Georg-August-Universität Göttingen

Institut für Numerische
und Angewandte Mathematik

Zusammenstellung der Abstracts

29. Workshop

Komplexitätstheorie, Datenstrukturen und Effiziente Algorithmen

25. Juni 1996 in Göttingen

Inhaltsverzeichnis

Nicolò Cesa-Bianchi, Paul Fischer, Eli Shamir, Hans Ulrich Simon
Randomisierte Hypothesen helfen beim Lernen aus verrauschten Beispielen 1

Andreas Birkendorf, Norbert Klasner, Hans Ulrich Simon, Eli Dichterman, Jeffrey Jackson
Die Lernbarkeit Boolescher Konzepte im Restricted-Focus-of-Attention Lernmodell 2

Stefan Lucks
Unbalancierte Luby-Rackoff Chiffren 3

Claudia Bertram-Kretzberg, Hanno Lefmann
The Algorithmic Aspects of Uncrowded Hypergraphs 4

Manfred Kunde, Kay Gürtzig
Efficient h-h Sorting and Routing on Constrained Reconfigurable Meshes 5

Detlef Sieling
Variablenordnungen und die Größe von OBDDs für partiell symmetrische Boolesche Funktionen 6

Rolf Niedermeier, Peter Sanders
On the Manhattan-Distance Between Points on Space-Filling Mesh-Indexings 7

Jörg Rothe, Lane A. Hemaspaandra
Characterizations of the Existence of Partial and Total One-Way Permutations 8

Klaus Reinhardt
Strikt sequentielle P-Vollständigkeit 9

Klaus Schröder
Routing on Networks of Optical Crossbars 10

Noga Alon, Phillip G. Bradford, Rudolf Fleischer
Sortieren von Schrauben und Muttern 11

Artur Czumaj, Przemysława Kanarek, Mirosław Kutyłowski, Krzysztof Loryś
Fast Generation of Random Permutations via Networks Simulation 12

Armin Bäumker, Wolfgang Dittrich, Friedhelm Meyer auf der Heide, Ingo Rieping
Realistic Parallel Algorithms: Priority Queue Operations and Selection for the BSP* Model 13

Bernd Borchert, Antoni Lozano
Ressource-Bounded Computational Concepts versus Boolean Concepts 14

Programm 15

Randomisierte Hypothesen helfen beim Lernen aus verrauschten Beispielen

Nicolò Cesa-Bianchi
DSI, Università di Milano
Via Comelico 39,
I-20135 Milano, Italy
cesabian@dsi.unimi.it

Paul Fischer
Lehrstuhl Informatik II
Universität Dortmund
D-44221 Dortmund, Germany
paulf@goedel.informatik.uni-dortmund.de

Eli Shamir
Hebrew University
Jerusalem, Israel
shamir@cs.huji.ac.il

Hans Ulrich Simon
Lehrstuhl Informatik II
Universität Dortmund
D-44221 Dortmund, Germany
simon@goedel.informatik.uni-dortmund.de

Das sogenannte PAC-Lernmodell (*probably approximately correct*) untersucht Lernszenarien mit einem passiven Lerner, der nur beobachten, aber keine Fragen stellen kann. Die Beobachtungen werden als fehlerfrei vorausgesetzt. Bekannt ist, daß es genügt, eine *konsistente Hypothese* zu finden, um in diesem Modell lernen zu können, d.h. eine fehlerfreie Erklärung der Beobachtungen. Realistischer sind Modelle, in denen man auch verfälschte Beobachtungen zu läßt. Wir betrachten hier das *malicious-noise*-Modell, in dem es einem Gegenspieler erlaubt ist einen Anteil der Beobachtungen beliebig zu verfälschen. Diesen Anteil nennt man die *Noise-Rate*. Für diese Rate ist eine obere Schranke $\eta_{det} = \frac{\varepsilon}{1+\varepsilon}$ bekannt, wobei ε die gewünschte Lerngenauigkeit bezeichnet. Für größere Noise-Raten ist ein Lernen aus informationstheoretischen Gründen unmöglich. Allerdings gilt diese Schranke nur für deterministische Hypothesen. Unterhalb von η_{det} genügt es zum Lernen, eine *Hypothese mit minimaler Fehlerzahl* zu finden.

