Klaus Ambos-Spies, Bernd Borchert, Wolfgang Merkle,
Jan Reimann, Frank Stephan

38. Workshop über Komplexitätstheorie, Datenstrukturen und effiziente Algorithmen

Heidelberg, 1. Juni 1999

Unterstützt von der Stiftung Universität Heidelberg

38. Workshop über Komplexitätstheorie, Datenstrukturen und effiziente Algorithmen

Heidelberg, 1. Juni 1999

Internationales Wissenschaftsforum, Hauptstraße 242

Programm

ab 8.30	Kaffee
9.25 - 9.30	Begrüßung
9.30 - 9.55	Andre Osterloh: *Sorting on the OTIS-Mesh*
9.55 - 10.20	Markus Nebel: *Die Stackgröße von Tries*
10.20 - 10.45	Elias Dahlhaus: *An Improved Linear Time Algorithm for Minimal Elimination Ordering in Planar Graphs that is Parallelizable*
10.45 - 11.15	Kaffeepause
11.15 - 11.40	Ulrich Hertrampf: *Generalized Regular Counting Classes*
11.40 - 12.05	Christian Schindelhauer: *Ein Baukasten für Mentale Kartenspiele*
12.05 - 14.00	Mittagspause
14.00 - 14.25	Henning Fernau, Rolf Niedermeier: *An Efficient Exact Algorithm for Constraint Bipartite Vertex Cover*
14.25 - 14.50	Rudolf Fleischer, Steve Seiden: *Page Replication — Variations on a Theme*
14.50 - 15.15	Jung-Bae Son, Günter Hotz *Konvexe Hüllen in erwarteter Linearzeit*
15.15 - 15.45	Kaffeepause
15.45 - 16.10	Jens Gramm: *Syntaktische Erkennung NL-vollständiger Probleme*
16.10 - 16.30	Frank Stephan, Thomas Zeugmann: *On the Uniform Learnability of Approximations to Non-Recursive Functions*
16.30	Ende des Workshops

Sorting on the OTIS-Mesh

Andre Osterloh

TU Ilmenau
osterloh@theoinf.tu-ilmenau.de

The Optical Transpose Interconnection System (OTIS) is a hybrid system using optical and electronical interconnections. The processors in the OTIS structure are partitioned into (topologically identical) groups where the connections within the groups are realized by electronic links and the connections among the groups are realized by optical links.

Each processor is indexed by a tuple (G, P), where G is the group index and P is the processor index within the group. The connection of the groups are of the form $[(G, P), (P, G)]$; that is, the group and processor indicies are transposed by an (optical) interconnection. Every group can be realized as mesh, torus, hypercube, etc., resulting in the OTIS-Mesh, OTIS-Torus, OTIS-Hypercube, etc.

An n^4 processor OTIS-Mesh consists of n^2 meshes (groups) of size $n \times n$ which are connected such that the processor (k, l) in mesh (i, j) is connected with processor (i, j) in mesh (k, l) for $1 \leq i, j, k, l \leq n$. So each node in the OTIS-Mesh has maximal degree five and the diameter of the OTIS-Mesh is $4n - 3$.

We study the k-k sorting problem where each processor initially contains k elements and finally receive k elements from a linearly ordered set and the i-th smallest element has to be sent to a memory place indexed by i for a fixed indexing of the n^4 processors, for all i in parallel.

We can show that for k-k sorting $8n + o(n)$ are sufficient for $k \in \{1, 2\}$ and $2kn + o(kn)$ steps for $k \geq 8$. For $k = 1$ this matches the running time of the best previous randomized algorithm. For the case $k \geq 2$ this problem has not been discussed before. The given algorithm can be modified to achieve $4n + o(n)$ steps for $k \in \{1, 2\}$ and $kn + o(kn)$ steps for $k \geq 8$ in the average case. We can further show a lower bound of $\max\{4n - 3, \frac{1}{\sqrt{2}}kn\}$ for k-k sorting on the OTIS-Mesh.

