Einleitung

Eine Menge A von natürlichen Zahlen heisst "entscheidbar", wenn es ein Verfahren gibt, welches zu vorgelegtem a in $\mathbb{N}$ in endlich vielen Schritten entscheidet, ob $a \in A$ oder nicht.

Der Begriff eines Verfahrens kann bekanntlich auf verschiedene Arten mathematisch formuliert werden. Den folgenden Betrachtungen sei die von Turing vorgeschlagene maschinelle Definition zu Grunde gelegt. Diese hat unter anderem den Vorteil, dass sie die intuitive Vorstellung der zeitlichen Dauer des Entscheidungsverfahrens mit Hilfe der Schrittzahl in natürlicher Weise zu präzisieren gestattet.

Eine Menge A ist in polynomialer Zeit entscheidbar, gewenn (genau dann, wenn) es eine Turingmaschine e und ein Polynom p gibt mit folgenden Eigenschaften: Setzt man die Maschine e auf die binär kodierte Zahl a an und ist $\ell(a)$ die Stellenzahl von a, so kommt e nach höchstens $p(\ell(a))$ Schritten zum Stillstand, und e akzeptiert a gewenn $a \in A$. (Man erhält eine äquivalente und etwas kürzere, wenn auch weniger einleuchtende Definition durch die Forderung: $a \in A \iff$ e akzeptiert a in $p(\ell(a))$ Schritten. Hier können also auch Zahlen akzeptiert werden, die gar nicht zu A gehören.)

Analog zu der Klasse P der in polynomialer Zeit entscheidbaren Mengen wird die Klasse Π der in polynomialer Zeit berechenbaren Funktionen definiert.

Die Klasse P ist abgeschlossen gegenüber den Boole'schen Operationen Vereinigung, Durchschnitt und Komplement, die Klasse Π gegenüber Komposition. Mit A in P und f in Π ist auch $f^{-1}A$ in P.

Die Begriffe der in polynomialer Zeit entscheidbaren Mengen und berechenbaren Funktionen nehmen in der Komplexitätstheorie eine wichtige Stellung ein. Dies hängt einmal damit zusammen, dass sie weitgehend unabhängig sind vom speziellen Maschinenmodell. Läuft ein Algorithmus z.B. auf einer Mehrband-Mehrkopf Turingmaschine in polynomial beschränkter Zeit ab, so auch auf einer Einband-Einkopf Maschine. Ferner sind es unter den in der Literatur auftretenden Algorithmen im wesentlichen gerade die polynomial beschränkten, für welche der Einsatz elektronischer Rechenanlagen eine deutliche Erweiterung des Anwendungsbereiches ermöglicht.

Was nun Beispiele anbetrifft, so ergibt sich die Zugehörigkeit zu P für viele Mengen unmittelbar aus ihrer Definition: Menge der Kubikzahlen,

Menge der Zweierpotenzen, Menge der Fibonaccizahlen. Für andere Mengen folgt die Zugehörigkeit zu P erst auf Grund eines nicht-trivialen "Kriteriums". Ein Beispiel hierfür ist die Menge der Primzahlen der Form 2^n-1; die Eigenschaft, eine solche Mersenne'sche Primzahl zu sein, ist nach dem Kriterium von Lucas in polynomialer Zeit entscheidbar (Knuth 1969).

Für viele zahlentheoretisch interessante Mengen ist die Zugehörigkeit zu P offen. So ist zwar bekanntlich entscheidbar, ob eine Zahl a Primzahl ist oder nicht; es ist aber nicht bekannt, ob es dafür ein in $\ell(a)$ polynomial beschränktes Entscheidungsverfahren gibt. Weitere solche Mengen findet man unter den Wertebereichen von Polynomen in mehreren Variablen (mit Koeffizienten und Argumenten in $\mathbb{N}$). Ist z.B. D die Menge der Zahlen a der Form x^3+y^3, so ist D ersichtlicherweise entscheidbar. Das naheliegende Entscheidungsverfahren für $a \in D$, bei dem alle Tripel $\langle a,x,y\rangle$ mit $x \leq a$, $y \leq a$ auf $a = x^3+y^3$ getestet werden, ist aber von der Grössenordnung $a^{1/3}$, also exponentiell in $\ell(a)$. (Und es scheint überhaupt kein polynomial beschränktes Entscheidungsverfahren für D zu geben.)