Wir zeigen hier, daß man bei der Verwendung von probabilistischen Hypothesen höhere Noise-Raten tolerieren kann. Auch hier gibt es aber eine Schranke $\eta_{prob} = \frac{2\varepsilon}{1+2\varepsilon} > \eta_{det}$, für $\varepsilon < 0,5$. Für Noise-Raten von der Größe η_{det} geben wir einen allgemeinen Algorithmus zum Lernen mit probabilistischen Hypothesen an, der das ,,minimale-Fehlerzahl-Paradigma" für deterministische Hypothesen ersetzt.

Weiter untersuchen wir, wie sich die Stichprobenkomplexität erhöht, wenn die Noise-Rate gegen η_{prob} strebt. Man beobachtet eine quadratisches ,,power-law", d.h., die Stichprobenkomplexität ist proportional zum Quadrat des Abstandes der Noise-Rate zu η_{prob}. Wir zeigen, daß dies notwendig zum Lernen ist, und daß in speziellen Situationen die resultierenden Stichprobengrößen auch ausreichen. Die zugehörigen oberen und unteren Schranken unterscheiden sich nur durch logarithmische Faktoren.

Die Lernbarkeit Boolescher Konzepte im Restricted-Focus-of-Attention Lernmodell

Andreas Birkendorf, Norbert Klasner, Hans Ulrich Simon
Lehrstuhl Informatik II
Universität Dortmund
D-44221 Dortmund, Germany
birkendo, klasner, simon@ls2.informatik.uni-dortmund.de

Eli Dichterman
Computer Science Department
Technion
Haifa 32000, Israel

Jeffrey Jackson
Math & Computer Science Department
Duquesne University
Pittsburgh, PA 15282, USA

In dem berühmten PAC-Lernmodell (PAC steht für *Probably Approximately Correct*) besteht das Ziel darin, ein verborgenes Konzept c einer bekannten Konzeptklasse $C_n \stackrel{\Delta}{=} \{f \mid f : X_n \to \{0,1\}\}$ zu lernen, indem man zufällig generierte Beispiele $(x, c(x))$, $x \in X_n$, beobachtet und auswertet.

Das Ziel ist erreicht, wenn es dem Lerner gelingt, nach einer endlichen (zumeist polynomiellen) Anzahl von Beispielen eine Hypothese $h : X_n \to \{0,1\}$ zu generieren, die sich mit hoher Wahrscheinlichkeit von c nicht allzu stark unterscheidet.

Für den Fall $X_n = \{0,1,\}^n$ betrachten wir in unserem Vortrag eine verallgemeinerte und für den Lerner schwierigere Variante des PAC-Lernens, das sogenannte *k-RFA-Lernen* (RFA steht für Restricted Focus of Attention).

Im Unterschied zum PAC-Modell erhält der Lerner in diesem Modell keine vollständigen Beispiele $(x, c(x))$ mehr. Stattdessen sieht er nur noch k Bits der Instanz $x = (x_1, \ldots, x_n)$, also z.B. $((1,*,0,*,1),0)$ für $k = 3$ anstelle von $((1,0,0,1,1,),0)$. Welche k Bits der Lerner sehen möchte, kann er für jedes neue Beispiel frei entscheiden.

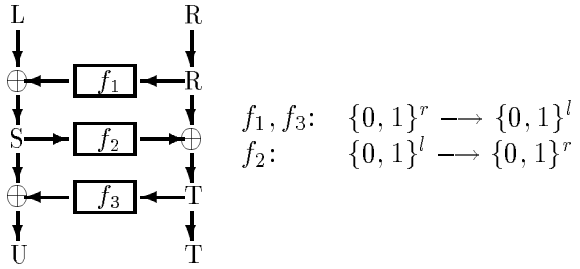
In unserem Vortrag werden wir ein Konstruktionsschema vorstellen, mit dem es uns gelingt, informationstheoretische Nichtlernbarkeitsresultate im k-RFA-Modell für ganze Konzeptklassen (z.B. Parity-Funktionen) schnell zu erzielen.

