Algebraische Berechnungsmodelle

Grundlagen

Gruppentheorie

- Ein Tripel (K,+,*), bestehend aus einer Menge K und zwei binären Verknüpfungen + und * (die üblicherweise Addition und Multiplikation genannt werden), ist genau dann ein **Körper**, wenn folgende Eigenschaften erfüllt sind:

1. (K,+) ist eine abelsche Gruppe (Neutralelement 0)
2. (K\{0},*) ist eine abelsche Gruppe (Neutralelement 1)
3. a*(b+c) = a*b + a*c,
   (a+b)*c = a*c + b*c (Distributivgesetz) für alle a,b,c aus K

- Eine **abelsche Gruppe** ist eine Gruppe (G,*), für die das Kommutativgesetz
  a * b = b * a
  für alle a, b aus G gilt.
- Ein Paar (G, *) mit einer Menge G und einer inneren zweistelligen Verknüpfung
  $*: G \times G \to G, (a,b) \mapsto a * b$
  heißt **Gruppe**, wenn folgende Axiome erfüllt sind:
  * Assoziativität: Für alle Gruppenelemente a, b und c gilt: (a * b) * c = a * (b * c).
  * Es gibt ein neutrales Element e∈G, mit dem für alle Gruppenelemente a ∈ G gilt: a * e = e * a = a.
  * Zu jedem Gruppenelement a∈G existiert ein inverses Element a^{-1}∈G mit: a * a^{-1} = a^{-1} * a = e.
- Eine **Ring** ist eine algebraische Struktur, in der, ähnlich wie in den ganzen Zahlen Z, Addition und Multiplikation definiert und miteinander bezüglich Klammersetzung verträglich sind.
- Die **Charakteristik** eines Körpers ist die Anzahl der 1-Elemente, die summiert werden müssen, um das 0-Element zu erzeugen.
  (beispielsweise: Charakteristik von R ist 0, die von {0,1} ist 2, denn 1+1=0)

Determinanten und Permanenten

Die Determinante als Funktion ihrer Minoren

Der ij-te **Minor** einer n x n - Matrix A ist für n >1 die (n-1) + (n-1) – Matrix $A_{[ij]}$, die wir durch Löschen der i-ten Zeile und j-ten Spalte von A erhalten

Die Determinante einer nxn Matrix **rekursiv dargestellt als Funktion ihrer Minoren** ist:
Det(A) = a_{11}, , falls n=1
Det(A) = $\Sigma_{(j=1 \text{ bis } n)} (-1)^{1+j} * a_{1j} * \det(A_{[1j]})$, falls n>1

Eigenschaften von Determinanten

Die Determinante eine quadratischen Matrix A hat folgende Eigenschaften:

- Wenn eine beliebige Spalte oder Zeile der Matrix null ist, so gilt det(A)=0.
- Die Terminante von a wird mit λ multipliziert, wenn die Elemente einer beliebigen Zeile (oder einer beliebigen Spalte) von A mit λ multipliziert werden.
- Die Determinante von A bleibt unverändert, wenn die Elemente in einer einzelnen Zeile (bzw. Spalte) zu einer anderen Zeile (bzw. Spalte) addiert werden.
- Die Determinante von A ist gleich der Determinante von A^T.
- Die Determinante von A wird mit –1 multipliziert, wenn zwei beliebige Zeilen (bzw. Spalten) ausgetauscht werden.

Die Permanente

$$\operatorname{perm}(A) := \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

(A ist n x n – Matrix)
Bis auf das wechselnde Vorzeichen entspricht die Permanente der Determinante. Trotzdem ist erstaunlicherweise kein Algorithmus (etwa analog zum Gausschen Eliminationsverfahren für Determinanten) bekannt, der dieses Problem effizient löst. Im Gegenteil: Die Permanente steht im Verdacht, ein hartes Problem im algebraischen Analog zu NP (VNP) zu sein.

