Sammlung der Zusammenfassungen

der Vorträge auf dem

35. Workshop über Datenstrukturen, effiziente Algorithmen und Komplexitätstheorie

am 9. Juni 1998

in Paderborn

Organisation:

Ben Juurlink, Friedhelm Meyer auf der Heide, Kay Salzwedel, Rolf Wanka

35. Workshop über Komplexitätstheorie,
Datenstrukturen und effiziente Algorithmen

Paderborn, 9. Juni 1998, Gebäude F, Raum F0.530

Programm

ab 8:45	IMBISS
9:25 – 9:30	BEGRÜSSUNG
9:30 – 9:55	Stefan Lucks, Rüdiger Weis: *Zufallsorakel und asymmetrische Verschlüsselung*
9:55 – 10:20	Andreas Jakoby, Maciej Liśkiewicz, Rüdiger Reischuk: *Scheduling Dynamic Graphs*
10:20 – 10:45	Matthias Fischer, Tamás Lukovszki, Martin Ziegler: *Geometric Searching in Walkthrough Animations with Weak Spanners in Real Time*
10:45 – 11:00	PAUSE
11:00 – 11:25	Martin Mundhenk: *Harte Instanzen*
11:25 – 11:50	Henning Fernau, Rolf Niedermeier: *Zur Rekonfigurierung von VLSI-Chips*
11:50 – 12:15	Alfons Avermiddig, Manfred Kunde, Andre Osterloh: *Routing Algorithms on the Multi-Mesh with Application to Matrix Transpose*
12:15 – 14:00	MITTAGSPAUSE und Mitgliederversammlung der GI-Fachgruppe 0.1.3
14:00 – 14:25	Ingo Althöfer, Walter Wenzel: *K-Best Solutions under Distance Constraints: The Model and Exemplary Results for Matroids and Dynamic Programming*
14:25 – 14:50	Carsten Damm: *Boolesche vs. modulare Arithmetik für Schaltkreise und Kommunikationsprotokolle*
14:50 – 15:15	Manindra Agrawal, Thomas Thierauf: *The Satisfiability Problem for Probabilistic Ordered Branching Programs*
15:15 – 15:30	PAUSE
15:30 – 15:55	Thomas Erlebach, Klaus Jansen: *Maximierung der Anzahl akzeptierter Verbindungsanfragen in optischen Netzwerken*
15:55 – 16:20	Eric Allender, Klaus Reinhardt: *Isolation, Matching, und Zählen*
16:20 – 16:45	Andreas Goerdt: *Zufällige reguläre Graphen mit defekten Kanten*
16:45	ENDE DES WORKSHOPS

Zufallsorakel und asymmetrische Verschlüsselung

Stefan Lucks
Theoretische Informatik
Universität Mannheim
68131 Mannheim, A5

Rüdiger Weis
Praktische Informatik IV
Universität Mannheim
68131 Mannheim, A5

lucks@th.informatik.uni-mannheim.de
ruediger.weis@rz.uni-mannheim.de

Eine Funktion $f : \mathrm{In}_f \longrightarrow \mathrm{Out}_f$ ist eine *Einwegfunktion*, falls es eine Darstellung von f gibt, die es erlaubt, für jeden Wert $x \in \mathrm{In}_f$ den Funktionswert $F(x)$ zu berechnen, während es praktisch unmöglich ist, f umzukehren, also zu zu einem Wert $y \in \mathrm{Out}_f$ einen Wert x zu finden mit $f(x) = y$. Eine Einwegfunktion heißt *Falltürfunktion*, falls es eine weitere Beschreibung von f gibt, die sog. *Falltür-Information*, die es erlaubt, die Umkehrung von f effizient zu berechnen. (Die bekannte RSA-Funktion $\mathrm{RSA}_{e,n}(x) = x^e \bmod n$ ist vermutlich eine Falltür-Funktion; als Falltür-Information dienen die Primfaktoren von n.)

