
Ein Beitrag zu einem Problem von gerichteten Graphen

Kurt Schütte

Kurt Schütte wurde 1909 in Salzwedel geboren. Er studierte in Berlin und Göttingen und promovierte 1933 als David Hilberts letzter Promovent. Von 1936 bis 1945 war er als Meteorologe tätig. Nach einigen Jahren im Schuldienst wurde er 1950 wissenschaftlicher Assistent in Marburg und habilitierte sich dort im Jahre 1952. Nach Gastaufenthalten am Institute for Advanced Study in Princeton, an der ETH Zürich und an der Pennsylvania State University folgte er 1963 einem Ruf an die Universität Kiel. Ab 1966 bis zu seiner Emeritierung war er dann an der Universität München tätig. Kurt Schütte verstarb am 18. August 1998.

Der Arbeitsschwerpunkt von Kurt Schütte war die Beweistheorie. Daneben hat er auch über die Grundlagen der Geometrie und über algebraische Probleme gearbeitet. Seine Monographie "Beweistheorie" wurde zum Standardwerk.

In Teil [2] meiner Dissertation hatte ich zur Konstruktion von endlichen Modellen für gewisse prädikatenlogische Formeln einen gerichteten Graphen von 7 Elementen gebraucht, der die Eigenschaft hat, daß je zwei Elemente des Graphen auf ein Element des Graphen gerichtet sind. Dies hatte mich zu der Frage geführt, ob es für jede positive ganze Zahl n einen endlichen gerichteten Graphen gibt mit der Eigenschaft, daß je n Elemente des Graphen auf ein Element des Graphen gerichtet sind.

Als ich einmal in Oberwolfach Herrn Erdős diese Frage gestellt hatte, hat er mir nach kurzer Zeit mitgeteilt, er könne mit wahrscheinlichkeitstheoretischen Methoden beweisen, daß es für jede positive ganze Zahl n einen derartigen endlichen gerichteten Graphen

Nicht selten lassen sich mathematische Probleme auf Fragen über Graphen zurückführen: Das Königsberger Brückenproblem ist dafür ein elementares und wohlbekanntes Beispiel. Auch das graphentheoretische Problem, das sich Kurt Schütte in seinem Beitrag stellt, hat seine Wurzel in einem anderen Gebiet, nämlich in der Logik. Gefragt wird nach dem kleinsten vollständig gerichteten Graphen, in dem jeder Knoten von mindestens n der gerichteten Kanten getroffen wird (allgemeiner: je m Knoten werden von n gerichteten Kanten getroffen.) Es ist dies eine einfache, attraktive Frage und interessanten Beispiele lassen sich ohne grosse Schwierigkeiten angeben. Die Lösung allerdings scheint schwierig zu sein: es sind jedenfalls bis heute nur Abschätzungen bekannt. – Die *Elemente der Mathematik* rechnen es sich als eine hohe Ehre an, diese letzte Arbeit des grossen Beweistheoretikers Kurt Schütte veröffentlichen zu dürfen. *ust*

gibt. Seine in dieser Hinsicht erzielten Ergebnisse hat er in [1] erwähnt. Es handelt sich hierbei um eine untere Schranke $2^{n+1} - 1$ und eine obere Schranke für die kleinste Zahl $f(n)$, für die es einen gerichteten Graphen von $f(n)$ Elementen gibt mit der Eigenschaft, daß je n Elemente des Graphen auf ein Element des Graphen gerichtet sind. Man hat $f(1) = 3$ und $f(2) = 7$. Im folgenden wird nun $f(3) = 19$ bewiesen und eine ab $n = 3$ stärker als $2^{n+1} - 1$ ansteigende untere Schranke für $f(n)$ nachgewiesen.

Ein vollständig gerichteter Graph $G = (M, R)$ besteht aus einer Menge M von mindestens zwei Elementen und einer Relation R auf $M \times M$ derart, daß für kein $x \in M$ $x R x$ gilt und für je zwei verschiedene $x, y \in M$ genau eine der beiden Beziehungen $x R y$ oder $y R x$ gilt. Für jeden vollständig gerichteten Graphen $G = (M, R)$ und jedes Element $c \in M$ sei M_c/R die Menge derjenigen $x \in M$, für die $c R x$ gilt.

Im folgenden bezeichnen k, m, n stets positive ganze Zahlen.

