SIIM-TR-B-**05-04**

SIIM Technical Report

52. Workshop über Komplexitätstheorie, Datenstrukturen und Effiziente Algorithmen („Theorietag“)

Jan Arpe, Bodo Manthey, Rüdiger Reischuk
(Herausgeber)

Schriftenreihe der Institute für

Informatik/Mathematik

Serie B

16. & 17. August 2005

Universität zu Lübeck
Technisch-Naturwissenschaftliche Fakultät

Email: arpe/manthey@tcs.uni-luebeck.de
Phone: +49-451-500-5312/5313
Fax: +49-451-500-5301

Vorwort

Der Workshop über Komplexitätstheorie, Datenstrukturen und Effiziente Algorithmen („Theorietag“) wird seit 1987 in der Regel dreimal jährlich von Mitgliedern der Fachgruppen „Komplexität“ (0.1.4) und „Parallele und Verteilte Systeme“ (0.1.3) der Gesellschaft für Informatik (GI) veranstaltet. Er ermöglicht einen intensiven Dialog zwischen Nachwuchswissenschaftlern und erfahrenen Forschern auf dem Gebiet der Theoretischen Informatik.

Der 52. Workshop am 16. und 17. August 2005 wird vom Institut für Theoretische Informatik der Universität zu Lübeck als Satellite Workshop zum *15th International Symposium on Fundamentals of Computation Theory (FCT 2005)* ausgerichtet. Er findet erstmals an zwei Tagen statt, um es Teilnehmern aus ganz Deutschland zu ermöglichen, bei nur einer Übernachtung bequem am gesamten Programm teilzunehmen. Am Abend des ersten Workshoptags wird ein Grillabend veranstaltet, bei dem sich die Teilnehmer in lockerer Atmosphäre austauschen können.

Wir bedanken uns bei den elf Vortragenden, insbesondere bei Martin Dietzfelbinger (Technische Universität Ilmenau) und Thomas Wilke (Christian-Albrechts-Universität zu Kiel) für ihre Gastvorträge.

Wir danken außerdem ganz besonders dem INTERREG III B-Projekt „Decision Support“ für die großzügige finanzielle Unterstützung des Workshops. Ferner danken wir der Sparkasse zu Lübeck für die Spende von Notizblöcken und Kugelschreibern.

Lübeck, im August 2005

Jan Arpe
Bodo Manthey
Rüdiger Reischuk

Programm

Dienstag, 16.8.2005

14:00 **Begrüßung**

14:05 Gastvortrag:
Synthesis from Knowledge-based Specifications
Thomas Wilke (Christian-Albrechts-Universität zu Kiel)

15:05 **Kaffeepause**

15:30 **Ein Algorithmus zur Entscheidung des Knotenproblems in einer Laufzeit $O(2^{4n})$**
Günter Hotz (Universität des Saarlandes Saarbrücken)

16:00 **Compression-Based Fixed-Parameter Algorithms for Feedback Vertex Set and Edge Bipartization**
Jiong Guo (Friedrich-Schiller-Universität Jena)

16:30 **Neues zu Teilinformation und Selbstreduzierbarkeit**
Arfst Nickelsen (Technische Universität Berlin)

17:00 **Kaffeepause**

17:30 **Data Exchange: On the Complexity of Answering Queries with Inequalities**
Alexander Mądry (University of Wrocław)

18:00 **Online-Algorithmen zur Lastbalanzierung auf dynamischen Netzwerken**
Bettina Rehberg (Universität Paderborn)

anschließend Grillen an der Wakenitz

Mittwoch, 17.8.2005

10:00 **Dynamische und t-private Auktionen**
Markus Hinkelmann (Universität zu Lübeck)

10:30 **Kryptographisch t-private Auktionen**
Nina Moebius (Universität zu Lübeck)

11:00 **Kaffeepause**

11:30 **Simulationsrelationen als Minimierungsheuristiken für ω-Automaten**
Carsten Fritz (Christian-Albrechts-Universität zu Kiel)

12:00 **Eingeschränkte Zyklenüberdeckungen**
Bodo Manthey (Universität zu Lübeck)

12:30 **Mittagspause**

14:00 Gastvortrag:
Hashing und Zufallsgraphen
Martin Dietzfelbinger (Technische Universität Ilmenau)

15:00 **Ende des Workshops**

Gastvortrag

Synthesis from Knowledge-based Specifications

Thomas Wilke

Christian-Albrechts-Universität zu Kiel

In program synthesis, one starts with a specification of a system and attempts to derive a program that implements this specification. This problem is particularly challenging in the context of open or reactive systems, which are required to respond appropriately to a sequence of inputs provided by an environment that is not under their full control.