Außerdem werden wir dieses Schema auf die Klasse der *Entscheidungslisten* anwenden. Hier lassen sich teilweise scharfe Grenzen zwischen Lernbarkeit und (informationstheoretischer) Nichtlernbarkeit ziehen, die wir in unserem Vortrag herausarbeiten wollen.

Unbalancierte Luby-Rackoff Chiffren

Stefan Lucks
Institut für Numerische und Angewandte Mathematik
Georg–August–Universität Göttingen
Lotzestr. 16–18, D–37083 Göttingen, Germany
lucks@math.uni-goettingen.de

Unter Verwendung von *Zufallsfunktionen* beschrieben Luby und Rackoff [1] beweisbar sichere Blockchiffren. Seien f_1, f_2 und f_3 Zufallsfunktionen, $f_1, f_3 : \{0,1\}^r \longrightarrow \{0,1\}^l$ und $f_2 : \{0,1\}^l \longrightarrow \{0,1\}^r$. Es bezeichne „$\oplus$“ das Bit-weise Exklusiv-Oder (XOR). Wir berechnen $S, U \in \{0,1\}^l$ und $T \in \{0,1\}^r$ durch $S = L \oplus f_1(R)$, $T = R \oplus f_2(S)$ und $U = S \oplus f_3(T)$. So erhalten wir die Permutation $p(L,R) = \psi(f_1, f_2, f_3)(L,R) = (U,T)$ über $\{0,1\}^{l+r}$, siehe die untenstehende Abbildung. Die Umkehrung von p ist $p^{-1} = \psi(f_3, f_2, f_1)$.



Luby und Rackoff fanden in ihrer berühmten Arbeit [1] eine obere Schranke für die Erfolgswahrscheinlichkeit eines Chosen Plaintext Angriffs – abhängig von der Anzahl der gewählten Klartexte. Maurer [2] fand einen neuen, einfacheren Beweis für diese obere Schranke. Luby und Rackoff und auch Maurer beschränkten sich auf den balancierten Fall $l = r$.

In dem Vortrag wird das Resultat von Luby und Rackoff auf unbalancierte Fälle verallgemeinert, die Gültigkeit des Beweises auch unter schwächeren Voraussetzungen wird demonstriert, und die Konsequenzen für den Entwurf von sicheren Blockchiffren werden diskutiert. Eine ausführlichere Darstellung findet sich in [3].

Literatur

[1] M. Luby, C. Rackoff, “How to construct pseudorandom permutations from pseudorandom functions”, in: SIAM J. Computing, Vol. 17, No. 2, 373–386, 1988.

[2] U. Maurer, “A Simplified and Generalized Treatment of Luby-Rackoff Pseudorandom Permutation Generators”, in: Proc. EuroCrypt ’92 (ed. R. Rueppel), Springer LNCS 658, 239–255.

[3] S. Lucks, “Faster Luby-Rackoff Ciphers”, in: Fast Software Encryption 1996 (ed. D. Gollmann), Springer LNCS 1039, 189–203.

The Algorithmic Aspects of Uncrowded Hypergraphs

Claudia Bertram-Kretzberg, Hanno Lefmann
Lehrstuhl Informatik II
Universität Dortmund
D-44221 Dortmund
Germany
bertram/lefmann@Ls2.informatik.uni-dortmund.de

We consider the problem of finding deterministically a large independent set of guaranteed size in a hypergraph on n vertices and with m edges. With respect to the Turán bound, the quality of the solutions is for several situations by a logarithmic factor in the input size better. The algorithms are fast. Namely, they often have a running time linear in the input size $O(n+m)$, in particular, if the edge density is high. In the other cases, the time bound is $O(m)+o(n^3)$. This gives algorithmic solutions with state-of-the-art quality, solutions of which so far only the existence was known. In some cases, the corresponding upper bounds match the lower bounds up to constant factors. The involved concepts are uncrowded hypergraphs.