Definition 1 Wir sagen, daß ein vollständig gerichteter Graph $G = (M, R)$ die Eigenschaft $E(m, n)$ hat, wenn es zu je m Elementen $x_1, \dots, x_m \in M$ mindestens n paarweise verschiedene Elemente $y_1, \dots, y_n \in M$ gibt mit $x_i R y_j$ für $i = 1, \dots, m$ und $j = 1, \dots, n$. $f(m, n)$ sei die kleinste Kardinalzahl, für die es einen vollständig gerichteten Graphen von $f(m, n)$ Elementen mit der Eigenschaft $E(m, n)$ gibt. Wir setzen $f(m) = f(m, 1)$.

Diese Definition von $f(m, n)$ und von $f(n)$ setzt nicht die Existenz von endlichen gerichteten Graphen mit der Eigenschaft $E(m, n)$ voraus, da offenbar die Menge aller natürlichen Zahlen bezüglich der $<$ -Relation einen vollständig gerichteten Graphen bildet mit der Eigenschaft $E(m, n)$ für alle m und n .

Lemma 1 $f(1, n) \geq 2n + 1$.

Beweis. $G = (M, R)$ sei ein vollständig gerichteter Graph von k Elementen, wobei k kleiner als $2n + 1$ ist. Dann ist die Anzahl $\binom{k}{2}$ der Elementenpaare von M kleiner als $k \cdot n$. Daher gibt es mindestens ein $c \in M$ derart, daß die Menge M_c/R weniger als n Elemente hat. Dann hat der Graph G nicht die Eigenschaft $E(1, n)$. Somit ist $f(1, n) \geq 2n + 1$.

Lemma 2 $f(m, n) \geq 2^m \cdot (n + 1) - 1$.

Beweis durch Induktion nach m . Setzt man $g(m, n) = 2^m \cdot (n + 1) - 1$, so erhält man $g(1, n) = 2n + 1$ und $g(m + 1, n) = 1 + 2 \cdot g(m, n)$. Für $m = 1$ folgt die Behauptung aus Lemma 1. Sei nun $G = (M, R)$ ein vollständig gerichteter Graph von k Elementen, wobei $k < g(m + 1, n) = 1 + 2 \cdot g(m, n)$ ist, dann ist die Anzahl $\binom{k}{2}$ der Elementenpaare von M kleiner als $k \cdot g(m, n)$. Daher gibt es mindestens ein c in M derart, daß die Menge M_c/R weniger als $g(m, n)$ Elemente hat. Diese Menge M_c/R kann nach Induktionsvoraussetzung nicht die Elementenmenge eines vollständig gerichteten Graphen mit der Eigenschaft $E(m, n)$ sein. Hiermit ergibt sich, daß der Graph G nicht die Eigenschaft $E(m + 1, n)$ hat. Somit hat jeder vollständig gerichtete Graph mit der Eigenschaft $E(m + 1, n)$ mindestens $g(m + 1, n)$ Elemente, womit die Behauptung auch für $m + 1$ bewiesen ist.

Lemma 3 Jeder vollständig gerichtete Graph mit der Eigenschaft $E(m+1, 1)$ hat die Eigenschaft $E(m, m+2)$.

Beweis. $G = (M, R)$ sei ein vollständig gerichteter Graph mit der Eigenschaft $E(m+1, 1)$. x_1, \dots, x_m seien m beliebige Elemente von M . M' sei die Menge derjenigen y aus M , für die x_1Ry, \dots, x_mRy gilt. Diese Menge M' ist aufgrund der Eigenschaft von G nicht leer. Angenommen, sie enthalte weniger als $m+2$ paarweise verschiedene Elemente. Dann gibt es aufgrund der Eigenschaft $E(m+1, 1)$ von G ein Element x_{m+1} von M mit yRx_{m+1} für alle y aus M' . In diesem Fall gibt es kein y in M mit x_iRy für alle $i = 1, \dots, m+1$ im Widerspruch zur Eigenschaft $E(m+1, 1)$ von G . Somit enthält die Menge M' mindestens $m+2$ paarweise verschiedene Elemente, womit die Behauptung bewiesen ist.

Für jede Primzahl $p \equiv 3$ modulo 4 ist bekanntlich -1 kein quadratischer Rest modulo p . Dann ist für je zwei verschiedene Elemente x, y des Primkörpers der Charakteristik p genau eine der beiden Differenzen $x-y$ oder $y-x$ ein quadratischer Rest modulo p . Wir können daher vollständig gerichtete Graphen Q_p von p Elementen folgendermaßen definieren.