Die Existenz von Falltür-Funktionen ist notwendig für *sichere asymmetrische Verschlüsselung*. Wichtig ist in diesem Zusammenhang jedoch auch, wie eine zu verschlüsselnde Nachricht in die Defintionsmenge In_f eingebettet wird. Es genügt im allgemeinen nicht, die Nachricht M auf beliebige umkehrbare Weise als Wert in In_f darzustellen. Geeignete Einbettungsverfahren sind in der Theorie bekannt, gelten in der Praxis aber meist als zu ineffizient.

Das „Zufallsorakel-Modell“ [1] von Bellare und Rogaway erlaubt Sicherheitsbeweise auch für vergleichsweise effiziente Einbettungsmethoden. Ziel eines Sicherheitsbeweises im Sinn der *konkreten Sicherheit* ist der Nachweis eines möglichst engen Zusammenhangs zwischen einem erfolgreichen Angriff auf ein Verschlüsselungsschema und einem Angriff auf die verwendeten kryptographischen Bausteine, z.B. auf die Falltür-Funktion f.

Wir untersuchen ein entsprechendes Einbettungsverfahren. Bezüglich seiner konkreten Sicherheit ist unser Verfahren den besten bisher bekannten Einbettungsverfahren [2] überlegen.

Literatur

[1] M. Bellare, P. Rogaway: “Random oracles are practical: a paradigm for designing efficient protocols,” Crypto 94, Springer LNCS 839.

[2] M. Bellare, P. Rogaway: “Optimal asymmetric encryption – how to encrypt with RSA,” Eurocrypt 94, Springer LNCS 950.

Für aktuelle Versionen von [1, 2] siehe `http://www.cs.ucdavis.edu/~rogaway/`.

Scheduling Dynamic Graphs*

Andreas Jakoby[1] Maciej Liśkiewicz[2] Rüdiger Reischuk[1]

[1]Med. Universität zu Lübeck
[2]Universität Tübingen

In parallel and distributed computing scheduling low level tasks on the available hardware is a fundamental problem. Traditionally, one has assumed that the set of tasks to be executed is known beforehand. Then the scheduling constraints are given by a *precedence graph.* Nodes represent the elementary tasks and edges the dependencies among tasks. This static approach is not appropriate in situations where the set of tasks is not known exactly in advance, for example, when different options how to continue a program may be granted.

In this paper a new model for parallel and distributed programs, the *dynamic process graph,* will be introduced, which represents all possible executions of a program in a compact way. The size of this representation is small – in many cases only logarithmically with respect to the size of any execution. An important feature of our model is that unlike precedence graphs, the encoded executions are directed acyclic graphs having a "regular" structure that is typical of parallel programs. Dynamic process graphs embed constructors for parallel programs, synchronization mechanisms as well as conditional branches. With respect to such a compact representation we investigate the complexity of different aspects of the scheduling problem: the question whether a legal schedule exists at all and how to find an optimal schedule. Our analysis takes into account communication delays between processors exchanging data.

Precise characterization of the computational complexity of various variants of this compact scheduling problem will be given in this paper. The results range from easy, that is NL-complete, to very hard, namely $NEXPTIME$-complete.

*supported by DFG Research Grant Re 672/2

[1]Institut für Theoretische Informatik, {jakoby|reischuk}@informatik.mu-luebeck.de

[2]Wilhelm-Schickard Institut für Informatik, liskiewi@informatik.uni-tuebingen.de, on leave from Instytut Informatyki, Uniwersytet Wrocławski

Geometric Searching in Walkthrough Animations with Weak Spanners in Real Time

Matthias Fischer Tamás Lukovszki Martin Ziegler

Heinz Nixdorf Institute
Paderborn University
33095 Paderborn, Germany

{mafi|talu|ziegler}@uni-paderborn.de

We study algorithmic aspects in the management of geometric scenes in interactive walkthrough animations. We consider arbitrarily large scenes consisting of unit size balls. For a smooth navigation in the scene we have to fulfill hard real time requirements. Therefore, we need algorithms whose running time is independent of the total number of objects in the scene and that use as small space as possible. In this work we focus on one of the basic operations in our walkthrough system: reporting the objects around the visitor within a certain distance.