Efficient h-h Sorting and Routing on Constrained Reconfigurable Meshes

Manfred Kunde, Kay Gürtzig
Technical University of Ilmenau
Department for Automata and Formal Languages
PF 0565, D-98684 Ilmenau, Fed. Rep. of Germany
kunde@theoinf.tu-ilmenau.de, guertzig@theoinf.tu-ilmenau.de

Sorting and balanced routing problems for synchronous mesh-like processor networks with reconfigurable buses are considered. Induced by the argument that broadcasting along buses of arbitrary length within unit time seems rather non-realistic, we consider basic problems on reconfigurable meshes that can be solved efficiently even with restricted bus length.

Best of recently known h-h sorting algorithms for reconfigurable meshes of size $n \times n$ (e.g. KAUFMANN, SCHRÖDER and SIBEYN) take $hn + o(hn)$ time for any load $h \geq 1$, provided that data transmission on buses of arbitrary length is possible within unit time. Since hn is the bisection bound of reconfigurable square meshes, this seems optimal, but the underlying assumption is crucial.

We show that h-h sorting and routing on r-dimensional reconfigurable meshes of side length n can be performed in a time close to the bisection bound even with bus length bounded to a constant l. More precisely, the h-h sorting and routing problem can be solved within $hn + \mathrm{o}(hrn)$ steps in any case and in $hn/2 + \mathrm{o}(hrn)$ steps with high probability, provided that $hl \geq 4r$. This result is due to a data concentration method that is explained in the paper, in conjunction with the fundamental mesh sorting approach first to sort blocks (i.e. submeshes), than to interchange data between the blocks ("all-to-all mapping"), and to sort the blocks again.

Moreover, the results will hold even for certain very light loadings, i.e. with significantly less than one element per processor on average.

Extensions to two-dimensional reconfigurable meshes with diagonal links are considered. The acceleration factor with respect to reconfigurable meshes without diagonal links exceeds the number of extra links.

Variablenordnungen und die Größe von OBDDs für partiell symmetrische Boolesche Funktionen

Detlef Sieling[1]
Fachbereich Informatik, Lehrstuhl II
Universität Dortmund, D-44221 Dortmund
sieling@ls2.informatik.uni-dortmund.de

OBDDs haben sich als Datenstruktur für Boolesche Funktionen in Anwendungen wie Logiksynthese und Model Checking bewährt. Jedoch werden OBDDs häufig sehr groß. Da die OBDD-Größe wesentlich durch die gewählte Variablenordnung bestimmt wird, ist es wichtig, effiziente Algorithmen für die Berechnung guter Variablenordnungen zu haben. Hierfür wurden viele Heuristiken vorgeschlagen. Ein oft benutztes Prinzip besteht darin, Variablen, die zusammengehören, in der Variablenordnung auch nahe beisammen zu lassen.

Wir untersuchen das Problem der Berechnung optimaler Variablenordnungen für eine spezielle Klasse von Funktionen, die partiell symmetrischen Funktionen. Eine Funktion heißt partiell symmetrisch bezüglich einer Partition $V_1, \ldots, V_k$ der Variablenmenge, wenn der Funktionswert nur von der Anzahl der mit 1 belegten Variablen in jeder Menge V_i abhängt, nicht aber von der Position dieser Variablen. Eine naheliegende Heuristik bei der Berechnung von Variablenordnungen besteht darin, Variablen aus jeder der Symmetriemengen V_i zusammen zu testen. Derartige Variablenordnungen heißen symmetrisch. Möller, Molitor und Drechsler (1994) haben die naheliegende Vermutung widerlegt, daß es für alle Funktionen eine symmetrische optimale Variablenordnung gibt. Wir machen an einem Beispiel deutlich, daß dies folgenden Grund hat: Verschmelzungen von OBDD-Teilen können durch unsymmetrische Variablenordnungen erst möglich werden.

