine Abkürzung von $((\ldots(f_1 \vee f_2)\vee\ldots)\vee f_k)$ und $(f_1 \wedge \ldots \wedge f_k \rightarrow f_{k+1} \vee \ldots \vee f_{k+j})$ eine Abkürzung von $(\neg (f_1 \wedge \ldots \wedge f_k) \vee (f_{k+1} \vee \ldots \vee f_{k+j}))$; weiter ist u=v eine Abkürzung von $(u_0=v_0 \wedge \ldots \wedge u_{r-1}=v_{r-1})$, wobei u_j die j-te Komponente des r-Tupels u bezeichnet.

f sei die Konjunktion der folgenden 24 Formeln:

(1) $(\forall u)\neg K(u,u)$

(2) $(\forall u)(\forall v)(K(u,v) \vee K(v,u) \vee u=v)$

(3) $(\forall u)(\forall v)(\forall w)(K(u,v) \wedge K(v,w) \rightarrow K(u,w))$

(4) $(\exists u)\, A(u)$

(5) $(\forall u)(\forall v)(A(u) \rightarrow \neg K(v,u))$

(6) $(\forall u)(\forall v)(N(u,v) \rightarrow K(u,v))$

(7) $(\forall u)(\forall v)(\forall w)(N(u,v) \rightarrow \neg K(u,w) \vee \neg K(w,v))$

(8) $(\forall u)(\exists v)(A(u) \vee N(v,u))$

(9) $(\forall v_0)(\exists u)\, F(v_0,u)$

(10) $(\forall v_0)(\forall v_1)(\forall u)(F(v_0,u) \wedge F(v_1,u) \rightarrow v_0=v_1)$

(11) $(\forall v_0)(\forall u)(\forall v)(F(v_0,u) \wedge F(v_0,v) \rightarrow u=v)$

(12) $(\forall v_0)(\forall v_1)(\forall u)(\forall v)(\forall w)(\exists v_2)$
$(F(v_0,u) \wedge F(v_1,v) \wedge K(u,w) \wedge K(w,v) \rightarrow F(v_2,w))$

(13) $(\forall u) \bigvee_{0\leq j<q} S_j(u)$

(14) $(\forall u) \bigwedge_{0\leq j<k<q} (\neg S_j(u) \vee \neg S_k(u))$

(15) $(\forall u)(\exists v)L(u,v)$

(16) $(\forall u)(\forall v)(\forall w)(L(u,v) \wedge L(u,w) \rightarrow v=w)$

(17) $(\forall u)(\forall v) \bigvee_{0\leq j\leq 2} B_j(u,v)$

(18) $(\forall u)(\forall v) \bigwedge_{0\leq j<k\leq 2} (\neg B_j(u,v) \vee \neg B_k(u,v))$

(19) $(\forall u)(\exists v)(\forall w)(A(u) \rightarrow (S_0(u) \wedge L(u,v) \wedge (\exists v_0)F(v_0,v)$
$\wedge (K(w,v) \rightarrow \neg (\exists v_0)F(v_0,w)))$

(20) $(\forall u)(\forall v)(A(u) \wedge (\exists v_0)F(v_0,v) \rightarrow B_1(u,v))$

(21) $(\forall u)(\forall v)(A(u) \wedge \neg (\exists v_0)F(v_0,v) \rightarrow B_0(u,v))$

(22) $(\forall u)(\forall v)(\forall w)(N(u,v) \wedge \neg L(u,w) \rightarrow \bigwedge_{0 \leq j \leq 2} (B_j(u,w) \rightarrow B_j(v,w)))$

(23) $(\forall t)(\forall u)(\forall v)(\forall w)(L(u,w) \wedge L(v,t) \wedge N(u,v) \rightarrow$

$$\bigvee_{<b_k,s_i,R,s_j> \in \overline{R}} (S_i(u) \wedge S_j(v) \wedge B_k(u,w) \wedge B_k(v,w) \wedge N(w,t)) \vee$$

$$\bigvee_{<b_k,s_i,L,s_j> \in \overline{R}} (S_i(u) \wedge S_j(v) \wedge B_k(u,w) \wedge B_k(v,w) \wedge N(t,w)) \vee$$

$$\bigvee_{<b_k,s_i,b_\ell,s_j> \in \overline{R}} (S_i(u) \wedge S_j(v) \wedge B_k(u,w) \wedge t=w \wedge B_\ell(v,w)))$$