In the talk we will consider the situation where the systems to be synthesized are distributed and specified in the "logic of knowledge and linear time." This is motivated by the fact that properties of distributed systems often refer to their temporal aspects and, in addition, the uncertainty that system components have about the global state of the system. For instance, a designer might make a statement such as "if process X knows that the transaction will be aborted, it should rollback its local contribution and terminate immediately." Such assertions can be made formal in the logic of knowledge and linear time.

Ein Algorithmus zur Entscheidung des Knotenproblems in einer Laufzeit $O(2^{4n})$

Günter Hotz

Universität des Saarlandes

Zur Lösung des Problems, die Äquivalenz von Knoten zu entscheiden, verwenden wir eine Normalisierung von Knotenprojektionen, die auf Gauss zurückgeht, in einer Form, die ihr von Reidemeister gegeben wurde. Gauss hatte bemerkt, dass man jeden Knoten so in die Ebene projizieren kann, dass es zwei Punkte A und B auf der Projektion gibt, die die Projektionslinie in zwei einfache Kurven zerlegt. Reidemeister bewegt die eine der beiden Kurven wieder in den Raum, so dass daraus eine Arkade mit Bögen über und unter der Projektionsebene entsteht. Der Knoten wird somit repräsentiert durch eine Arkade und einen Faden, der an Anfangs- und Endknoten befestigt sich in der Ebene liegend sich doppelpunktfrei um die Pfeiler der Arkade schwingt. Wir nennen diese Knotenrepräsentation eine Arkaden-Faden-Lage (AFL). Jede AFL wird auf der Kugeloberfläche angelegt bis auf Isomorphie eindeutig durch ein Wort beschrieben, dessen Alphabet aus den Namen der Arkaden der AFL besteht bereichert durch einen Exponenten, der angibt, in welcher Richtung der Faden den entsprechenden Arkadenbogen unter- bzw. überkreuzt. Zu jedem Knoten gehört eine formale Sprache über einem unendlichen Alphabet, das die beschriebenen Alphabete umfasst. Es gibt eine leicht beschreibbare Grammatik, die diese Sprache aus jedem vorgegebenen Repräsentanten der Sprache erzeugt.

Wir geben einen Algorithmus an, der zu jeder Knotenprojektion K mit n Kreuzungspunkten maximal reduzierte AFL erzeugt, die höchstens zwei Kreuzungspunkte besitzen. Wir zeigen, dass zwei Knotenprojektionen K und K' genau denselben Knoten repräsentieren, wenn die zugehörigen Mengen von AFL $M(K)$ und $M(K')$ einen nichtleeren Durchschnitt besitzen. Das lässt sich mit Hilfe der zugehörigen Sprachen in einer Zeit $O(2^{4n})$ entscheiden.

Wir definieren weiter eine starke Knoteninvariante, die sich wesentlich effizienter berechnen lässt.

Compression-Based Fixed-Parameter Algorithms for Feedback Vertex Set and Edge Bipartization

Jiong Guo[a,1] *Jens Gramm*[b,2] *Falk Hüffner*[a,1]
Rolf Niedermeier[a] *Sebastian Wernicke*[a,3]

[a] Institut für Informatik, Friedrich-Schiller-Universität Jena
Ernst-Abbe-Platz 2, 07743 Jena, Germany
guo/hueffner/niedermr/wernicke@minet.uni-jena.de

[b] Wilhelm-Schickard-Institut für Informatik, Universität Tübingen
Sand 13, 72076 Tübingen, Germany
gramm@informatik.uni-tuebingen.de

We show that the NP-complete Feedback Vertex Set problem, which asks for the smallest set of vertices to remove from a graph to destroy all cycles, is deterministically solvable in $O(c^k \cdot m)$ time. Here, m denotes the number of graph edges, k denotes the size of the feedback vertex set searched for, and c is a constant. As a further result, we present a fixed-parameter algorithm with runtime $O(2^k \cdot m^2)$ for the NP-complete Edge Bipartization problem, which asks for the smallest set of edges to remove from a graph to make it bipartite.