Anhand der Menge D soll nun ein wichtiger neuer Begriff eingeführt werden. Man denke sich das oben angegebene Entscheidungsverfahren für eine Zahl a einmal durchgeführt. Je nach dem Ausgang befindet man sich in ganz verschiedenen Situationen. Ist der Test positiv ausgefallen, so liegt ein Tripel $\langle a,x,y\rangle$ mit $a = x^3+y^3$ vor. Der Besitz eines solchen Tripels ermöglicht aber schon den Nachweis für $a \in D$ in polynomialer Zeit, indem die Summe x^3+y^3 berechnet und mit a verglichen wird. Ist andererseits das Testergebnis negativ, so lässt sich aus der geleisteten Arbeit anscheinend kein kurzer Beweis für $a \notin D$ entnehmen. Dieser häufig auftretende Sachverhalt führt zu den folgenden Definitionen:

1. Die Turingmaschine e verifiziert a in m Schritten, gewenn es ein x gibt, so dass e den Input $\langle a,x\rangle$ in höchstens m Schritten akzeptiert.

Bemerkung. Trotz des Existenzquantors über x ist entscheidbar, ob e die Zahl a in m Schritten verifiziert. Denn in der Zeitspanne m liest die Maschine e höchstens m Stellen des Inputs $\langle a,x\rangle$. Gibt es also überhaupt ein x, für welches $\langle a,x\rangle$ akzeptiert wird, so auch eins mit der zusätzlichen Eigenschaft $\ell(x) \leq m$.

2. Eine Menge A ist in polynomialer Zeit verifizierbar, gewenn es eine Turingmaschine e und ein Polynom p gibt, so dass gilt:

$$a \in A \iff e \text{ verifiziert } a \text{ in } p(\ell(a)) \text{ Schritten.}$$

NP ist die Klasse der in polynomialer Zeit verifizierbaren Mengen. (NP steht für "nichtdeterministisch polynomial beschränkt" - in der Tat kann das x in der ersten Definition als eine Art nicht determinierten Leitfadens aufgefasst werden.)

Die Klasse P ist offenbar eine Teilklasse von NP. Erstaunlicherweise ist es bisher nicht gelungen zu entscheiden, ob die beiden Klassen P und NP gleich sind oder nicht. Wenn in der Mathematik überhaupt von einem "Indizienbeweis" gesprochen werden darf, so gewiss hier für die Vermutung $P \neq NP$ ("Cook'sche Hypothese"); der Leser wird die Indizien im folgenden kennen lernen.

Die Klasse NP ist abgeschlossen gegenüber Vereinigung und Durchschnitt; mit A in NP und f in Π gehört auch $f^{-1}A$ zu NP.

Unbekannt ist, ob NP komplement-abgeschlossen ist oder nicht. Es ist zu vermuten, dass es Mengen in NP gibt, deren Komplement nicht zu NP gehört; ein Beweis dafür würde natürlich die Cook'sche Hypothese bestätigen. Und wenn schon Vermutungen formuliert werden: Es gibt wohl auch Mengen A mit der Eigenschaft, dass zwar A und das Komplement von A zu NP gehören, die Menge A aber nicht zu P gehört. Sollte dies zutreffen, so würde sich das Begriffspaar P-NP in einer wesentlichen Eigenschaft vom Begriffspaar entscheidbare-aufzählbare Menge unterscheiden, zu dem es ja der Definition nach in enger Analogie steht.

Dass die Analogie auf alle Fälle nicht vollkommen ist, zeigt die Tatsache, dass es zwar universelle aufzählbare, aber keine universellen NP-Mengen gibt - gäbe es nämlich eine solche, so wären alle Mengen aus NP polynomial verifizierbar mit Polynomen eines festen Grades, im Widerspruch zu (Cook 1970).

Trotz dieser Unterschiede ist die Analogie der Begriffspaare von beträchtlichem heuristischen Wert. Ueberträgt man zum Beispiel die universelle Menge der Paare <e,a> ("die Maschine e akzeptiert a") aus der Rekursionstheorie in die PNP-Theorie, so wird man unmittelbar zu einer Menge V geführt, die zwar nicht universell, aber immerhin noch NP-vollständig ist. (D.h. V gehört zu NP und zu jedem A aus NP gibt es ein f in Π mit $A = f^{-1}V$.) Dabei ist V folgendermassen definiert: Das Tripel $<e,a,2^m>$ gehört zu V gewenn gilt: Die Maschine e verifiziert den Input