(24) $(\exists u)(S_1(u) \wedge (\forall v) \neg K(u,v))$

(a) Nach Definition gibt es ein $n_0 \in \mathbb{N}$ derart, dass es eine akzeptierende Berechnung von T der Länge kleiner als $(n+1)^r-(n+1)$ mit Input $b_1^{(n+1)}$ gibt, falls $n>n_0$ und $n+1 \in M$. Dies ist aber genau dann der Fall, wenn es eine Berechnung von $\overline{T}$ der Länge $(n+1)^r-1$ mit demselben Input gibt, deren letzte Konfiguration den Zustand s_1 enthält. Sei $<K_i>_{i \in (n+1)^r}$ mit $K_i = <<a^i_j>_{j \in \mathbb{Z}}, p^i, s^i>$ eine solche Berechnung.

Ein $(n+1)$-elementiges Modell $<M,I>$ von f kann jetzt folgendermassen definiert werden: $M = n+1 = \{0,1,\ldots,n\}$;

$I(K)$ sei die lexikographische Ordnung (bez. $<$) von M^r und $I(N)$ die entsprechende Nachfolgerrelation; $I(A)$ sei die charakteristische Relation von $<0,\ldots,0>$. Dadurch sind die Formeln (1)-(8) erfüllt.

Sei $-\ell$ die Nummer des am weitesten links gelegenen Feldes, welches im Laufe der Berechnung durch den Kopf erreicht wird; da die Länge der entsprechenden Berechnung von T kleiner ist als $(n+1)^r-(n+1)$, so ist auch ℓ kleiner als $(n+1)^r-(n+1)$.

$I(F)$ sei die injektive Abbildung von M nach M^r, welche dem Element i von M das $(\ell+i)$-te Element von M^r bezüglich der lexikographischen Ordnung zuordnet; dies ist auf Grund der obigen Bemerkung möglich. Dadurch sind auch die Formeln (9)-(12) erfüllt.

$I(S_i)$ sei genau dann vom j-ten Element von M^r (bez. der lexikographischen Ordnung) wahr, wenn $s^j = s_i$; $I(B_i)$ bzw. $I(L)$ sei genau dann von den j-ten und k-ten Elementen von M^r (bez. derselben Ordnung), wenn $a^j_{k+\ell} = b_i$ bzw. $p^{j+\ell} = k$. Auf Grund der obigen Bemerkung sind dann die Formeln (13)-(18) automatisch erfüllt. (19)-(21) sind erfüllt, weil die Berechnung $<K_i>_{i \in (n+1)^r}$ den Input $b_1^{(n+1)}$ hat, und (22)-(23), weil K_{i+1} Folgekonfiguration von K_i ist. Endlich ist (24) erfüllt, weil $\overline{T}$ zum Zustand s_1 gelangt.

Somit liegt n+1 im Spektrum von f, falls $n>n_0$ und $n+1 \in M$.

(b) Umgekehrt gehöre n+1 zum Spektrum von f. Dann gibt es ein Modell $\langle M,I\rangle$ von f mit (n+1)-elementigem M. Wegen (1)-(3) ist I(K) eine totale Ordnung von M^r; wegen (4)-(5) gilt I(A) nur für deren erstes Element; wegen (6)-(8) ist I(N) die Nachfolgerelation bezüglich I(K); schliesslich ist wegen (9)-(12) I(F) eine bijektive Abbildung von M auf ein Segment von M^r bezüglich I(K).
Sei $m_0,m_1,\ldots,m_{(n+1)^r-1}$ die durch I(K) geordnete Abzählung von M^r. Nach (13)-(14) gibt es zu jedem $j\in(n+1)^r$ genau ein i $(0\leq i<q)$ mit $I(S_i)(m_j)$ und nach (15)-(16) genau ein $k\in(n+1)^r$ mit $I(L)(m_j,m_k)$, sowie zu jedem $j,k\in(n+1)^r$ genau ein i $(0\leq i<2)$ mit $I(B_i)(m_j,m_k)$. Sei weiter ℓ die kleinste Zahl mit $m_\ell \in I(F)(M)$.