Um herauszufinden, wann unsymmetrische Variablenordnungen gut sind, betrachten wir zufällige partiell symmetrische Funktionen. Für Funktionen mit zwei Symmetriemengen, von denen die eine die Größe 1 und die andere die Größe n hat, sind mit Wahrscheinlichkeit $1 - o(1)$ nur unsymmetrische Variablenordnungen optimal. Falls beide Symmetriemengen die Größe n haben, sind mit Wahrscheinlichkeit $1 - o(1)$ nur symmetrische Variablenordnungen optimal. Analoge Ergebnisse für Verallgemeinerungen führen zu der Regel, daß symmetrische Variablenordnungen häufig optimal sind, wenn die Symmetriemengen die gleiche Größe haben, und daß unsymmetrische Variablenordnungen häufig optimal sind, wenn die Symmetriemengen sehr verschiedene Größen haben. Mit den Struktureigenschaften, die diesen Ergebnissen zugrundeliegen, kann außerdem ein einfacher Algorithmus für die Berechnung optimaler Variablenordnungen für partiell symmetrische Funktionen konstruiert werden.

[1]Gefördert durch die Deutsche Forschungsgemeinschaft unter Projekt We 1066/7.

On the Manhattan-Distance Between Points on Space-Filling Mesh-Indexings

Rolf Niedermeier
Wilhelm-Schickard-Institut für Informatik,
Universität Tübingen,
Sand 13,
D-72076 Tübingen,
niedermr@informatik.uni-tuebingen.de

Peter Sanders
Fakultät für Informatik,
Universität Karlsruhe,
D-76128 Karlsruhe,
sanders@ira.uka.de

Indexing schemes based on space filling curves like the Hilbert curve are a powerful tool for building efficient parallel algorithms on mesh-connected computers. The main reason is that they are locality-preserving, i.e., the Manhattan-distance between processors grows only slowly with increasing index differences. We present a simple and easy-to-verify proof that the Manhattan-distance of any indices i and j is bounded by $3\sqrt{|i-j|}-2$ for the 2D-Hilbert curve. The technique used for the proof is then generalized for a large class of self-similar curves. We use this result to show a (quite tight) bound of $4.73458\sqrt[3]{|i-j|}-3$ for a 3D-Hilbert curve.

A technical report is available via WWW. Try

`http://www-fs.informatik.uni-tuebingen.de/~niedermr`
`http://liinwww.ira.uka.de/~sanders`

Characterizations of the Existence of Partial and Total One-Way Permutations[2]

Jörg Rothe[3]
Institut für Informatik
Friedrich-Schiller-Universität Jena
07743 Jena, Germany
rothe@mipool.uni-jena.de

Lane A. Hemaspaandra[4]
Department of Computer Science
University of Rochester
Rochester, NY 14627
lane@cs.rochester.edu

In this note, we study the easy certificate classes introduced by Hemaspaandra, Rothe, and Wechsung [HRW95], with regard to the question of whether or not surjective one-way functions exist. This is an important open question in cryptology. We show that the existence of partial one-way permutations can be characterized by separating P from the class of UP sets that, for all unambiguous polynomial-time Turing machines accepting them, always have easy (i.e., polynomial-time computable) certificates. This extends results of Grollmann and Selman [GS88]. By Grädel's recent results about one-way functions [Grä94], this also links statements about easy certificates of NP sets with statements in finite model theory. Similarly, there exist surjective poly-one one-way functions if and only if there is a set L in P such that not all FewP machines accepting L always have easy certificates. We also establish a condition necessary and sufficient for the existence of (total) one-way permutations.

Literatur

[Grä94] E. Grädel. Definability on finite structures and the existence of one-way functions. *Methods of Logic in Computer Science*, 1:299–314, 1994.

[GS88] J. Grollmann and A. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17(2):309–335, 1988.

[HRW95] L. Hemaspaandra, J. Rothe, and G. Wechsung. Easy sets and hard certificate schemes. Technical Report Math/95/5, Institut für Informatik, Friedrich-Schiller-Universität Jena, Jena, Germany, May 1995.

[2]Supported in part by grants NSF-INT-9513368/DAAD-315-PRO-fo-ab and NSF-CCR-9322513.
[3]Work done in part while visiting the University of Rochester and Le Moyne College.
[4]Work done in part while visiting Friedrich-Schiller-Universität Jena.