a in m Schritten.
Erstens zeigt nämlich eine einfache Ueberlegung, dass V in polynomialer Zeit verifizierbar ist. (Dabei wird auch klar, warum Tripel $\langle e,a,2^m\rangle$ und nicht etwa Tripel $\langle e,a,m\rangle$ verwendet werden.) Ist zweitens A eine Menge aus NP (die etwa durch die Turingmaschine e_o und das Polynom p verifiziert wird), so definiere man f durch

$$f(a) = \langle e_o, a, 2^{p(\ell(a))}\rangle.$$

Dann sind $a \in A$ und $f(a) \in V$ beide gleichbedeutend mit der Aussage "e_o verifiziert a in $p(\ell(a))$ Schritten".

Die Existenz einer vollständigen Menge V reicht nun zwar nicht aus, um mit Hilfe eines Diagonalverfahrens die Cook'sche Hypothese zu beweisen, aber doch, um sie auf eine besonders einfache Form zu bringen:

$$P \neq NP \iff V \notin P.$$

(Gleicherweise gilt: Gibt es überhaupt eine Menge A in NP, deren Komplement nicht zu NP gehört, so ist V eine solche.) Unter der Annahme der Cook'schen Hypothese ist also V nicht polynomial entscheidbar. Es liegt nun nahe, ähnlich wie in der Rekursionstheorie, die Menge V in interessante mathematische Entscheidungsprobleme zu transformieren. Wie (Cook 1970) und (Karp 1972) gezeigt haben, gelingt dies auf erstaunlich vielfältige Weise.

Ganz allgemein ist ein Entscheidungsproblem gegeben durch ein Paar von Mengen (A,B) mit $A \subset B$ (in der Meinung, dass zu entscheiden ist, welche b aus B zu A gehören). Da die Mengen A, B im allgemeinen keine Zahlmengen sind, müssen sie zuerst als solche kodiert werden. Für die vorliegenden Zwecke ist eine Kodierung eine injektive Abbildung von B in $\mathbb{N}$, deren Bild zu P gehört. (D.h. man kann in polynomialer Zeit entscheiden, ob eine Zahl die Kodenummer eines Elements von B ist.) Zwei Kodierungen φ und ψ werden als äquivalent betrachtet, gewenn die partiellen Funktionen $\psi\varphi^{-1}$ und $\varphi\psi^{-1}$ Einschränkungen von in polynomialer Zeit berechenbaren Funktionen sind.

Vermöge solcher Kodierungen lassen sich die Begriffe "in polynomialer Zeit berechenbar", "in polynomialer Zeit entscheidbar", "in polynomialer Zeit verifizierbar" und "vollständig" ohne weiteres auf allgemeine Entscheidungsprobleme übertragen. Das Ergebnis dieser Uebertragung hängt dabei nur von der Aequivalenzklasse der gewählten Kodierung ab.

Für viele Mengen ist (bis auf Aequivalenz) klar, wie man sie kodieren wird, da ihre Elemente als Wörter über einem endlichen Alphabet gegeben

sind. Beispiele hierfür sind Mengen von Polynomen oder Matrizen über den ganzen Zahlen oder über einem endlichen Körper, Mengen von aussagenlogischen Formeln, von Formeln einer Sprache erster Stufe.

Andere Mengen werden in natürlicher Weise auf solche zurückgeführt. Z.B. beschreibt man endliche Relationalstrukturen eines festen nichtleeren Typs (Graphen, Gruppen usw.) dadurch, dass man ihre Träger als Anfangsabschnitte der Menge der natürlichen Zahlen annimmt und die Diagramme ihrer Relationen etwa lexikographisch aufzählt. Man bemerke, dass dann die Länge der Kodenummer einer Struktur polynomial beschränkt ist in der Mächtigkeit der Struktur und umgekehrt. Polynomiale Entscheidbarkeit und Verifizierbarkeit werden also gemessen an der Grösse der betrachteten Strukturen.

Aus der Liste der von (Cook 1970) und (Karp 1972) angegebenen NP-vollständigen Entscheidungsprobleme greifen wir die folgenden heraus:

1. Zu entscheiden, ob eine aussagenlogische Formel erfüllbar ist (hier besteht also die obige Menge B aus allen aussagenlogischen Formeln, die Menge A aus den erfüllbaren).