Nun sei für $i\in(n+1)^r$ $K_i = \langle\langle a^i_j\rangle_{j\in\mathbb{Z}},p^i,s^i\rangle$ durch folgende Gleichungen definiert:

$$a^i_j = \begin{cases} b_k \text{ falls } I(B_k)(m_i,m_{j+\ell}) \\ \quad \text{und } -\ell\leq j<(n+1)^r-\ell, \\ b_0 \text{ sonst;} \end{cases}$$

$$p^i = j \quad \text{falls } I(L)(m_i,m_{j+\ell});$$

$$s^i = s_j \quad \text{falls } I(S_j)(m_i);$$

dies ist auf Grund der vorigen Bemerkung eine vernünftige Definition.

Nach (19)-(21) gilt insbesondere:

$$a^0_j = \begin{cases} b_1 \text{ falls } 0\leq j\leq n, \\ b_0 \text{ sonst;} \end{cases}$$

$$p^0 = 0;$$

$$s^0 = s_0;$$

also ist K_0 die Konfiguration zum Input $b_1^{(n+1)}$. Nach (22) und (23) ist $\langle K_i\rangle_{i\in(n+1)^r}$ eine Berechnung von $\overline{T}$, und nach (24) gilt $s^{(n+1)^r-1} = s_1$. Dann ist aber $\langle K_i\rangle_{i\in h+1}$ eine akzeptierende Berechnung von T mit dem Input $b_1^{(n+1)}$, d.h. $b_1^{(n+1)}$ liegt in M_1; folglich liegt n+1 in M. $(h<(n+1)^r)$

(c) Somit ist gezeigt, dass oberhalb n_0 die Menge M mit dem Spektrum von f zusammenfällt. Daraus folgt leicht, dass auch M ein Spektrum ist: M ist nämlich das Spektrum der Formel $(f\wedge f_1)\vee f_2$, wobei f_1 die Gleichheitsformel ist, deren koendliches Spektrum aus den Zahlen grösser als n_0 besteht und f_2 die Gleichheitsformel ist, deren endliches Spektrum aus

den Zahlen kleiner oder gleich n_0 besteht, welche zu M gehören.

Korollar 4.1 Eine Menge M von positiven Zahlen ist genau dann ein Spektrum erster Stufe, wenn $M_1 = \{b_1^{(n+1)} \mid n+1 \in M\}$ in NP liegt.

Beweis Dies ist eine direkte Folgerung aus den Sätzen 3 und 4.

Korollar 4.2 Eine Menge M von positiven Zahlen ist genau dann ein Spektrum erster Stufe, wenn es eine schliesslich exponentiell-beschränkte (d.h. durch $\lambda x \cdot 2^{cx}$ für ein c) nicht-deterministische NTM gibt, welche $\overline{M} = \{\overline{n+1} \mid n+1 \in M\}$ akzeptiert.

Beweis Da $lh(\overline{n+1}) = \lfloor \log_2(n+2) \rfloor$ gilt

$$2^{c\,lh(\overline{n+1})} \leq (n+2)^c < 2^{c(1+lh(\overline{n+1}))} \leq 2^{2c\,lh(\overline{n+1})} ;$$

eine Funktion ist also genau dann polynomial in $n+1 = lh(b_1^{(n+1)})$, wenn sie exponentiell in $lh(\overline{n+1})$ ist.