Previously a randomized data structure was presented that supports reporting the balls around the visitor in an output sensitive time and allows insertion and deletion of objects nearly as fast as searching. These results were achieved by exploiting the real volume of the balls and the continuous motion of the visitor. A serious disadvantage of the aforementioned data structure is a big space overhead and the use of randomization.

Our first result is a construction of weak spanners that leads to an improvement of the space requirement of the previously known data structures. Then we develop a deterministic data structure for the searching problem in which insertion of objects are allowed. Our incremental data structure supports $O(1+k)$ reporting time, where k is a certain quantity close to the number of reported objects. The insertion time is similar to the reporting time and the space is linear to the total number of objects.

Harte Instanzen

Martin Mundhenk

Universität Trier
FB IV – Informatik

mundhenk@ti.uni-trier.de

Der Begriff der *Instanzen-Komplexität* wurde von Orponen, Ko, Schöning, and Watanabe (*JACM 1994*) als Maß für die individuelle Komplexität einzelner Instanzen von Entscheidungsproblemen eingeführt. Durch den Vergleich von Instanzen- mit Kolmogoroff-Komplexität entstand der Begriff von *p-harten Instanzen.* Orponen et al. vermuten, daß jede Menge außerhalb von P unendlich viele *p*-harte Instanzen haben muß (IC-Vermutung). Fortnow und Kummer (*TCS 1996*) bewiesen eine etwas schwächere Vermutung für "honest" NP-harte Mengen. Die Frage, ob man durch Weglassen der Ressourcen-Schranken aus der IC-Vermutung eine Charakterisierung der rekursiven Mengen erhält, wurde von Kummer (*Structures 1995*) negativ beantwortet.

Wir haben eine Abschwächung der IC-Vermutung gesucht, die wir beweisen können und die sich von bekannten Begriffen unterscheidet. Dazu müssen wir einen schwächeren Begriff harter Instanzen einführen. Ohne Ressourcen-Schranken lassen sich damit die rekursiv aufzählbaren und die rekursiven Mengen charakterisieren. Mit entsprechenden Ressourcen-Schranken erhalten wir eine Charakterisierung von P. Wir zeigen, daß harte Instanzen einen Komplexitätskern bilden (eingeführt von Lynch (*JACM 1975*)). Allerdings ist unser Begriff harter Instanzen wesentlich strenger: es gibt Mengen mit dichten Komplexitätskernen, aber nur dünnen harten Instanzen. Trotzdem zeigen wir, daß keine NP-harte Menge nur dünne harte Instanzen haben kann, falls P$\neq$NP.

Die Arbeit findet man im Web unter
www.informatik.uni-trier.de/~mundhenk/papers/inst.ps

Zur Rekonfigurierung von VLSI-Chips

Henning Fernau[1]

Wilhelm-Schickard-Institut für Informatik
Universität Tübingen

Rolf Niedermeier[2]

Center for Discrete Mathematics,
Theoretical Computer Science,
and Applications (DIMATIA), Prag

{fernau|niedermr}@informatik.uni-tuebingen.de

In diesem Vortrag soll gezeigt werden, wie die von Downey, Fellows und anderen entwickelten Methoden der "fixed parameter complexity" zur Entwicklung von Algorithmen benutzt werden können, die zur Maximierung der Ausbeute in der Fertigung von VLSI-Chips ihre Anwendung finden.