Bedeutung der Permanente

Während eine geometrische Interpretation der Permanente nicht bekannt ist, hat sie eine Bedeutung in der Graphentheorie beim Finden perfekter Matchings (besser gesagt deren Anzahl) auf bipartiten Graphen.
Die Zahl, die sich auf einer 0,1 Matrix der Dimension n (bei n Knoten) ergibt, ist die Anzahl der perfekten Matchings. Hierbei steht in der Matrix genau dann eine 1, wenn eine Kante zwischen den zwei betreffenden Knoten besteht, 0 sonst.

Komplexitätsklassen

P

umfasst alle in {0,1} (oder einer polynomiell verwandten Codierung) codierten Probleme, die auf eine deterministischen Turingmaschine in polynomieller Zeit (in der Größe der Eingabe) berechenbar (bzw. entscheidbar) sind.

NP

umfasst alle wie in P codierten Probleme, die von einer nichtdeterministischen Turingmaschine in polynomieller Zeit gelöst (entschieden) werden können.
Analog kann eine deterministische Turingmaschine diese Probleme in polynomieller Zeit verifizieren, wenn man ihr zusätzlich zur Probleminstanz einen Zeugen (polynomiell in Länge der Probleminstanz) übergibt.

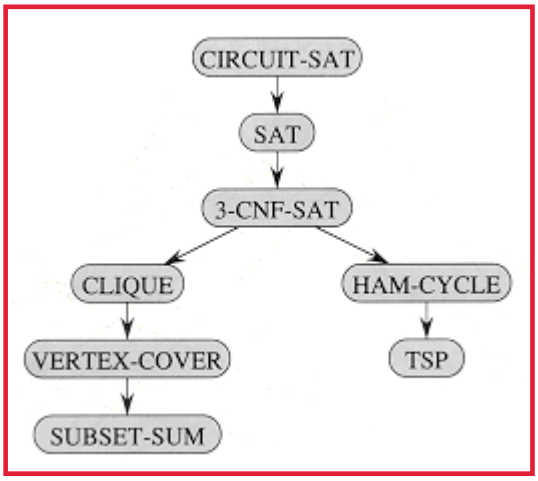
FP

umfasst die Menge von Funktionen f:{0,1}* → {0,1}* (und äquivalent {0,1}* → N), die von einer deterministischen Turingmaschine in polynompieller Zeit berechenbar sind.

Damit ist FP die Klasse der effizient berechenbaren Funktionen, d.h. das Analog zu P für Funktionen mit mehr als einem Ausgabebit.

#P (Count P)
bezeichnet diejenigen Probleme, die die Anzahl von Lösungen (also Zeugen) für die Probleme in NPC berechnen.

NPC
umfasst alle NP-vollständigen Probleme. Es gilt NPC $\subseteq$ NP und alle Probleme in NPC lassen sich in polynomieller Zeit aufeinander reduzieren (bzw. in einander überführen). Damit sind die NPC – Probleme in gewissem Sinne die schwierigsten Probleme in NP.



Cook und Levin bewiesen mit Circuit –Sat die erste NP - vollständige Sprache und zeigten, dass sich alle Sprachen aus NP auf Circuit - Sat reduzieren lassen.

Eine untere Schranke für die Komplexität boolscher Schaltkreise ist nicht bewiesen.

Die Frage NP?=P ist daher offen.

Algebraische Komplexitätsklassen

AlgP (:=VP)
umfasst alle Polynomfamilien polynomiell beschränkten Grades, die berechenbar sind von algebraischen Schaltkreisen polynomieller Größe (in der Anzahl ihrer Eingabevariablen).

AlgNP (:=VNP)
umfasst diejenigen Polynomfamilien polynomiell beschränkten Grades, die definierbar sind als:
$\mathbf{P_n(x_1,x_2,\ldots,x_n) = \Sigma_{e\in\{0,1\}^{m-n}} g_m(x_1,x_2,\ldots,x_n,e_{n+1},\ldots,e_m),}$
wobei: $g_m \in$ AlgP und m ist polynomiell in n.