[1]Supported by the Deutsche Forschungsgemeinschaft (DFG), Emmy Noether research group PIAF (fixed-parameter algorithms), NI 369/4.

[2]Supported by the Deutsche Forschungsgemeinschaft (DFG), project OPAL (optimal solutions for hard problems in computational biology), NI 369/2.

[3]Supported by Deutsche Telekom Stiftung and Studienstiftung des deutschen Volkes.

Neues zu Teilinformation und Selbstreduzierbarkeit

André Hernich *Arfst Nickelsen*

Technische Universität Berlin
hernich@informatik.hu-berlin.de
nicke@cs.tu-berlin.de

Ein *Teilinformationsalgorithmus* für eine Sprache A berechnet (für festes m) für Eingabewerte $x_1, \ldots, x_m$ eine Menge von Bitstrings, die $\chi_A(x_1, \ldots, x_m)$ enthält. Zum Beispiel sind die Klassen der p-selektiven, der approximierbaren oder der leicht zählbaren Sprachen durch die Existenz von polynomiell zeitbeschränkten Algorithmen definiert, die jeweils Teilinformation eines bestimmten Typs berechnen.

Für eine *selbstreduzierbare* Sprache A lässt sich Zugehörigkeit zu A in polynomieller Zeit auf die Zugehörigkeit zu A von Worten geringerer Länge zurückführen. Selbstreduzierbare Sprachen für verschiedene Reduktionsarten (Turing, truth-table etc.) bilden Teilklassen von PSPACE.

Selbstreduzierbare Sprachen mit Teilinformationsalgorithmus lassen sich oft in Teilklassen von PSPACE einordnen. Bekanntestes Ergebnis dieser Art ist: Selbstreduzierbare p-selektive Sprachen sind in P [Buhrman, van Helden, Torenvliet 1993].

Eng verwandt damit sind Ergebnisse, die besagen, dass die Existenz eines Teilinformationsalgorithmus für A den Typ von Reduktionen oder Selbstreduktionen auf A vereinfacht. Bekanntestes Ergebnis dieser Art ist: Turing-Reduktionen auf leicht zählbare Sprachen vereinfachen sich zu truth-table-Reduktionen [Beigel, Kummer, Stephan 1995].

Wir können folgendes beweisen:

1. Selbstreduzierbare *leicht* 2-*zählbare* Sprachen sind in P.
   Dies bestätigt eine Vermutung von [BKS95] für den Fall $m = 2$.

2. Selbstreduzierbare $(2m-1, m)$-*verbose* Sprachen sind truth-table-selbstreduzierbar.
   Dies verallgemeinert ein Ergebnis von [BvHT93] für p-selektive Sprachen. (P-selektive Sprachen sind $(m+1, m)$-verbose.)

3. Selbstreduzierbare Sprachen in $\mathrm{P}[\langle sel, xor\rangle]$ sind in P.
   Dies verallgemeinert ein entsprechendes Ergebnis für p-selektive Sprachen von [BvHT93].

4. Disjunktiv selbstreduzierbare Sprachen, die 2-*membership comparable* sind, liegen in UP.

Data Exchange: On the Complexity of Answering Queries with Inequalities

Aleksander Mądry

Institute of Computer Science, University of Wrocław

The *data exchange problem* arises when we require data (called *source instance*) structured under one schema (*source schema*) to be translated into an instance (*target instance*) of a different schema (*target schema*), reflecting the source instance as accurately as possible, i.e. satisfying *source-to-target dependences*. Of course, in most cases there are many valid target instances corresponding to a particular problem – we can think of the solution of this problem as an indefinite database consisting of all possible target instances that are valid. So we can adapt the notion of certain answers used in the theory of incomplete databases for the semantics of query answering in data exchange, i.e. we focus only on those positive answers that hold in every target instance that satisfies the source-to-target dependences. In this paper we consider existential Boolean queries and the *local-as-view* (LAV) setting, which is a widely used, special case of the general data exchange problem setting.

We investigate the complexity of answering such queries. Fagin et al. [2] proved that the certain answers for queries being unions of conjunctive queries can be computed in polynomial time. But when we allow inequalities within queries, then the situation changes. It was shown by Abiteboul et al. [1] that computing the certain answers of unions of conjunctive queries with inequalities is in co-NP. This paper establishes also co-NP-hardness of this problem for conjunctive queries with six inequalities. It has been shown [2] that there is a polynomial-time algorithm for computing the certain answers of unions of conjunctive queries with at most one inequality per disjunct. Thus the minimal number of inequalities giving rise to co-NP-hardness of this problem is at least two (unless P=NP) and six at most. So the problem of precisely determining this number arises. Fagin et al. [2] stated a conjecture that this number equals two. This paper presents a proof of this conjecture, closing the gap in the complexity of computing the certain answers of this kind of queries.