Vornehmlich betrachten wir das folgende Rekonfigurierungsproblem: Gegeben sei ein (fertigungstechnisch bedingt i. allg. fehlerbehafteter) VLSI-Chip mit $n_1 \times n_2$ vielen identischen gitterartig verknüpften Elementen (z.B. Speicherbausteinen), auf dem zusätzlich k_1 bzw. k_2 als fehlerfrei angenommene Reservezeilen bzw. -spalten integriert sind. Durch Austausch von fehlerbehafteten Zeilen (bzw. Spalten) durch fehlerfreie Zeilen (bzw. Spalten) soll nun der Chip möglichst zu einem voll funktionsfähigen Chip gemacht werden.

Abstrakt betrachtet behandeln wir dabei folgende, CBVC (constraint bipartite vertex cover) genannte Abart des Knotenüberdeckungsproblems: Gegeben seien ein paarer Graph $G = (V_1 \cup V_2, E)$ sowie Schranken k_1, k_2. Gefragt ist, ob es eine Überdeckung $C = C_1 \cup C_2$ (d.h., jeder Knoten in $V_1 \cup V_2$ liegt bereits in C oder ist zu irgendeinem Knoten in C unmittelbar benachbart) von G gibt derart, daß $C_i \subseteq V_i$ und $|C_i| \leq k_i$ für $i = 1, 2$ gilt.

Kuo und Fuchs (*IEEE Design and Test*, **4**:24–31, 1987) zeigten, daß das CBVC Problem NP-vollständig ist, während ja das allgemeine Knotenüberdeckungsproblem für paare Graphen in polynomieller Zeit lösbar ist. Wir gelangen zu einem deterministischen Algorithmus, der $O((k_1 + k_2)n + (1.47)^{k_1+k_2} k_1 k_2)$ Zeit benötigt (n ist die Graphengröße). Da in der Praxis k_1 und k_2 (die der Zahl der Reservezeilen bzw. -spalten entsprechen) sehr klein gegenüber n sind, ist es durchaus möglich, diese Algorithmen zur erschöpfenden Suche einzusetzen.

[1] gefördert durch DFG La 618/3-2.
[2] gefördert durch die Alexander von Humboldt-Stiftung.

Routing Algorithms on the Multi-Mesh with Application to Matrix Transpose[1]

Alfons Avermiddig Manfred Kunde Andre Osterloh

TU Ilmenau
PF 10 05 65
D-98684 Ilmenau, Germany

{aaver|kunde|osterloh}@theoinf.tu-ilmenau.de

We present routing algorithms on the multi-mesh. The multi-mesh is a 4-dimensional torus like architecture with n^4 nodes and a constant degree of only 4, whereas the degree of the 4-dimensional torus with n^4 nodes is 8. The network consists of n^2 meshes of size $n \times n$ which are connected by the free marginal links of the meshes.

We can show that for off-line routing only $8n-9$ steps are sufficient for $k=1$ and $2.5kn+o(kn)$ steps for $k \geq 4$. This algorithm can be transformed in such way that it needs only $13n-9$ steps in the restricted one-packet model, where at every step at most one packet is at each processor. By using some of the methods developed in the context with off-line routing we were also able to improve the results for on-line routing. The algorithms need only $25.5n$ steps for 1-1 routing and $7.25kn$ steps for k-k routing, $k \geq 8$. These results are also valid for k-k sorting.

The off-line results demonstrate that the multi-mesh has a relatively good ability for routing. In contrast to the ordinary mesh it is still an open question whether on-line routing can be done as fast as off-line routing.

Some of the methods of the off-line routing algorithm can be applied to the problem of matrix transposition. A new algorithm is presented which needs only $5n$ steps, a significant improvement to the so far best known results of $8n-4$ steps.