Die Stackgröße von Tries

Markus E. Nebel

Fachbereich Informatik
Johann Wolfgang Goethe-Universität, Frankfurt am Main
nebel@sads.informatik.uni-frankfurt.de

Ein Trie (der Name ist vom engl. *re***trie***val* abgeleitet) ist eine baumförmige Datenstruktur, die es ermöglicht, eine Menge von Daten effizient zu verwalten. Schlüssel werden nur in Blättern des Baumes gespeichert, innere Knoten dienen nur der Verzweigung. In diesem Vortrag befassen wir uns mit der Traversierung von Tries in Preorder. Dabei gehen wir davon aus, daß eine mittels Endrekursions-Beseitigung optimierte rekursive Prozedur verwendet wird. In diesem Fall beschreibt der aus der Literatur bekannte Parameter der Stackgröße die Anzahl an Zellen auf einem Stack, die zur Speicherung der Rücksprungadressen bei der Traversierung benötigt werden.
In diesem Vortrag untersuchen wir die mittlere Stackgröße von Tries in zwei Modellen.
Das erste Modell geht davon aus, daß alle Tries mit α inneren Knoten gleichwahrscheinlich sind. Hier ergibt sich die mittlere Stackgröße asymptotisch zu $\sqrt{\frac{3}{2}\pi\alpha}$. Da sich dieses Ergebnis nur um einen konstanten Faktor von der bekannten mittleren Stackgröße der erweiterten binären Bäume unterscheidet, versuchen wir anschließend mittels quantitativer Untersuchungen einen entsprechenden Zusammenhang herzustellen. Dabei stellt sich jedoch heraus, daß die Existenz eines einfachen Zusammenhangs sehr unwahrscheinlich ist.
Im zweiten Modell betrachten wir alle Tries mit α inneren Knoten und β gespeicherten Schlüsseln als gleichwahrscheinlich. Es gelingt uns auch in diesem Modell eine exakte Asymptotik für die mittlere Stackgröße zu bestimmen. Diese besagt beispielsweise, daß unter der Annahme unseres uniformen Modells dünn besetzte Tries eine merklich schlechte mittlere Stackgröße besitzen. Am Ende des Vortrags zeigen wir, daß es möglich ist, das klassische Resultat von deBruijn, Knuth und Rice zur mittleren Stackgröße erweiterter binärer Bäume direkt aus unserem Ergebnis zum zweiten Modell abzuleiten.

An Improved Linear Time Algorithm for Minimal Elimination Ordering in Planar Graphs that is Parallelizable

Elias Dahlhaus

Institut für Informatik
Universität zu Köln
dahlhaus@informatik.uni-koeln.de

We present an alternative linear time algorithm that computes an ordering that produces a fill-in that is minimal with respect to the subset relation. It is simpler than a previous algorithm of the author (presented at SWAT98) and is easily parallelizable. The algorithm does not rely on the computation of a breadth-first search tree.

Generalized Regular Counting Classes

Ulrich Hertrampf

Abteilung Theoretische Informatik
Universität Stuttgart
hertramp@informatik.uni-stuttgart.de

Complexity classes, which are defined via finite commutative monoids, can be considered as (very) regular counting classes. These include well-known classes like NP, coNP, $\oplus$P, other MOD-classes, but also the classes of finite acceptance type, and many more.

In these cases, the acceptance mechanism can be defined by a regular leaf language, where acceptance really depends only on the number of occurrences of the various letters in the actual leafstring. In other words, the acceptance mechanism is given by a symmetric regular language. Generally all classes described in this way are the so called eventually periodic counting classes.

In this paper we relax the symmetry condition on the regular leaf language: We allow all regular leaf languages, but we admit only machines, which on all input words will only produce symmetric leafstrings, which means all appearing leaf strings will either under all permutations belong to the acceptance language, or under all permutations not belong to the acceptance language.

We give an exact characterization of all complexity classes, which can be described in this manner. It turns out that besides the classes obtained via finite commutative monoids, we also can describe promise classes like UP or MODZ_2P in this way.

Ein Baukasten für Mentale Kartenspiele

Christian Schindelhauer

Institut für Theoretische Informatik
Medizinische Universität zu Lübeck
schindel@tcs.mu-luebeck.de

Mentale Kartenspiele werden zwischen mehreren Personen, ohne vertrauenswürdige dritte Person (z.B. Notar) und natürlich ohne Karten gespielt. Ziel ist es, ein kryptographisches System zu definieren, welches das mentale oder elektronische Kartenspiel genauso sicher implementiert wie das reale (wenn nicht sogar sicherer).

Hierbei sind u.a. folgende Sicherheitsaspekte zu berücksichtigen:

- Das System muß verschiedene Grade der Geheimhaltung gewährleisten (z.B. verdeckter gemischter Kartenstapel, Karten auf der Hand, Karten die für andere verdeckt von einer Person zu einer anderen geschoben werden und aufgedeckte Karten).
- Das System soll sämtliche Betrugs- und Manipulationsmöglichkeiten der Spieler ausschließen.
- Selbst einer beliebig großen Koalition von Spielern darf es nicht möglich sein, die Geheimnisse eines anderen Spielers zu entschlüsseln.
- Die Strategie eines Spielers soll auch nach Beendigung des Spielers anderen nicht bekannt werden. So soll z.B. beim mentalen Poker verhindert werden, nach dem Spiel zu erfahren, ob ein Spieler geblufft hat.