Weiter ist die Zuordnung $\overline{n+1} \mapsto b_1^{(n+1)}$ (durch wiederholtes Verdoppeln) in exponentieller Zeit berechenbar auf einer mehrköpfigen TM; ebenfalls ist die Zuordnung $b_1^{(n+1)} \mapsto (\overline{n+1})$ (durch wiederholtes Halbieren) in der Zeit $c(n+1)$ für ein passendes c auf einer mehrköpfigen TM berechenbar, also in Π.

Folglich gibt es genau dann eine schliesslich exponentiell-beschränkte NTM, welche $\overline{M}$ akzeptiert, wenn es eine schliesslich polynomial-beschränkte NTM gibt, welche M_1 akzeptiert.

Analog lassen sich die beiden nächsten Korollare beweisen:

Korollar 4.3 Ist NP = P, so sind die Spektren erster Stufe genau die Mengen von positiven Zahlen, welche durch schliesslich exponentiell-beschränkte deterministische TM akzeptiert werden.

Korollar 4.4 Ist NP gegenüber Komplementbildung abgeschlossen, so ist auch die Klasse der Spektren erster Stufe gegenüber Komplementbildung abgeschlossen.

Korollar 4.5 Ist $\overline{M}$ kontext-sensitiv, so sind beide Mengen $\{n+1 \mid \overline{n+1} \in \overline{M}\}$ und $\{n+1 \mid \overline{n+1} \notin \overline{M}\}$ Spektren erster Stufe.

Beweis Bekanntlich sind die kontext-sensitiven Mengen genau die Mengen, welche durch NTM akzeptiert werden, die mit linearem Raum operieren (Kuroda 1964 und Landweber 1963); diese Mengen sowie ihre Komplemente werden durch schliesslich exponentiell-beschränkte deterministische TM akzeptiert.

Korollar 4.6 Jede Menge, deren charakteristische Funktion in der Klasse $\mathfrak{E}^2$ von Grzegorczyk liegt, ist ein Spektrum erster Stufe.

Beweis Diese Mengen sind nämlich genau diejenigen, welche durch TM akzeptiert werden, die mit linearem Raum operieren (Ritchie 1963).

4. Projektive Klassen und NP

Gemäss Korollar 4.1 besteht eine direkte Verbindung zwischen den Spektren erster Stufe und den Mengen aus $\{b_1\}^*$, welche in NP liegen. Da man aber auf $\{b_1,b_2\}^*$ auch Teilmengen einer n-elementigen Menge mit Wörtern der Länge n darstellen kann, entsteht auf natürliche Weise die Frage, ob die Mengen aus NP nicht noch enger mit Modellklassen als mit Spektren im Zusammenhang stehen.

Der nicht-deterministische Charakter einer Berechnung entsprach im vorigen Paragraphen der Bewertung eines Prädikatszeichens: Also müssen wohl projektive Klassen (manchmal pseudo-elementare genannt) betrachtet werden. Wäre jede solche Klasse zugelassen, so wäre (wie bei den Spektren) jede Teilmenge der natürlichen Zahlen darstellbar. Deshalb werden nur endlich axiomatisierbare Klassen betrachtet; natürlich kommen für die Charakterisierung nur endliche Strukturen von endlichem Typus in Frage, d.h. Strukturen mit endlich vielen endlichstelligen Relationen (oder Funktionen) auf einem endlichen Träger.

Weil die Wörter aus $\{b_1,b_2\}^*$ Folgen sind, müssen bei der Darstellung die Permutationen des Trägers ausgeschaltet werden: Deshalb werden ausschliesslich geordnete Modelle betrachtet. Ist R eine s-stellige Relation einer n-elementigen geordneten Struktur, so ist ihre Kodierung das Wort w der Länge n^s mit der Eigenschaft:

$$R(i_1,\ldots,i_s) \longleftrightarrow (w)_{\sum_{k=1}^{s} i_k n^{k-1}} = b_2 \ ;$$

Funktionen können durch ihren Graphen dargestellt werden. Die Kodierung der Relationen $R_1,\ldots,R_k$ ist die Concatenation $w_1\ldots w_k$ der Kodierungen