2. Zu entscheiden, ob ein Graph G einen k-punktigen vollständigen Untergraphen besitzt (hier besteht B aus allen Paaren (G,k), A aus jenen mit der verlangten Eigenschaft).

3. Zu entscheiden, ob ein Graph G_1 isomorph einem Untergraphen eines Graphen G_2 ist. (Die Vollständigkeit des Problems zu entscheiden, ob zwei Graphen isomorph sind, ist dagegen noch fraglich.)

4. Zu entscheiden, ob ein Graph G einen Hamilton-Kreis besitzt. (Dagegen ist in polynomialer Zeit entscheidbar, ob G einen Euler-Kreis hat.)

5. Zu entscheiden, ob ein Graph dreifärbbar ist. (Dagegen ist in polynomialer Zeit entscheidbar, ob G zweifärbbar ist.)

6. Zu entscheiden, ob zu einem Paar (U,T) von endlichen Mengen mit $U \subset T^3$ eine Menge W existiert, so dass $W \subset U$ und die drei Projektionen $T^3 \rightarrow T$ bijektiv auf W sind. (Das analoge Problem mit $U \subset T^2$ ist in polynomialer Zeit entscheidbar.)

7. Zu entscheiden, ob eine lineare diophantische Gleichung $a_1x_1+\ldots+a_nx_n = b$ einen Lösungsvektor aus Komponenten 0 oder 1 besitzt. (Verlangt man vom Lösungsvektor nur, dass seine Komponenten ganzzahlig sind, so erhält man ein Problem, welches in polynomialer Zeit entscheidbar ist. Dies gilt sogar für Systeme von Gleichungen.)

Unter der Annahme der Cook'schen Hypothese ist keines dieser Probleme polynomial entscheidbar.

Wäre andererseits die Cook'sche Hypothese falsch, so könnte man nicht nur die Probleme 1 bis 7 in polynomialer Zeit entscheiden, sondern überhaupt alle Probleme in NP, seien sie nun vollständig oder nicht, und das mit einer einzigen allgemeinen Methode. Bedenkt man, dass z.B. die meisten algorithmischen Probleme der klassischen Zahlentheorie als Entscheidungsprobleme aus NP interpretiert werden können und dass es bisher nur in speziellen Fällen und mit speziellen Methoden gelungen ist, polynomiale Lösungsverfahren anzugeben, so erscheint die obige Annahme sehr unwahrscheinlich.

Ein weiteres Indiz für die Cook'sche Hypothese kann darin gesehen werden, dass in einem ganz anderen Zusammenhang (nämlich in der Modelltheorie) eine Vermutung aufgestellt worden ist, welche die Cook'sche Hypothese impliziert: Ist φ eine Formel erster Stufe, so ist das Spektrum von φ die Menge derjenigen natürlichen Zahlen n, für die ein n-zahliges Modell von φ existiert (Scholz 1952). Die "Spektrum-Hypothese" behauptet, dass es ein Spektrum gibt, dessen Komplement selbst kein Spektrum ist. Wie (Jones-Selman 1974) gezeigt haben, folgt aus der Spektrumhypothese, dass es Mengen in NP gibt, deren Komplement nicht in NP liegt (und die also sicher nicht zu P gehören).

Der im vorangehenden beschriebene Themenkreis wird in den Vorträgen I-IV und VII dargestellt. Der erste Vortrag gibt eine Einführung in die verschiedenen Typen von Turingmaschinen, ihre gegenseitigen Beziehungen und die Hierarchie der durch Zeitschranken definierten Klassen von Entscheidungsproblemen. Im zweiten Vortrag wird die NP-Vollständigkeit des Problems nachgewiesen, zu entscheiden, ob eine aussagenlogische Formel erfüllbar ist. Ausgehend von dieser Tatsache werden in den folgenden beiden Vorträgen eine grosse Anzahl von weiteren vollständigen Entscheidungsproblemen abgehandelt. Der siebente Vortrag ist dem Spektrumproblem gewidmet.

Im fünften Vortrag wird im Anschluss an (M. Hall 1956) ein polynomialer Algorithmus angegeben, welcher (unter anderem) gestattet, zu einer Folge $S_1, S_2, \ldots, S_m$ von endlichen Mengen eine maximale Teilmenge T von $\bigcup S_i$ zu bestimmen, für welche die Durchschnitte $T \cap S_i$ $(1 \leq i \leq m)$ höchstens ein Element enthalten. Die Existenz dieses Algorithmus mag ein Hinweis darauf sein, dass auch in Fällen, wo sich zunächst ein exponentieller Suchalgorithmus aufdrängt, eine genauere Analyse bisweilen zu

einem polynomialen Algorithmus führt.