Es ist schon länger bekannt, daß dieses Problem durch Anwendung von Zero-Knowledge-Protokollen im Prinzip gelöst werden kann. Leider ergibt sich daraus noch kein praxistaugliches System, da eine Übertragung dieser theoretischen Ergebnisse weder überschaubar ist, noch ein effizientes Krypto-System zur Folge haben muß.

Bis jetzt ist nur eine brauchbare Lösung für mentales Poker bekannt (C. Crépeau, *A Zero-Knowledge Poker Protocol that Achieves Confidentiality of the Players' Strategy or How to Achieve an Electronic Poker Face*, Crypto'86, pp. 239-247, 1987). Für andere Spiele läßt sich Crépeaus System nicht übertragen: So ist es z.B. nicht möglich, eine ausgespielte Karte wieder in einen Stapel verdeckt einzumischen.

Wir stellen ein allgemeines und sogar effizienteres Krypto-System für mentale Kartenspiele vor. Hierbei wird eine Datenstruktur für Karten eingeführt, die, obgleich sehr einfach, sämtliche Sicherheitsaspekte gewährleistet. Die Protokolle nutzen diese Datenstruktur und stellen einen Wergzeugkasten dar, der direkte sichere Implementation eines beliebigen mentalen Kartenspiels ermöglicht.

Als Operationen stehen unter anderen zur Verfügung: Kartenstapel (neu) mischen, Karte aufnehmen, Karte aufdecken, Karte einem anderen Spieler verdeckt zuschieben und Karte verdeckt in den Stapel schieben. Die Korrektheit und Sicherheit der Operationen wird durch Zero-Knowledge-Protokolle basierend auf der Quadratischen-Reste-Annahme bewiesen.

An Efficient Exact Algorithm for Constraint Bipartite Vertex Cover[1]

Henning Fernau[2], Rolf Niedermeier[3]

Wilhelm-Schickhard-Institut für Informatik
Universität Tübingen
fernau,niedermr@informatik.uni-tuebingen.de

The "Constraint Bipartite Vertex Cover" problem (CBVC for short) is: given a bipartite graph G with n vertices and two positive integers k_1, k_2, is there a vertex cover taking at most k_1 vertices from one and at most k_2 vertices from the other vertex set of G? CBVC is NP-complete. It formalizes the spare allocation problem for reconfigurable arrays, an important problem from VLSI manufacturing.

We provide the first nontrivial so-called "fixed parameter" algorithm for CBVC, running in time $O(1.3999^{k_1+k_2} + (k_1+k_2)n)$. Our algorithm is efficient and practical for small values of k_1 and k_2, as occurring in applications. Despite of the seemingly great similarity between CBVC and Vertex Cover for general graphs, only little ideas developed for Vertex Cover algorithms carry over to CBVC, so several new techniques had to be developed in this work. In particular, we introduce some kind of "bonus system," which may have applications elsewhere.

[1]Extended abstract to appear at *24th International Symposium on Mathematical Foundations of Computer Science (MFCS'99)*, Szklarska Poręba, Poland, September 1999

[2]Partially supported by Deutsche Forschungsgemeinschaft grant DFG La 618/3-2.

[3]Partially supported by a Feodor Lynen fellowship of the Alexander von Humboldt-Stiftung, Bonn, and the Center for Discrete Mathematics, Theoretical Computer Science and Applications (DIMATIA), Prague.

Page Replication — Variations on a Theme

Rudolf Fleischer[1], Steve Seiden[1]

Max-Planck-Institut für Informatik
rudolf@mpi-sb.mpg.de, sseiden@acm.org

In the page replication problem, we are given a weighted graph and a start node s which initially contains a page. Other nodes which want to access this page can do so by sending a request to any other node holding the page. The cost of this access is then the distance between the two nodes. A node can also choose to copy the whole page at a cost of d times the distance, where d is usually a large constant (the page size). If the sequence of requests is not known in advance, we have an online problem so we use competitive analysis to measure the performance of algorithms, i.e., we compare the cost of our algorithm to the cost of the best possible offline algorithm. Various graph topologies (trees, rings, arbitrary graphs) have been studied in this model.