Definition 2 Für jede Primzahl $p \equiv 3$ modulo 4 sei K_p der Primkörper der Charakteristik p und $Q_p = (K_p, R)$ derjenige vollständig gerichtete Graph, in dem für je zwei verschiedene Elemente $x, y \in K_p$ genau dann xRy gilt, wenn $y-x$ ein quadratischer Rest modulo p ist.

Offenbar hat der Graph Q_3 die Eigenschaft $E(1, 1)$. Mit Lemma 1 folgt $f(1) = 3$.

Bekanntlich hat der Graph Q_7 die Eigenschaft $E(2, 1)$. Mit Lemma 2 folgt $f(2) = 7$.

Lemma 4 Der Graph Q_{19} hat die Eigenschaft $E(3, 1)$.

Beweis. Die quadratischen Reste modulo 19 sind

$$1, 4, 5, 6, 7, 9, 11, 16, 17.$$

Ein quadratischer Rest q heie ausgezeichnet, wenn auch $q-1$ ein quadratischer Rest ist. Die ausgezeichneten quadratischen Reste modulo 19 sind 5, 6, 7, 17. Wir stellen zunchst folgendes fest.

- (1) Zu jedem von 0 und 1 verschiedenen Element c von K_{19} gibt es einen ausgezeichneten quadratischen Rest q modulo 19 derart, da cRq in Q_{19} gilt.

In Q_{19} ergibt sich

$$2R6, 3R7, 4R5, 5R6, 6R7, 7R5, 8R6, 9R7, 10R17, 11R17, \\ 12R17, 13R17, 14R6, 15R7, 16R17, 17R5, 18R6,$$

womit (1) besttigt ist.

Nach (1) gibt es quadratische Reste q_1, q_2, q_3 modulo 19 mit

$$(2) q_1 = 1 + q_2 = c + q_3.$$

Seien nun x, y, z paarweise verschiedene Elemente von K_{19} . Wir können ohne Beschränkung der Allgemeinheit annehmen, daß $y - x$ ein quadratischer Rest modulo 19 ist. Dann sind für $i = 1, 2, 3$ auch $r_i = q_i \cdot (y - x)$ quadratische Reste modulo 19. Hiermit ergibt sich, da K_{19} ein Körper ist, aus (2) durch Multiplikation mit $y - x$

$$r_1 = y - x + r_2 = c \cdot (y - x) + r_3.$$

Für $c = \frac{z-x}{y-x}$ folgt $x + r_1 = y + r_2 = z + r_3$, womit die Behauptung von Lemma 4 bewiesen ist.

Theorem $f(3) = 19$.

Beweis. Nach den Lemmata 3 und 2 hat man $f(3) \geq f(2, 4) \geq 4 \cdot 5 - 1 = 19$. Mit Lemma 4 folgt $f(3) = 19$.

Lemma 5 $f(m+1) \geq 2^m \cdot (m+3) - 1$, wobei aufgrund von $f(2) = 7$ und $f(3) = 19$ für $m = 1$ und $m = 2$ die Gleichheit gilt.

Beweis. Nach den Lemmata 3 und 2 hat man $f(m+1) \geq f(m, m+2) \geq 2^m \cdot (m+3) - 1$.

Anmerkung Nach Lemma 5 ist $f(4) \geq 47$. Der Graph Q_{47} hat jedoch nicht die Eigenschaft $E(4, 1)$, da z.B. die vier Elemente 0, 1, 6, 25 von K_{47} auf kein Element von Q_{47} gerichtet sind. Vermutlich ist $f(4) > 47$.

Herrn Prof. Dr. Wolfram Pohlers, Herrn Hochschuldozenten Dr. Andreas Weiermann, Frau Martina Pfeifer und Frau Anne Ernst danke ich herzlich für die Durchsicht und Niederschrift des vorliegenden Textes.

Literatur

- [1] P. Erdős. *Applications of Probability to Combinatorial Problems*. Colloquium on Combinatorial Methods in Probability Theory. Matematisk Institut, Aarhus Universitet, Denmark, August 1–10, 1962
- [2] K. Schütte. *Über die Erfüllbarkeit einer Klasse von logischen Formeln*. Math. Ann. 110 (1934), S. 161–194

Kurt Schütte
Belgradstr. 86
D-80804 München