[1]This research was supported in part by the DFG-Project Ku 658/8–3

K-Best Solutions under Distance Constraints: The Model and Exemplary Results for Matroids and Dynamic Programming

Ingo Althöfer Walter Wenzel

Fakultät für Mathematik und Informatik
Friedrich-Schiller-Universität Jena
07740 Jena, Germany

althofer@mipool.uni-jena.de
wawenzel@minet.uni-jena.de

Consider a discrete maximization problem $f : M \to \mathbb{R}$. Typically one wants to find some $x \in M$ with $f(x) = \max\{f(y) \mid y \in M\}$. However, in several topics like "alignment of RNA- or DNA-strings," "automatic speech recognition," and "computer chess," people have been asking for finding not only the best but the k best solutions. Here k is a natural number greater than 1.

More precisely, k distinct solutions $x_1, x_2, \ldots, x_k$ in M have to be determined, such that

$$f(x_1) \geq f(x_2) \geq \ldots \geq f(x_k) \geq f(y) \quad \text{for all} \quad y \quad \text{in} \quad M - \{x_1, \ldots, x_k\}.$$

One important motivation for searching the k best and not only a single best solution comes from the modelling process:

(i) Often some constraints of the original problem are difficult to specify. In this case you may simply omit these difficult constraints and solve the (simpler) remaining problem in a k-best mode. Among the k solutions you choose the best one which satisfies also the omitted constraints. Of course this will not always work, for instance, when the original problem is unsolvable. The hope however is that for k large enough the approach works sufficiently often.

(ii) Sometimes you simply forget some constraints. When you finally get k best solutions, there is the chance that at least some of them fulfill also these forgotten conditions.

Frequently the k best solutions do not help much more than the best solution alone would do. This happens particularly, when the second, third, ..., k-th best are merely copies of the best solution with some small mutations. Especially human decision makers do not like when their alternatives are too similar to each other. Also, similar solutions often have the disadvantage that either all or none of them fulfill additional constraints (for instance those that had been forgotten, see (ii)).

In computer chess, several commercial programs have a k-variation mode: not only the best but the k best moves (according to the heuristic criteria of the program) are computed. Settings with $k = 2$ or 3 are widely used for analysing purposes. Often all these k proposals have the same weak spot(s) due to some bias of the program.

Taking into consideration such practical experiences with similarity problems, it is quite natural to look at the following modification of the k-best task:

Find k best solutions $x_1, \ldots, x_k$ under the additional constraint that distance $(x_i, x_j) \geq d^* \quad$ for all $\quad 1 \leq i < j \leq k$.

Here d^* is an appropriate constant > 0.

Some points have to be made more precise in this setting. First of all an appropriate distance function on M has to exist. Secondly there are several possibilities to define "k-best with distances $\geq d^*$":

(α) x_1 is a best solution in M.
x_2 is a best solution in $M' = \{y \mid d(x_1, y) \geq d^*\}$.
...
x_k is a best solution in $\{y \mid \min\{d(x_1, y), \ldots, d(x_{k-1}, y)\} \geq d^*\}$.

(β) Maximize $\frac{1}{k} \sum_{i=1}^{k} f(x_i)$.

(γ) Maximize $\min\{f(x_1), \ldots, f(x_k)\}$.

Scenario (β) may be appropriate if the boss (= the person, who has the final choice among the k candidates) decides completely at random. (γ) would be a conservative criterion, if the boss is expected to make his final choice under the influence of Murphy's law.

(δ) More generally, one may investigate arbitrary **symnotone** optimization criteria for the k-tuples, i.e., criteria which are both **sym**metric and componentwise mo**notone** in $(f(x_1), \ldots, f(x_k))$.

In this talk we present basic results for matroids and dynamic programming.

References

[AW97] I. Althöfer and W. Wenzel, 2-Best Solutions under Distance Constraints: The Model and Exemplary Results for Matroids. Technical Report Math/Inf/97/17, FSU Jena.

[AW98] I. Althöfer and W. Wenzel, k-Best Solutions under Distance Constraints in Valuated Δ-Matroids. Technical Report Math/Inf/98/14, FSU Jena.