$w_1,\ldots,w_k$ von $R_1,\ldots,R_k$.
Der folgende Satz entspricht dem Satz 3, und wird analog bewiesen:

Satz 5 Zu jeder Formel erster Stufe f mit den (unter anderen) Prädikatszeichen $p_{i_1}^{s_1},\ldots,p_{i_k}^{s_k}$ gibt es eine Menge L aus NP derart, dass die Kodierung von $I(p_{i_1}^{s_1}),\ldots,I(p_{i_k}^{s_k})$ genau dann in L liegt, wenn es ein Modell <M,I'> von f gibt, mit $I'(p_{i_1}^{s_1}) = I(p_{i_1}^{s_1}),..,I'(p_{i_k}^{s_k}) = I(p_{i_k}^{s_k})$.

Beweisskizze Zu f gibt es eine NTM T, welche folgendermassen operiert:

(1) Aus dem Input w der Länge lh(w) - welcher eventuell eine Kodierung von Relationen ist - wird zunächst n mit $\sum_{j=1}^{k} n^{s_j} = lh(w)$ berechnet. Dafür wird n nicht-deterministisch gewählt, $\sum_{j=1}^{k} n^{s_j}$ berechnet, und mit lh(w) verglichen. Sind beide Zahlen verschieden, so stellt T ab, sonst geht sie zu (2) über.

(2) Die Kodierungen der einzelnen Prädikate werden auf verschiedene Bänder gebracht.

(3) Die weiteren Prädikatszeichen von f werden nicht-deterministisch interpretiert.

(4) Schliesslich wird f auf Erfüllung durch die vorgeschlagene Interpretation getestet:

Für jede der vier Teilberechnungen (1)-(4) wird eine Schrittzahl benötigt, die in n polynomial ist. Da $lh(w) \geq n$ ist also T schliesslich polynomial-beschränkt.

Die Umkehrung wird mittels folgendem Analogon von Satz 4 erreicht:

Satz 6 Zu jeder Menge L aus NP gibt es eine Formel erster Stufe f mit den - unter anderen - Prädikatszeichen p_o^2, p_1^1, p_2^2, p_3^1 derart, dass das Wort $w \neq \emptyset$ genau dann zu L gehört, wenn es ein geordnetes endliches Modell <M,I> von f gibt, für welches gilt:

(1) $I(p_o^2) = (\lambda xy \cdot x<y)\restriction M$

(2) $I(p_1^1) = (\lambda x \cdot x=o)\restriction M$

(3) $I(p_2^2) = (\lambda xy \cdot y=x+1)\restriction M$

(4) $\overline{M} = lh(w)$

(5) Die Kodierung von $I(p_3^1)$ ist w.

Beweisskizze f' ist die Konjunktion der Formeln (1)-(8) des Lemmas auf Seite 10, der Formeln (1)-(9), (13)-(19) und (22)-(24) aus Satz 4 (Seiten 16-17) und der folgenden Formeln:

$$(10') \quad (\forall v_0)(\forall v_1)(\forall u)(\forall w)(F(v_0,u) \wedge F(v_1,w) \rightarrow (p_2^2(v_0,v_1) \leftrightarrow N(u,w)))$$

$$(20') \quad (\forall u)(\forall v)(A(u) \rightarrow (B_0(u,v) \leftrightarrow \neg (\exists v_0)F(v_0,v)))$$

$$(21') \quad (\forall u)(\forall v_0)(A(u) \rightarrow (p_3^1(v_0) \leftrightarrow (\exists v)(F(v_0,v) \wedge B_2(u,v))))$$

Dadurch wird erzwungen, dass der Input der Berechnung die Kodierung von $I(p_3^1)$ ist. Der Rest des Beweises verläuft ganz analog.

Korollar 6.1 Die Mengen von nicht-leeren Wörtern aus $\{b_1,b_2\}^*$, welche in NP liegen, sind genau die Kodierungsmengen der endlichen Strukturen der endlich axiomatisierbaren projektiven Klassen von endlichem Typus.