Strikt sequentielle P-Vollständigkeit

Klaus Reinhardt
Wilhelm-Schickhard Institut für Informatik
Eberhard-Karls-Universität Tübingen
Sand 13, 72076 Tübingen
reinhard@informatik.uni-tuebingen.de

Ziel der Arbeit ist es, die wirklich inherent sequentiellen Probleme zu charakterisieren. Da es ein offenes Problem ist, ob sich alle Probleme in P durch Parallelisierung beschleunigen lassen, suchen wir nach Problemen mit einer Vollständigkeitseigenschaft, welche besagt, daß aus der Beschleunigung eines solches Problems durch Parallelisierung folgen würde, daß alle Probleme in P sich durch Parallelisierung beschleunigen lassen. Die bisher bekannten P-vollständigen Probleme haben diese Eigenschaft, wenn man sich auf die Klasse NC, d.h. eine Beschleunigung auf eine polylogarithmische Laufzeit durch Parallelisierung bezieht. Erkennt man jedoch realistischerweise bereits eine polynomielle Beschleunigung relativ zur besten sequentiellen Laufzeit an, so stellt man fest, daß viele der P-vollständigen Probleme in diesem Sinne parallelisierbar sind.

Wir beschreiben das *Multiplex-select Circuit Problem* MCP und zeigen, daß es *strikt sequentiell P-vollständig* ist, d.h. wenn sich dieses Problem durch Parallelisierung polynomiell beschleunigen lässt, so lassen sich alle Probleme in P durch Parallelisierung polynomiell beschleunigen. Dazu definieren wir auch die *Register Stack Maschine*, welche ein adäquateres Modell für pure Sequentialiät zu sein scheint.

Routing on Networks of Optical Crossbars

Klaus Schröder
Heinz Nixdorf Institut
Universität-GH Paderborn
D-33102 Paderborn
ellern@hni.uni-paderborn.de

Wir beschreiben Routingalgorithmen für mehrere Probleme auf Netzwerken aus Optical Crossbars. Ein Optical Crossbar ist eine durch optische Kommunikation mittels gerichteter Laserstrahlen motivierte Verbindungsstruktur. Neben Algorithmen für einzelne Optical Crossbars, auch *Completely Connected Optical Computer (OCPC)* genannt, sind in der Vergangenheit auch Routingalgorithmen für Netzwerke aus OCPCs untersucht worden. Netzwerke aus OCPC haben den Vorteil eine große Zahl von Prozessoren mit relativ kurzen OCPC verbinden zu können; der Grad des Netzwerks bleibt dabei klein. Frühere Untersuchungen konzentrierten sich vor allem auf sogenannte *Meshes of Optical Busses (MOBs)*, vorwiegend für Dimension 2. Ein MOB ist ein (mehrdimensionales) Gitter dessen Zeilen und Spalten jeweils durch OCPC verbunden sind.

Wir geben ein neues Schichtnetzwerk an, auf dem sich verschiedene Routingprobleme (Permutationen, zufällige Funktionen und h–Relationen) effizient lösen lassen. Die dabei verwendeten Protokolle sind durch hashingbasierte Shared Memory Simulationen inspiriert. Die Ergebnisse auf dem Schichtnetzwerk werden durch Simulation auf MOBs übertragen. Insbesondere erreichen wir einen Algorithmus für h–Relationen, dessen Laufzeit doppelt logarithmisch von der Größe des MOB, linear von h und polynomiell von der Dimension des MOB abhängt. Die Laufzeit früherer Algorithmen hängt exponentiell von der Dimension ab.

Sortieren von Schrauben und Muttern

Noga Alon
Dept. of Mathematics
Tel Aviv University
Tel Aviv, Israel
noga@math.tau.ac.il

Phillip G. Bradford, Rudolf Fleischer
MPI für Informatik
66123 Saarbrücken
{bradford,rudolf}@mpi-sb.mpg.de

Das Schrauben-Sortierproblem ist wie folgt : Gegeben ein Haufen von n Schrauben unterschiedlicher Größe und ein Haufen mit dazu passenden Muttern, finde zu jeder Schraube die passende Mutter. Das Problem dabei ist, daß wir nur feststellen können, ob eine Mutter kleiner/gleich/größer als eine Schraube ist, aber wir können nicht Schrauben mit Schrauben oder Muttern mit Muttern vergleichen.