References

[1] S. Abiteboul and O. M. Duschka. Complexity of Answering Queries Using Materialized Views. In *Proceedings of the ACM Symposium on Principles of Database Systems (PODS)*, Seattle, WA, 1998, pages 254-263.

[2] R. Fagin, P. G. Kolaitis, R. J. Miller, L. Popa. Data Exchange: Semantics and Query Answering. Proc. *International Conference on Database Theory (ICDT)*, 2003, pp. 207-224. To appear in *Theoretical Computer Science*.

Online-Algorithmen zur Lastbalanzierung auf dynamischen Netzwerken

Bettina Rehberg

Universität Paderborn
bettina@upb.de

Im Regelfall sind die einzelnen Rechner eines Rechnernetzes (z.B. LAN, W-LAN oder Internet) nicht ständig voll ausgelastet, sondern es stehen Restrechenkapazitäten zur Verfügung. Eine bekannte Idee ist es, diese so genannten Idle-Zeiten für die Berechnung rechenintensiver paralleler Programme zu nutzen.

Hierbei ergibt sich einerseits die Frage, wie die Idle-Zeiten möglichst realitätsnah modelliert werden können, um Online-Algorithmen zu analysieren. Andererseits besteht selbst dann, wenn die Idle-Zeiten bekannt sind, noch das Problem, wie die voneinander unabhängigen Teilprozesse eines parallelen Programms zugewiesen werden sollen, damit das Gesamtprogramm in möglichst kurzer Zeit abgearbeitet werden kann.

S. Leonardi, A. Marchetti-Spaccamela und F. Meyer auf der Heide (*Scheduling against an Adversarial Network*, SPAA 2004) haben ein Modell vorgestellt, das auch die Kosten für Kommunikation und Synchronisation berücksichtigt.

In diesem Modell sind die Ausführungszeiten der einzelnen Teilprozesse jeweils im voraus bekannt. Die Idle-Zeiten werden jedoch durch einen Gegenspieler bestimmt.

Dort werden u.a. Online-Algorithmen für zwei verschiedene Situationen vorgestellt. Das eine Mal werden gleichgroße Jobs und eine schwache Einschränkung an das Verhalten des Gegenspielers untersucht. Das andere Mal werden Jobs mit unterschiedlichen Ausführungszeiten und eine stärkere Einschränkung an das Verhalten des Gegenspielers betrachtet.

In diesem Vortrag wird ein Online-Algorithmus für den Fall der schwachen Einschränkung und unterschiedlicher Ausführungszeiten der Jobs vorgestellt.

Dynamische und *t*-private Auktionen

Markus Hinkelmann

Institut für Theoretische Informatik, Universität zu Lübeck
hinkelma@tcs.uni-luebeck.de

Die bekanntesten Auktionshäuser heutzutage sind wohl *Southeby's* in London oder die Internetplatform *eBay*. Bei einer Auktion sind dort zu jeder Zeit der Höchstbietende (durch Heben der Hand bzw. Nutzername) und sein Gebot öffentlich bekannt. Doch drückt sich das Bedürfnis, die eigene Identität von dem Gebot zu trennen, klar aus: Mittelsmänner geben das Gebot ab oder man benutzt nichtssagende Loginnamen im Netz. Erfahrungsgemäß steigt dieses Bedürfnis mit dem Wert des zu ersteigernden Produkts an.

Bei der Ausschreibung, die ebenfalls eine Art Auktion ist, möchte sich am liebsten kein Mitbewerber von anderen in sein Angebot hineinschauen lassen, könnten doch sonst Geschäftsgeheimnisse offen gelegt werden. Insbesondere gilt dies für den Fall, wenn man die Ausschreibung nicht gewinnt.

Das Ziel unserer Arbeit [3, 1] ist es, außer dem Ergebnis der Auktion keinerlei Wissen im informationstheoretischen Sinn über die Gebote der Bieter preiszugeben. Wir stützen uns auf das kryptographisch 1-private Auktionssystem von Naor, Pinkas und Sumner [2] unter Verwendung von Yaos *garbled circuits* [4]. Wir verwenden neben Bietern und dem Auktionator sogenannte *Auction Issuer*, die die Privatheit der Gebote garantieren sollen.