Beweis Unmittelbar aus Satz 5 und Satz 6.

Korollar 6.2 NP ist genau dann gegenüber Komplementbildung abgeschlossen, wenn es zu jeder endlich axiomatisierbaren projektiven Klasse K von endlichem Typus eine endlich axiomatisierbare projektive Klasse vom selben Typus gibt, deren endliche Strukturen genau diejenigen sind, die nicht in K liegen.

5. Ausblicke auf Spektren höherer Stufe

Das Spektrumproblem lässt sich für die Formeln höherer Stufe der Typentheorie ohne weiteres verallgemeinern - zumindest für natürliche Zahlen. Die Einschränkung auf $\mathbb{N}$ ist hier nicht in der gleichen Weise wie für die erste Stufe berechtigt, und vermeidet eher mengentheoretische Schwierigkeiten: Sind allgemeine Modelle zugelassen (d.h. Modelle, wo die Interpretation der Potenzmenge nicht die volle Potenzmenge zu sein braucht), so gelten zwar immer noch der Kompaktheitssatz und der Satz von Löwenheim; das ist nicht mehr der Fall, wenn nur Standardmodelle zugelassen sind. Leider ist aber dann die Klasse der gültigen Formeln nicht mehr rekursiv aufzählbar.

Der Darstellungssatz aus dem dritten Paragraphen lässt sich wie folgt verallgemeinern (vgl. Christen 1974): Sei $f_0 = \lambda x \cdot x$ und $f_{i+1} = \lambda x \cdot 2^{f_i(x)}$. Eine Menge von positiven Zahlen ist genau dann ein

Spektrum der (i+1)-ten Stufe, wenn es eine schliesslich $\lambda x \cdot f_{i+1}(cx)$-beschränkte nicht-deterministische Turingmaschine gibt, welche sie akzeptiert. Daraus folgt, dass die Klasse $\mathfrak{Y}_i^*$ von Rödding die Klasse der Relationen ist, die durch deterministische Turingmaschinen im Raum $\lambda x \cdot f_i(cx)$ akzeptiert werden, und dass die Mengen von positiven Zahlen aus $\mathfrak{Y}_i^*$ Spektren von (i+1)-ter Stufe sind (Rödding und Schwichtenberg 1972). Insbesondere sind die Spektren beliebiger Stufe genau die elementaren ($\mathcal{E}^3$) Mengen von positiven Zahlen (Bennett 1962). Weiter folgt auch, dass es zu jedem i ein Spektrum der (i+2)-ten Stufe gibt, das kein Spektrum der (i+1)-ten Stufe ist (Bennett 1962, in Christen 1974 vereinfacht).

Als weitere Folgerung des Darstellungssatzes lässt sich zeigen, dass es für jedes unendliche Spektrum der Typentheorie mit unendlichem Komplement eine polynomial entscheidbare Menge gibt, welche das Spektrum sowie sein Komplement in je zwei unendliche Mengen teilt (Christen 1974) (Analoges gilt für kontext-sensitive Mengen und Mengen aus NP). Für jedes $i \in \mathbb{N}$ ist also der Verband $\mathcal{S}_{i+1}/\mathcal{F}$ dicht, wobei $\mathcal{S}_{i+1}$ die Klasse der Spektren der (i+1)-ten Stufe und $\mathcal{F}$ die Klasse der endlichen Teilmengen von $\mathbb{N}$ ist; insbesondere gibt es weder minimale noch maximale Spektren einer gegebenen Stufe - noch minimale oder maximale Mengen aus NP.