Die in den Vorträgen III und IV behandelten Transformationen von Entscheidungsproblemen stehen in unmittelbarer Beziehung zu Transformationen, wie sie in der axiomatischen Mengenlehre benützt werden, um die Aequivalenz von Abschwächungen des Auswahlaxioms zu beweisen. Man betrachte etwa das folgende Paar von Entscheidungsproblemen

E_1: Zu entscheiden, ob ein endlicher Graph dreifärbbar ist.

E_2: Zu entscheiden, ob eine endliche Menge von aussagenlogischen Formeln erfüllbar ist.

Diesem Paar stelle man das folgende Paar von "abgeschwächten Auswahlaxiomen" gegenüber:

A_1: Jeder nicht dreifärbbare Graph besitzt einen endlichen, nicht dreifärbbaren Teilgraphen.

A_2: Jede unerfüllbare Menge von aussagenlogischen Formeln besitzt eine endliche, unerfüllbare Teilmenge.

Die "Aequivalenzen" $E_1 \sim E_2$ und $A_1 \sim A_2$ sind (unabhängig voneinander) auf sehr verwandte Weise bewiesen worden, nämlich durch zwei Kodierungen: Die eine kodiert Graphen in Formelmengen, die andere Formelmengen in Graphen, und zwar so, dass sich Erfüllbarkeit und Dreifärbbarkeit entsprechen.

Der sechste Vortrag ist der Herausarbeitung dieser Analogie gewidmet. Insbesondere werden dabei Transformationen konstruiert, welche sich zum Beweis der beiden Aequivalenzen eignen.

Die eingangs dargestellte Theorie von Cook und Karp lässt sich kurz so zusammenfassen: Es wird ein mit an Sicherheit grenzender Wahrscheinlichkeit schwieriges Entscheidungsproblem V angegeben. Dieses Problem wird in eine Vielzahl von konkreten mathematischen Entscheidungsproblemen derart transformiert, dass es seine mutmassliche Schwierigkeit auf jene überträgt. Die Analogie dieser Schlussweise mit der (in ihrer Substanz auf Gödel zurückgehenden) Beweisführung für die Unentscheidbarkeit mathematischer Theorien ist offenkundig. Die Analogie ist freilich nur unvollständig, weil das Entscheidungsproblem V nur vollständig (und nicht universell und damit nachweislich schwierig) ist.

Eine vollständige Uebertragung des Gödelschen Gedankengangs von der Fragestellung der Unentscheidbarkeit auf die der Schwerentscheidbarkeit ist aber auch möglich. Die Konstruktion schwer entscheidbarer Mengen mit Hilfe des Cantorschen Diagonalverfahrens war seit langem

bekannt (siehe Hopcroft-Ullman 1969). Die Einsicht, dass sich solche schwer entscheidbaren Mengen in interessante mathematische Entscheidungsprobleme transformieren lassen, verdankt man (Meyer-Stockmeyer 1972, siehe auch Meyer-Stockmeyer 197?). Während sich Meyer und Stockmeyer hauptsächlich mit Wortproblemen und mit Entscheidungsproblemen für Theorien höherer Stufe beschäftigen, haben (Fischer-Rabin 1974) gezeigt, dass praktisch alle (entscheidbaren) Theorien erster Stufe wenigstens "exponentielle Komplexität" haben. Beispiele sind die Presburgerarithmetik und die elementare Theorie der reellen Zahlen.

Der achte Vortrag ist der Arbeit von Fischer und Rabin gewidmet.

Im neunten Vortrag wird im Anschluss an (Collins 1975) und Monck-Solovay ein Entscheidungsverfahren (sogar ein Verfahren zur Quantoreneliminination) für die elementare Theorie der reellen Zahlen entwickelt, welches "nur" doppelt exponentiellen Aufwand benötigt.

Der zehnte Vortrag leitet von der Turing-Komplexität zur Boole'schen Komplexität über. Es wird der folgende Satz von (Fischer-Pippenger 197?) bewiesen: Sei f eine Funktion der Menge der endlichen {0,1}-Folgen in sich mit der Eigenschaft, dass lh(f(X)) nur von lh(X) abhängt (lh(X) = Länge der Folge X). Gibt es eine Mehrband-Turingmaschine, die f(X) in der Zeit t(lh(X)) berechnet, so lässt sich für jedes natürliche n die aus f durch Restriktion auf Inputs der Länge n entstehende Boole'sche Abbildung durch ein logisches Netz der Grösse O(t(n)logt(n)) darstellen.