Unser Auktionssystem ist t-privat, d.h. dass jede Koalition der Größe t kein Wissen über die Geheimnisse der anderen Parteien erlangt, falls die Koalition das Protokoll befolgt (*honest but curious*). Wir präsentieren zwei Protokolle. Das erste benötigt polynomiell in t viele Zufallsbits, jedoch eine quadratische Anzahl an Auction Issuern. Aus der Literatur ist bekannt, dass jede Funktion t-privat mit $2t+1$ Parteien berechnet werden kann. Diese Schranke erreichen wir durch Modifikation unseres ersten Protokolls, jedoch erhöht sich die Zahl der Zufallsbits exponentiell in t.

Ist die Koalition aktiv oder bösartig, können wir zeigen, dass jegliche Manipulation der Kommunikation im ersten Protokoll, die das Auktionsergebnis nicht ändert, keinen Informationsgewinn erbringt.

Literatur

[1] M. Hinkelmann, A. Jakoby, P. Stechert, *Dynamic t-Private Auctions*, Technical Report SIIM-TR-A-05-11, Universität zu Lübeck, 2005

[2] M. Naor, B. Pinkas, R. Sumner, *Privacy Preserving Auctions and Mechanism Design*, 1st ACM Conference on Electronic Commerce, pp. 129–139, 1999.

[3] P. Stechert, *Dynamic Private Auctions*, Diplomarbeit, Institut für Theoretische Informatik, Universität zu Lübeck, 2005

[4] A. C. Yao. *Protocols for secure computations*, 23rd FOCS, pp. 160–164, 1982.

Kryptographisch t-private Auktionen

Nina Moebius

Universität zu Lübeck

In diesem Vortrag soll ein in die Praxis umsetzbares Modell zur privaten Berechnung einer Auktion vorgestellt werden. Hierbei soll es einer Koalition von t an der Auktion beteiligten Parteien nicht möglich sein, zusätzliche Informationen zu gewinnen. Ein Protokoll, bei dem t konspirierende Angreifer zusammen nicht mehr Informationen erhalten als sich aus den Eingaben der Angreifer sowie dem Ergebnis der Berechnung ableiten lassen, bezeichnet man als t-privat. Die hier betrachteten Angreifer sind passiv, d.h. sie folgen der Protokollspezifikation.

M. Naor, B. Pinkas und R. Sumner entwickeln in [3] ein 1-privates Protokoll zur Berechnung einer Auktion, das auf den von A. Yao eingeführten Garbled Circuits basiert [5].

M. Hinkelmann, A. Jakoby und P. Stechert stellen in [1] einen t-privaten Mechanismus zur Berechnung einer Auktion vor. Dieser Algorithmus verwendet ebenfalls Garbled Circuits und nutzt außerdem randomisierende Polynome, deren Idee von Y. Ishai und E. Kushilevitz stammt [2]. Das von ihnen vorgeschlagene Protokoll ist informationstheoretisch sicher, benötigt aber eine sehr große Zahl an zufälligen Bits, so dass eine praktische Umsetzung nicht möglich ist.

Bei der Erstellung eines in dieser Hinsicht verbesserten Protokolls kann durch Zuhilfenahme von kryptographischen Primitiven die Anzahl der Zufallsbits eingeschränkt werden. Die Idee ist deshalb, ein t-privates kryptographisch sicheres Protokoll zur Berechnung einer Auktion zu entwickeln, das ohne randomisierende Polynome auskommt und stattdessen Pseudozufallszahlengeneratoren verwendet.

Literatur

[1] M. Hinkelmann, A. Jakoby, P. Stechert, *Dynamic t-Private Auctions*, Technical Report SIIM-TR-A-05-11, Universität zu Lübeck, 2005

[2] Y. Ishai, E. Kushilevitz, *Perfect Constant-Round Secure Computation via Perfect Randomizing Polynomials*, 29th ICALP, pp. 244–256, 2002.

[3] M. Naor, B. Pinkas, R. Sumner, *Privacy Preserving Auctions and Mechanism Design*, 1st ACM Conference on Electronic Commerce, pp. 129–139, 1999.

[4] P. Stechert, *Dynamic Private Auctions*, Diplomarbeit, Institut für Theoretische Informatik, Universität zu Lübeck, 2005.