Boolesche vs. modulare Arithmetik für Schaltkreise und Kommunikationsprotokolle

Carsten Damm

Universität Trier, Abteilung Informatik
54296 Trier
damm@uni-trier.de

Wir vergleichen 2 Berechnungsmodelle, die in der Literatur in einer Booleschen und in einer analogen, auf Restklassenarithmetik beruhenden Fassung untersucht wurden. Wir zeigen, daß in beiden Fällen die arithmetische Version die Boolesche bis zu einem gewissen Grade simulieren kann.

Das erste Resultat betrifft semi-unbeschränkte Schaltkreise. Diese bestehen aus *AND*-Gattern beschränkten Grades sowie im Booleschen bzw. arithmetischen Fall aus *OR*-Gattern bzw. *PARITY*-Gattern unbeschränkten Grades (Negationen sind nur an den Eingängen erlaubt). Semi-unbeschränkte Schaltkreise logarithmischer Tiefe und polynomieller Größe charakterisieren genau die Probleme, die sich durch logspace-Reduktionen auf kontextfreie Sprachen reduzieren lassen. Gál und Wigderson haben mit einer randomisierten Konstruktion gezeigt, daß das Boolesche Modell durch das arithmetische Modell simuliert werden kann. Dabei wächst bei einem Schaltkreis der Größe s die Tiefe von d auf $3d + \log n + \log s + O(1)$. Wir beweisen die Existenz einer Simulation, die die Tiefe nur auf $2d + \log d + \log n + O(1)$ wachsen läßt, unabhängig von der Größe des Schaltkreises. Unsere Konstruktion hat neben ihrer Einfachheit den weiteren Vorteil, daß sie mit weniger Zufallsbits auskommt als die von Gál und Wigderson angegebene.

Das zweite Resultat betrifft nichtdeterministische und modulare Kommunikationsprotokolle — Modelle die im Zusammenhang mit unteren Schranken für Schaltkreise untersucht wurden. Es gibt Beispiele von Funktionen, deren nichtdeterministische Kommunikationskomplexität exponentiell größer ist als ihre Parity-Kommunikationskomplexität und umgekehrt [1]. Wir können jedoch zeigen, daß es zu einer Funktion f mit nichtdeterministischer Kommunikationskomplexität t zu jedem $\varepsilon > 0$ eine Funktion g gibt, die sich von f nur auf einem ε-Anteil aller Eingaben unterscheidet und deren Parity-Kommunikationskomplexität höchstens $\log(1/\varepsilon) \cdot (t+1)$ ist.

Literatur

[1] Carsten Damm, Matthias Krause, Christoph Meinel, and Stephan Waack. On Relations Between Counting Communication Complexity Classes. *Journal on Computer System Sciences* (to appear).

[2] Anna Gál and Avi Wigderson. Boolean complexity classes vs. their arithmetic analogs. *Random Structures and Algorithms.* John Wiley & Sons, Inc., 1996. *see also:* Electronic Colloquium on Computational Complexity, Report 95-49, http://www.eccc.uni-trier.de/eccc/, 1995.

The Satisfiability Problem for Probabilistic Ordered Branching Programs

Manindra Agrawal
Dept. of Computer Science
Indian Institute of Technology

Thomas Thierauf
Fachbereich Mathematik/Informatik
Universität Paderborn

We show that the satisfiability problem for bounded error probabilistic ordered branching programs is **NP**-complete. If the error is very small however (more precisely, if the error is bounded by the reciprocal of the width of the branching program), then we have a polynomial-time algorithm for the satisfiability problem.