Eine Familie von Polynomen $\{p_n\}$ hat **polynomiell beschränkten Grad**, falls eine Konstante $c\in N$ existiert, so dass für jedes n der Grad des Polynoms höchstens cn^c ist.
(n ist die Anzahl der Variablen aus dem Körper K, die p benutzt)

Sätze über algebraische Berechnungsmodelle

☐ *(maximaler Grad der Ausgabe eines algebraischen Linearen Programms)*
Jedes algebraische lineare Programm (alP) berechnet ein Polynom in Abhängigkkeit von dessen Grad.

Die Ausgabe eines alP nach T Schritten mit Variablen $x_1, ..., x_n$ ist ein Polynom $p(x_1,...,x_n)$ mit maximalem Grad 2^T.

☐ *(Zusammenhang zwischen alP und Algebraischen Schaltkreisen AS)*
Gegeben eine Funktion f: K→K
Besitzt f ein alP der Größe S, hat es einen AS der Größe 3S.
Ist f berechenbar von einem AS der Größe S, dann auch von einem alP der Größe S.

Die Topologie - Methode zur Bestimmung unterer Schranken für Algebraische Berechnungsbäume

☐ *(Zusammenhangskomponente)*
Eine Menge $S \subseteq R^n$ ist (weg)zusammenhängend, wenn für alle $x,y \in S$ ein Pfad p von x nach y existiert, der innerhalb von S liegt.
Eine Zusammenhangskomponente von S ist eine zusammenhängende Teilmenge von S, die keine echte Teilmenge einer anderen zusammenhängenden Teilmenge ist.

☐ *(Anzahl der Zusammenhangskomponenten in einer Menge)*
Sei $W = \{ (x_1,...,x_n) \mid \Pi_{(i\neq j)} (x_i - x_j) \neq 0\}$.
Dann ist die Anzahl der Zusammenhangskomponenten in $W \geq n!$

☐ *(Ben Or)*
Für jede Funktion f: $R^n \rightarrow \{0,1\}$ ist die algebraische Berechnungsbaumkomplexität:
$AC(f) = \Omega (\log (\max \{ \#f^{(-1)}(1) , \#R^n \backslash f^{(-1)}(1) \})-n)$

☐ *(Konsequenz aus Milnor-Thom-Theorem)*
Wenn $S \subseteq Rn$ von Grad-d-Ausdrücken mit m Gleichungen und h Ungleichungen definiert ist, dann gilt für die Anzahl der Zusammenhangskomponenten (#(S)):
$\#(S) \leq d(2d-1)^{n+h-1}$

Die Idee der Reduktion in VNP

☐ *(Projektion)*
Eine Funktion $f(x_1,...,x_n)$ ist eine Projektion einer Funktion $g(y_1,...,y_m)$, wenn ein Mapping σ von der Menge $\{y_1,...,y_m\}$ in die Menge $\{0,1,x_1,...,x_n\}$ existiert, so daß gilt:
$f(x_1,x_2,...,x_n) = g(\sigma(y_1), \sigma(y_2),..., \sigma(y_m))$.

☐ *(Projektionsreduzierbarkeit)*
Eine Funktion f heißt projektionsreduzierbar auf g, wenn f eine Projektion von g ist.

Vollständigkeit von Determinante und Perminante

Für jeden Körper K ist jede Polynomfamilie mit n Variablen, die mit einer algebraischen Formel der Größe n berechenbar ist, **projektionsreduzierbar auf die Determinantenfunktion** (über K) mit höchsten **n+2** Variablen.

Für jeden Körper K mit **Charakeristik 2** läßt sich jede Polynomfamilie aus VNP **projektionsreduzieren auf die Permanentenfunktion** (über K) mit höchstens **polynomiell** mehr Variablen.