[5] A. C. Yao. *Protocols for secure computations*, 23rd FOCS, pp. 160–164, 1982.

Simulationsrelationen als Minimierungsheuristiken für ω-Automaten

Carsten Fritz

Christian-Albrechts-Universität zu Kiel

ω-automata (automata on infinite words) play a central role in model checking when properties are specified in temporal logic. For these model checking procedures to be efficient, it is crucial that the used automata are small, but computing minimum-state automata is PSPACE-hard. Simulation relations, capturing the notion that one automaton state "mimicks" another state, are therefore used as a minimization heuristic. In the talk, we discuss simulation relations for alternating Büchi automata, using a game-theoretical approach. We show how to apply these relations for state space reductions in the automata construction from LTL. If time permits, we outline extensions of this notion to other acceptance modes and their application.

Eingeschränkte Zyklenüberdeckungen

Bodo Manthey

Institut für Theoretische Informatik, Universität zu Lübeck
manthey@tcs.uni-luebeck.de

Eine Zyklenüberdeckung eines Graphen ist eine Menge knotendisjunkter Zyklen, so dass jeder Knoten des Graphen auf genau einem Zyklus liegt. Eine L-Zyklenüberdeckung ist eine Zyklenüberdeckung, bei die Länge jedes Zyklus in der Menge L liegt. Für ungerichtete Graphen ist $L \subseteq \{3, 4, 5, \ldots\} = \mathcal{U}$, für gerichtete Graphen ist $L \subseteq \{2, 3, 4, \ldots\} = \mathcal{D}$. Wir untersuchen das Problem, L-Zyklenüberdeckungen maximalen Gewichts zu berechnen.

Für $L \subseteq \mathcal{U}$ sei Max-L-UCC folgendes Optimierungsproblem: Gegeben sei ein ungerichteter, vollständiger Graph, dessen Kanten mit 0 oder 1 gewichtet sind. Ziel ist es, eine L-Zyklenüberdeckung maximalen Gewichts zu berechnen. Max-W-L-UCC ist wie Max-L-UCC definiert, der einzige Unterschied ist, dass nun beliebige natürliche Zahlen als Gewichte zugelassen sind. Für gerichtete Graphen und $L \subseteq \mathcal{D}$ sind Max-L-DCC und Max-W-L-DCC analog definiert.

Es wird gezeigt, dass es für fast alle L APX-hart ist, L-Zyklenüberdeckungen maximalen Gewichts zu berechnen.

- Max-L-UCC ist APX-hart, falls $\overline{L} = \mathcal{U} \setminus L \not\subseteq \{3, 4\}$. Max-W-$L$-UCC ist APX-hart, falls $\overline{L} \not\subseteq \{3\}$.
- Max-L-DCC und Max-W-L-DCC sind APX-hart, falls $L \neq \mathcal{D}$ und $L \neq \{2\}$.

Andererseits können Max-W-L-UCC und Max-W-L-DCC in polynomieller Zeit mit Faktor $2,5$ bzw. 3 approximiert werden. Dies gilt für alle L, obwohl die meisten Mengen L nicht einmal rekursiv aufzählbar sind.

Gastvortrag

Hashing und Zufallsgraphen

Martin Dietzfelbinger

Technische Universität Ilmenau

Wir betrachten die Situation, die entsteht, wenn zwei Hashfunktionen h_1, h_2 mit Wertebereich $[m] = \{0, \ldots, m-1\}$ auf die Schlüssel einer Menge S (Kardinalität n) angewendet werden. Die (Hyper-)Graph-Struktur $G(S, h_1, h_2)$, die entsteht, wenn man die Elemente von $[m]$ als Knoten und die Mengen $\{h_1(x), h_2(x)\}$ als Kanten auffasst, wurde schon vor längerem als nützlich und interessant identifiziert.

Im Vortrag diskutieren wir, wie man mit recht einfachen, schnell auswertbaren Hashfunktionen (aus einer passenden universellen Klasse zufällig gewählt) erreichen kann, dass $G(S, h_1, h_2)$ ein *annähernd* zufälliger Graph wird. Dies kann benutzt werden, um vollständig zufällige Hashfunktionen platzeffizient zu „simulieren“ [2, 5, 6].