Obwohl die Spektren höherer Stufe eine Hierarchie bilden, lassen sie sich alle als Urbilder von Spektren erster Stufe durch ganz einfache Funktionen darstellen: Eine Menge M ist genau dann ein Spektrum (i+1)-ter Stufe, falls es ein c und ein Spektrum erster Stufe M_1 derart gibt, dass $M = \{n \mid f_i(n^c) \in M_1\}$ (Bennett 1962). Sie sind ebenfalls Urbilder der Mengen aus NP durch die Funktionen $\lambda x \cdot f_{i+1}(x^c)$. Daraus folgt, dass für jedes $i \in \mathbb{N}$ die Klasse der Spektren (i+2)-ter Stufe gegenüber Komplementbildung abgeschlossen ist, falls die Klasse der Spektren (i+1)-ter Stufe gegenüber Komplementbildung abgeschlossen ist, und analog, dass die Spektren (i+2)-ter Stufe für $c \in \mathbb{N}$ deterministisch $\lambda x \cdot f_{i+2}(cx)$-berechenbar sind, falls die Spektren (i+1)-ter Stufe deterministisch $\lambda x \cdot f_{i+1}(cx)$ berechenbar sind. In analoger Weise lassen sich die Spektren der sogenannten "schwachen" (i+2)-ten Stufe (d.h. die Spektren von Formeln, welche eventuell gebundene Prädikatszeichen der (i+1)-ten Stufe, doch keine Prädikatszeichen der (i+2)-ten Stufe enthalten) als Urbilder (durch $\lambda x \cdot f_{i+1}(cx)$ für $c \in \mathbb{N}$) der konstruktiv arithmetischen Mengen darstellen (Bennett 1962), von (Rödding und Schwichtenberg 1972) unabhängig wiedergefunden).

Auf Grund dieser Eigenschaften ist die kombinatorische Komplexität der höheren Klassen in einem gewissen Sinne die gleiche wie diejenige der tieferen Klassen. Vielleicht ist ein Teil der Schwierigkeiten in der Komplexitätstheorie - wie z.B. der manchmal ungeheure Unterschied zwischen den bekannten oberen und unteren Komplexitätsschranken - auf ein derartiges Phänomen zurückzuführen.

Literatur

Ackermann, W., Ueber die Hilbertsche Definition der reellen Zahlen, Math. Ann. 99 (1928) 118-133.

Ackermann, W., Solvable Cases of the Decision Problem, North-Holland, Amsterdam 1954.

Asser, G., Das Repräsentantenproblem im Prädikatenkalkül der ersten Stufe mit Identität, Z. Math. Logik Grundlagen Math. 1 (1956) 252-263.

Bennett, J., On Spectra, Doctoral Dissertation, Princeton University, 1962 (Microfilm H01: 63-496).

Büchi, J.R., Turing Machines and the Entscheidungsproblem, Math. Ann. 148 (1962) 201-213.

Christen, C.A., Spektren und Klassen elementarer Funktionen, Dissertation 5330, ETH Zürich 1974.

Jones, N.D./Selman, A.L., Turing Machines and the Spectra of First-order Formulas, J. Symbolic Logic 39 (1974) 139-150.

Kuroda, S.Y., Classes of languages and linear-bounded automata, Information and Control 7 (1964) 207-223.

Landweber, P., Three theorems on phrase structure grammars of type 1, Information and Control 6 (1963) 131-137.

Löwenheim, L., Ueber Möglichkeiten im Relativkalkül, Math. Ann. 76 (1915) 137-148.

Pazderski, G., Die Ordnungen, zu denen nur Gruppen mit gegebener Eigenschaft gehören, Arch. Math. 10 (1959) 331-343.

Ritchie, R.W., Classes of predictably computable functions, Trans. AMS 106 (1963) 139-173.

Rödding, D./Schwichtenberg, H., Bemerkungen zum Spektralproblem, Z. Math. Logik Grundlagen Math. 18 (1972) 1-12.

Scholz, H., Ein ungelöstes Problem in der symbolischen Logik, J. Symbolic Logic 17 (1952) 160.

Smullyan, R., Theory of Formal Systems, Ann. of Math. Studies 47, Princeton 1961.

Trachtenbrot, B.A., Névozmojnost algorifma dla problemy razréšimosti na konécyh klassah (Unmöglichkeit eines Algorithmus für das Entscheidungsproblem in endlichen Klassen), Doklady Akad. Nauk SSSR 70 (1950) 569-572.