In this talk, we present several variants of the classical page replication problem and give some new upper and lower bounds. In the *continuous page replication problem* we allow requests at and replication to arbitrary points on any edge of the graph. In this model randomization does not help, and the deterministic algorithms are equivalent to randomized algorithms in the classical discrete model. In the *unequal cost model* we assume that the online algorithm has a replication factor different from d, the replication factor of the offline algorithm. We give optimal deterministic and randomized algorithms for the discrete and continuous variant of this model on trees. From this we can derive much simpler proofs for known algorithms on rings.

[1]Both authors were partially supported by the EU ESPRIT LTR Project No. 20244 (ALCOM-IT), WP 3.2. The first author was also supported by a Habilitation Scholarship of the German Research Foundation (DFG).

Konvexe Hüllen in erwarteter Linearzeit

Jung-Bae Son, Günter Hotz

FB Informatik
Universität des Saarlandes
sjubae@cs.uni-sb.de

Im folgenden wird ein Reduktions-Algorithmus zur Berechnung der konvexen Hülle einer Punktmenge im reellen, d-dimensionalen, euklidischen Raum angeben und seine erwartete Laufzeit ermittelt.

Es handelt sich dabei um eine Verallgemeinerung eines Algorithmus von G. Hotz [3] : Zunächst wird in einem Aussiebschritt die Anzahl der Eingabepunkte reduziert, undzwar so, daß die konvexe Hülle der reduzierten Punktmenge identisch ist mit der der Ausgangspunktmenge. Anschließend wird mit einem Algorithmus der worst-case Laufzeit $O(n \log n)$ im R^d, $d \leq 3$, und $O(n^{\lfloor \frac{d}{2} \rfloor})$ im R^d, $d > 3$, die konvexe Hülle der übriggebliebenen Punkte berechnet.

Man kann zeigen, daß das Verfahren bei einer Vielzahl von Riemann-Dichten $f : R^d \to R$ lineare erwartete Laufzeit erreicht. Einige Beispiele sind: Dichten von Gleichverteilungen auf einem d-dimensionalen Hyperquader, Dichten bestimmter rotationssymmetrischer Verteilungen im R^d, Dichten mit $f(x) > 0$ für alle $x \in R^d$, z.B. die Dichte der d-dimensionalen Standard-Normalverteilung.

References

[1] Bentley, J.L.; Clarkson, K.L. und Levine, D.B.: Fast Linear Expected-Time Algorithms for Computing Maxima and Convex Hulls, Algorithmica, Bd.9 - 1993

[2] Golin, M. und Sedgewick, R.: Analysis of a Simple yet Efficient Convex Hull Algorithm, Proceedings of the 4th Annual Symposium on Computational Geometry, 1988

[3] Hotz, Günter: Algorithmische Informationstheorie, B.G. TEUBNER Verlagsgesellschaft, Stuttgart/Leipzig 1997

[4] Jünger, M.; Borgwardt, K.H.; Gaffke, N. und Reinelt, G.: Computing the Convex Hull in the Euclidean Plane in Linear Expected Time, in: Applied Geometry and Discrete Mathematics (Gritzmann, P. und Sturmfels, B. Hrsg.), Bd.4 - 1991

[5] Schulz, Frank: Sortieren und Suchen unter dem Gesichtspunkt der statistischen Informationstheorie, 31. Workshop Komplexitätstheorie, Datenstrukturen und Effiziente Algorithmen (Lautemann, Clemens und Schwentick, Thomas Hrsg.), 1997

Syntaktische Erkennung NL-vollständiger Probleme

Jens Gramm

Wilhelm-Schickard Institut für Informatik
Universität Tübingen
gramm@informatik.uni-tuebingen.de

Vom Standpunkt der Descriptive Complexity aus studieren wir die syntaktische Struktur von Problemen, die vollständig sind für nichtdeterministischen logarithmischen Platz (NL). Das Fernziel eines solchen Studiums ist die Erstellung von systaktischen Regeln, mit denen die Vollständigkeit natürlicher Probleme erkannt werden kann. Liessen sich diese Regeln automatisieren, wäre es möglich, die formale Spezifikation eines Problems automatisch auf Vollständigkeit prüfen zu lassen.

Die Descriptive Complexity geht die Fragen der Komplexität mit Mitteln der Logik an, die Probleme werden mit Formeln einer gegebenen Logiksprache beschrieben. Bisher stand im Mittelpunkt des Interesses, die Mitgliedschaft von Problemen zu einer Klasse zu zeigen. Hier konnten alternative Definitionen für schon bekannte Komplexitätsklassen gegeben werden, etwa ist nach Fagin $NP = SO\exists$ und nach Immerman lassen sich P, NL und L durch Sprachen erster Ordnung charakterisieren, die mit einer bestimmten Art von Transitivem Hüllen-Operator ergänzt werden.