Unter der Annahme, dass reine Zufälligkeit schon vorliegt, kann man eine Hashtabelle bauen, die die Speicherung von n Schlüsseln in Platz $(1+\varepsilon)n$ zulässt, dabei garantiert konstante Suchzeit $O(\log(1/\varepsilon))$ hat — das entspricht der *mittleren erwarteten* Zeit für eine erfolgreiche Suche bei „idealem (uniformem)“ Hashing — und erwartete konstante Einfügezeit aufweist. Dies wurde schon in [4] geleistet. Wir zeigen, dass man mit der Auswertung von zwei Hashfunktionen und Zugriffen auf nur zwei Speicherpositionen auskommt. Hierfür ist eine komplexe Analyse des Zufallsgraphen $G(S, h_1, h_2)$ nötig [3, 7]. Diese Analyse klärt auch das Verhalten des „balanced allocation“-Ansatzes [1] im Offline-Fall.

Für viele Anwendungen lässt sich die Annahme der vollen Zufälligkeit rechtfertigen.

Literatur

[1] Y. Azar, A. Z. Broder, A. R. Karlin, E. Upfal, Balanced Allocations, SICOMP 29 (1999) 180–200.

[2] M. Dietzfelbinger, P. Woelfel, Almost random graphs with simple hash functions, 35th ACM STOC, 2003, pp. 629–638.

[3] M. Dietzfelbinger, C. Weidling, Balanced allocation and dictionaries with tightly packed constant sized bins, 32nd ICALP, 2005, pp. 166–178.

[4] D. Fotakis, R. Pagh, P. Sanders, P. G. Spirakis, Space efficient hash tables with worst case constant access time, 20th STACS, 2003, pp. 271–282.

[5] A. Östlin, R. Pagh, Uniform hashing in constant time and linear space, 35th ACM STOC, 2003, pp. 622-628.

[6] R. Pagh, F. F. Rodler, Cuckoo hashing, J. Algorithms 51 (2004) 122–144.

[7] C. Weidling, Platzeffiziente Hashverfahren mit garantierter konstanter Zugriffszeit, Dissertation, TU Ilmenau, 2004, elektronische Version:
`http://www.db-thueringen.de/servlets/DocumentServlet?id=2431`

Teilnehmer

Jan Arpe	Universität zu Lübeck arpe@tcs.uni-luebeck.de
Frank Balbach	Universität zu Lübeck balbach@tcs.uni-luebeck.de
Monika Demichowicz	University of Wrocław monika@ii.uni.wroc.pl
Martin Dietzfelbinger	Technische Universität Ilmenau martin.dietzfelbinger@tu-ilmenau.de
Carsten Fritz	Christian-Albrechts-Universität zu Kiel fritz@ti.informatik.uni-kiel.de
Jiong Guo	Friedrich-Schiller-Universität Jena guo@minet.uni-jena.de
Markus Hinkelmann	Universität zu Lübeck hinkelma@tcs.uni-luebeck.de
Stephan Holzer	Johannes Gutenberg-Universität Mainz stholzer@students.uni-mainz.de
Günter Hotz	Universität des Saarlandes Saarbrücken hotz@cs.uni-sb.de
Andreas Jakoby	Universität zu Lübeck jakoby@tcs.uni-luebeck.de
Lothar Krause	Universität zu Lübeck lkrause@informatik.uni-luebeck.de
Maciej Liśkiewicz	Universität zu Lübeck liskiewi@tcs.uni-luebeck.de
Alexander Mądry	University of Wrocław a.madry@psz.pl
Bodo Manthey	Universität zu Lübeck manthey@tcs.uni-luebeck.de
Nina Moebius	Universität zu Lübeck moebiusn@informatik.uni-luebeck.de
Arfst Nickelsen	Technische Universität Berlin nicke@cs.tu-berlin.de
Bettina Rehberg	Universität Paderborn bettina@uni-paderborn.de
Rüdiger Reischuk	Universität zu Lübeck reischuk@tcs.uni-luebeck.de
Tiark Rompf	Universität zu Lübeck tr@nachtlicht-media.de

Matthias Schmalz Universität zu Lübeck
schmalz@informatik.uni-luebeck.de

Till Tantau Technische Universität Berlin
tantau@cs.tu-berlin.de

Hagen Völzer Universität zu Lübeck
voelzer@tcs.uni-luebeck.de

Volker Weber Philipps-Universität Marburg
webervo@mathematik.uni-marburg.de

Thomas Wilke Christian-Albrechts-Universität zu Kiel
wilke@ti.informatik.uni-kiel.de