Der elfte Vortrag ("Länge von Formeln") beschäftigt sich mit der Frage, welche "inneren Eigenschaften" von Funktionen zur Folge haben, dass jede die Funktion darstellende Formel lang ist. Es werden dabei im wesentlichen Boole'sche Funktionen betrachtet, und die darstellenden Formeln sind gebildet aus den Konstanten 0,1, den Variablen x_0, x_1, .. und den Boole'schen Operationen + und · (Ein Beispiel einer solchen Formel ist also etwa $(x_1+x_2)(x_2+x_3)+1$.)

Ist f eine Boole'sche Funktion, so sei $\ell(f)$ die Länge einer kürzesten Formel, welche f darstellt. Für untere Abschätzungen von $\ell(f)$ scheinen im wesentlichen zwei Methoden bekannt zu sein. Beide Methoden beruhen auf der Untersuchung der in einer Funktion enthaltenen Teilfunktionen. Dabei heisst g (in den Variablen $x_1,\ldots,x_n$) enthalten in f (in den Variablen $p_1,\ldots,p_m,x_1,\ldots,x_n$) falls für ein geeignetes $\vec{p}$ für alle $\vec{x}$ gilt: $g(\vec{x}) = f(\vec{p},\vec{x})$. Die erste Methode (Nečiporuk 1966) schätzt nun $\ell(f)$ nach unten ab auf Grund der Anzahl der in f enthaltenen Teilfunk-

tionen. Im allgemeinen liefert diese Abschätzung eine viel zu kleine Schranke; es gelingt aber, ein Beispiel zu konstruieren, wo die Schranke genau ist, und damit zu zeigen, dass die Methode in einem gewissen Sinne doch scharf ist.

Die zweite Methode (Hodes-Specker 1968) zeigt, dass jede Funktion, welche durch eine kurze Formel darstellbar ist, eine Teilfunktion von besonders einfacher Art enthält. Diese Methode liefert noch schlechtere Schranken, doch ist sie auch auf Funktionsklassen anwendbar, bei der die erste Methode versagt, wie etwa auf die Klasse der symmetrischen Funktionen.

Literatur

Collins, G.E., Quantifier elimination for real closed fields by cylindrical algebraic decomposition, Lecture Notes in Computer Science No. 33 (1975) 134-183, Springer-Verlag.

Cook, S.A., The complexity of theorem proving procedures, Conf. Rec. of 3rd ACM Symp. on Theory of Computing (1970) 151-158.

Fischer, M.J. und Pippenger, N.J., in Vorbereitung.

Fischer, M.J. and Rabin, M.O., Super-exponential complexity of Presburger arithmetic, MAC Technical Memorandum 43, M.I.T., 1974.

Hall, M. Jr., An algorithm for distinct representatives, Amer. Math. Monthly 63 (1956) 716-717.

Hodes, L. and Specker, E., Length of formulas and elimination of quantifiers I, Contr. to Math. Logic (1968) 175-188.

Hopcroft, J.E. and Ullman, J.D., Formal Languages and their Relation to Automata, Addison-Wesley, Reading, Massachusetts, 1969.

Jones, N.D. and Selman, A.L., Turing machines and the spectra of first-order formulas, J. Symbolic Logic 39 (1974) 139-150.

Karp, R.M., Reducibility among combinatorial problems, IBM Symposium 1972: Complexity of Computer Computations, Plenum Press, New York, 1972.

Knuth, D.E., The Art of Computer Programming, vol. 2, Addison-Wesley, Reading, Massachusetts, 1969.

Meyer, A.R. and Stockmeyer, J.L., The equivalence problem for regular expressions with squaring requires exponential space, Conf. Rec. of 13th Annual Symp. on Switching and Automata Theory (1972) 125-129.

Meyer, A.R. and Stockmeyer, L.J., Inherent computational complexity of decision problems in logic and automata theory, erscheint in Lecture Notes in Computer Science, Springer-Verlag.

Nečiporuk, È.I., A boolean function, Dokl. Akad. Nauk SSSR 169 (1966) 765-766, Engl. Transl.: Soviet Math. Dokl. 7 (1966) 999-1000.

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