Maximierung der Anzahl akzeptierter Verbindungsanfragen in optischen Netzwerken

Thomas Erlebach
TU München
erlebach@in.tum.de

Klaus Jansen
IDSIA Lugano
klaus@idsia.ch

In optischen Netzwerken mit Wellenlängen-Multiplexing können verschiedene logische Verbindungen gleichzeitig dasselbe Glasfaserkabel benutzen, sofern die Signale auf Laserstrahlen verschiedener Wellenlängen übertragen werden. Die Anzahl zur Verfügung stehender Wellenlängen ist jedoch durch physikalische Gegebenheiten begrenzt. Wir untersuchen das Problem, aus einer gegebenen Menge von Verbindungsanfragen in einem optischen Netzwerk mit Baumtopologie eine maximal große Teilmenge auszuwählen, so daß die zur Verfügung stehenden Wellenlängen ausreichen, um alle Verbindungsanfragen in dieser Teilmenge gleichzeitig zu erfüllen. Dabei betrachten wir sowohl die Variante ohne Wellenlängen-Konvertierung (Problem MaxPC), bei der für jede akzeptierte Verbindung auf dem gesamten Pfad vom Sender zum Empfänger dieselbe Wellenlänge verwendet werden muß, als auch die Variante mit vollständiger Wellenlängen-Konvertierung (Problem MaxPP).

Die Eingabe für das betrachtete Optimierungsproblem besteht aus einem Baum $T = (V,E)$, einer Liste P von gerichteten einfachen Pfaden in T und einer ganzen Zahl W, die die Anzahl zur Verfügung stehender Wellenlängen angibt. Mit Δ bezeichnen wir den maximalen Grad von T. Die Ausgabe besteht bei MaxPC aus einer Teilmenge P' von P und einer Zuordnung von höchstens W Farben (Wellenlängen) zu den Pfaden in P', so daß Pfade mit derselben Farbe keine gemeinsame Kante in derselben Richtung benutzen. Bei MaxPP besteht die Ausgabe aus einer Teilmenge P' von P, so daß durch keine Kante von T in einer Richtung mehr als W Pfade aus P' laufen. Ziel ist jeweils die Maximierung der Kardinalität von P'.

Wir zeigen, daß MaxPC und MaxPP in polynomieller Zeit gelöst werden können, wenn entweder T ein Baum der Höhe 1 ist oder wenn sowohl W als auch Δ konstant beschränkt sind. Für $W = 1$ und beliebiges Δ oder für durch eine Konstante ≥ 3 beschränktes Δ und beliebiges W sind MaxPC und MaxPP dagegen *NP*-hart.

Ferner präsentieren wir Approximationsalgorithmen für die *NP*-harten Varianten: $(5/3+\varepsilon)$-Approximationen für MaxPC und MaxPP im Fall $W = 1$ für jedes feste $\varepsilon > 0$, eine 2-Approximation für MaxPP bei beliebigem W, eine 1.58-Approximation für MaxPC bei beliebigem W und konstant beschränktem Δ, und eine 2.22-Approximation für MaxPC bei beliebigem W und Δ.

Isolation, Matching, und Zählen[1]

Eric Allender

Department of Computer Science
Rutgers University
P.O. Box 1179
Piscataway, NJ 08855-1179, USA

Klaus Reinhardt

Wilhelm-Schickhard Institut für Informatik
Eberhard-Karls-Universität Tübingen
Sand 13
72076 Tübingen

allender@cs.rutgers.edu
reinhard@informatik.uni-tuebingen.de

Wir zeigen, daß das Problem, ob ein Graph ein perfektes Matching hat, nichtuniform in der Komplexitätsklasse SPL liegt, was eine bessere obere Schranke für dieses Problem liefert. (nonuniform SPL := $\{A : \chi_A \in \text{GapL/poly}\}$.) Hierzu verwenden wir die Methode aus [MVV87] um sicherzustellen, daß unter einer der durch die Advicefunktion gelieferten Gewichtsfunktionen das minimale Matching eindeutig wird. Mit Hilfe der 'clow' Sequenzen aus [MV97] konstruieren wir eine GapL/poly - Funktion, die 0 ist, wenn der Graph ein perfektes Matching besitzt und 1 sonst.