Aber wie sieht es mit der syntaktischen Erkennung von vollständigen Problemen aus? Kann man nicht nur die Mitgliedschaft, sondern auch die Vollständigkeit aus der Formel ablesen? Medina und Immerman begannen, diese Frage für NP zu studieren. In der Suche nach dem 'NP-Anteil' entwickelten sie syntaktische Methoden, um eine Formel zu verändern, ohne die Vollständigkeit zu verletzen. Damit zeigen sie auch, daß bekannterweise NP-vollständige Probleme sogar vollständig via Projektionen erster Ordnung sind. Diese Projektionen sind eine schwache Art von Reduktionen, die sich aus dem Formalismus der Descriptive Complexity ergeben. Aufbauend auf die Arbeit von Medina und Immerman nehmen wir nun eine niedere Klasse, NL, in Augenschein.

Die Klasse NL ist charakterisierbar durch $FO(TC)$, die Sprache erster Ordnung FO, angereichert mit dem Transitiven Hüllen-Operator TC. Immerman zeigte eine Normalform für die Beschreibung von Problemen aus NL: Jedes NL-Problem läßt sich durch eine Formel ausdrücken, die nur eine Anwendung des TC-Operators enthält, der auf eine Projektion erster Ordnung angewendet wird. Durch diese Formel wird gerade das Graphen-Erreichbarkeits-Problem beschrieben, dessen Vollständigkeit via Projektionen erster Ordnung damit bewiesen wird.

Ausgehend von der Formel des Graphen-Erreichbarkeits-Problems versuchen wir die Formeln anderer NL-vollständige Probleme zu erzeugen. Wir entwickeln syntaktische Regeln, mit denen wir die Formel eines NL-vollständigen Problems verändern können ohne die Vollständigkeit zu verletzen. Mit diesen syntaktischen Regeln zeigen wir, daß bekannterweise NL-vollständige Probleme wie *2-SAT*, *Strong Connectivity* oder die Erreichbarkeit von Nonterminalen in einer kontextfreien Grammatik sogar NL-vollständig via Projektionen erster Ordnung sind.

On the Uniform Learnability of Approximations to Non-Recursive Functions

Frank Stephan[1]

Mathematisches Institut
Universität Heidelberg
fstephan@math.uni-heidelberg.de

Thomas Zeugmann[2]

Department of Informatics
Kyushu University, Japan
thomas@i.kyushu-u.ac.jp

Let $\Phi_0, \Phi_1, \ldots$ be a recursive enumeration of the complexity measures of all partial recursive functions. Blum and Blum[3] considered the following class of approximations to the Halting problem K:

$$\mathcal{B} = \{f : (\exists \text{ monotone and total } \Phi_e)\,[f(x) = 1 \Leftrightarrow \Phi_x(x) \leq \Phi_e(x)]\,\}$$

They showed that the class $\mathcal{B}$ is reliably EX-learnable. We carry on these investigations by showing that $\mathcal{B}$ is neither in NUM nor robustly EX-learnable[4]. Since the definition of the class $\mathcal{B}$ is quite natural and does not contain any self-referential coding, $\mathcal{B}$ serves as an example that the notion of robustness for learning is quite *more restrictive* than intended.

Moreover, variants of this problem obtained by approximating any given recursively enumerable set A instead of the halting problem K are studied. All corresponding classes $\mathcal{U}(A)$ are still EX-inferable but may fail to be reliably EX-learnable, for example if A is non-high and hypersimple. Furthermore, $\mathcal{U}(A)$ is not robustly EX-learnable for every non-recursive set A. Using only "slow enumerations" and the corresponding measures, we finally show that for these $\mathcal{U}(A)$ is in NUM if and only if A is recursive.

[1]Supported by the Deutsche Forschungsgemeinschaft (DFG) under grant no. Am 60/9-2.

[2]Supported by the Grant-in-Aid for Scientific Research in Fundamental Areas from the Japanese Ministry of Education, Science, Sports, and Culture under grant no. 10558047.

[3]L. Blum and M. Blum. Towards a mathematical theory of inductive inference. Information and Control, 28:125–155, 1975.

[4]Where the definition of robust EX-learning follows the publication: S. Jain, C. Smith and R. Wiehagen. On the power of learning robustly. In *Proceedings of Eleventh Annual Conference on Computational Learning Theory* (COLT), pages 187–197, ACM Press, New York, 1998.