Für die Konstruktionsprobleme maximales Matching und maximaler Fluss mit unären Gewichten zeigen wir (in Analogie zu [KUW86], wo Enthaltensein in Random-NC gezeigt wurde), daß sie in der entsprechenden Funktionenklasse nonuniform FSPL liegen.

Auf ähnliche Weise wie in [RA97] zeigen wir daß NL und die Klasse LogFew aus [BDHM92] in ihrer nichtuniformen Version gleich sind.

Auch liefern wir Indizien dafür, daß unsere Ergebnisse möglicherweise auch im uniformen Fall gelten.

Literatur

[BDHM92] Gerhard Buntrock, Carsten Damm, Ulrich Hertrampf, and Christoph Meinel. Structure and importance of logspace-MOD class. *Math. Systems Theory*, 25:223–237, 1992.

[KUW86] R.M. Karp, E. Upfal, and A. Wigderson. Constructing a perfect matching is in random NC. *Combinatorica*, 6(1):35–48, 1986.

[MV97] M. Mahajan and V. Vinay. Determinant: Combinatorics, algorithms, and complexity. *Chicago Journal of Theoretical Computer Science*, (5), 1997.

[MVV87] K. Mulmuley, U. Vazirani, and V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7:105–113, 1987.

[RA97] K. Reinhardt and E. Allender. Making nondeterminism unambiguous. In *38 th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 244–253, 1997.

[1] `ftp://ftp.eccc.uni-trier.de/pub/eccc/reports/1998/TR98-019/index.html` erscheint auch in Computational Complexity 1998

Zufällige reguläre Graphen mit defekten Kanten

Andreas Goerdt

TU Chemnitz
Theoretische Informatik

goerdt@informatik.tu-chemnitz.de

Sei G ein gegebener Graph (z.B. das Modell eines Kommunikationsnetzwerkes) mit statischen Kantendefekten: Jede Kante des Graphen ist mit der Wahrscheinlichkeit p vorhanden (bzw. mit der Fehlerwahrscheinlichkeit $f = 1 - p$ nicht vorhanden). Im Speziellen betrachten wir den Fall, daß G zufällig aus den d-regulären Graphen gewählt wurde. Wir zeigen zwei Resultate:

Ist der Grad d fest, so ist $p/(d-1)$ der Schwellwert für die Existenz einer linear großen Komponente in fast allen zufälligen regulären Graphen mit Kantenfehlern. Wir zeigen weiter: Wenn jede Kante eines *beliebigen* Graphen G mit maximalem Grad d mit der Wahrscheinlichkeit $p = \lambda/(d-1)$ $(\lambda < 1, \text{fest})$ auftritt, dann hat der Graph G mit Kantenfehlern mit hoher Wahrscheinlichkeit nur Komponenten, deren Größe logarithmisch in der Knotenanzahl ist. Ist G andererseits ein d-regulärer Graph mit Kantenwahrscheinlichkeit $p = \lambda/(d-1)$ $(\lambda > 1)$, dann enthalten fast alle Graphen G mit Kantenfehlern eine linear große Komponente. Diese Resultate implizieren eine Art Optimalität der zufälligen regulären Graphen in Bezug auf die Klasse der Graphen mit beschränktem Grad.

Sei $d \geq 42$, fest und $p = \kappa/d$, $\kappa \geq 20$, dann enthalten fast alle d-regulären Graphen G eine linear große Komponente, welche einen Expander darstellt. Dieser Subgraph kann mit einem einfachen Algorithmus in linearer Zeit gefunden werden.

Diese Resultate beantworten offene Fragen, die sich aus einem Artikel von Nikoletseas und Spirakis ergeben. Derartige Resultate sind von Bedeutung, um die effiziente Simulation des fehlerfreien im fehlerhaften Kommunikationsnetzwerk sicherzustellen.