Randomisiertes Quicksort löst das Problem offensichtlich in Zeit $O(n \log n)$, aber deterministisch ist es schwierig, ein gutes Pivot-Element für Quicksort zu finden (jedenfalls in subquadratischer Zeit). Die erste Lösung dazu stammt von Alon et al. [ABF94] und braucht $\Theta(n \log^3 n)$ Zeit (und damit $\Theta(n \log^4 n)$ Zeit für Quicksort).

Wir stellen hier ([BF95]) einen einfacheren Algorithmus vor, der in Zeit $O(n \log n)$ ein gutes Pivot-Element findet. Dazu verbinden wir (konzeptuell) die Schrauben mit den Muttern durch einen Expander mit konstantem Grad und machen alle Vergleiche entlang dieser Verbindungen. Wir eliminieren alle Schrauben, die nur mit größeren oder nur mit kleineren Muttern verbunden sind. Auf den restlichen Schrauben spielen wir dann ein einfaches KO-Turnier, das garantiert, daß der Gewinner des Turniers ein gutes Pivot-Element ist. Jede Runde des Turniers bruacht nur lineare Zeit.

Gibt man sich mit der Existenz eines Algorithmus zufrieden, kann man in [Br95] bzw. [KMS95] eine $O(n \log n)$-Lösung finden.

Literatur

[ABF94] N. Alon, M. Blum, A. Fiat, S. Kannan, M. Naor and R. Ostrovsky. *Matching nuts and bolts.* Proceedings of the 5th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'94), 1994, pp. 690–696.

[Br95] P.G. Bradford. *Matching nuts and bolts optimally.* Technical Report MPI-I-95-1-025, Max-Planck-Institut für Informatik, 66123 Saarbrücken, Germany, September 1995.

[BF95] P.G. Bradford, and R. Fleischer. *Matching nuts and bolts faster.* Proceedings of the 6^{th} International Symposium on Algorithms and Computation (ISAAC'95), 1995, pp. 402–408.

[KMS95] J. Komlós, Y. Ma, and E. Szemerédi. *Matching nuts and bolts in $O(n \log n)$ time.* Proceedings of the 7^{th} Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'96), 1996, pp. 232–241.

Fast Generation of Random Permutations via Networks Simulation

Partially supported by
KBN grant 8 S503 002 07,
TEMPUS project JEP 8145,
DFG-Sonderforschungsbereich 376 "Massive Parallelität", and
DFG Leibniz Grant Me872/6-1. To appear in ESA'96

Artur Czumaj
Heinz Nixdorf Institute
and Dept. of Math. & Computer Science,
University of Paderborn,
D-33095 Paderborn,
artur@uni-paderborn.de

Przemysława Kanarek
Institute of Computer Science,
University of Wrocław,
Przesmyckiego 20,
PL-51-151 Wrocław,
pka@tcs.uni.wroc.pl

Mirosław Kutyłowski
Heinz Nixdorf Institute
and Dept. of Math. & Computer Science,
University of Paderborn,
D-33095 Paderborn,
mirekk@uni-paderborn.de

Krzysztof Loryś
Dept. of Computer Science,
University of Trier,
D-54286 Trier,
lorys@TI.Uni-Trier.DE

Abstract

We consider the classical problem of generating random permutations with the uniform distribution. That is, we require that for an arbitrary permutation π of n elements, with probability $1/n!$ the machine halts with the ith output cell containing $\pi(i)$, for $1 \leq i \leq n$. We study this problem on two models of parallel computations: the CREW PRAM and the EREW PRAM.

Because of the logarithmic time lower bound for the OR computation, any nontrivial problem that can be solved in $o(\log n)$ time on the CREW PRAM is of special interest. The main result of the paper is an algorithm for generating random permutations that runs in $O(\log\log n)$ time and uses $O(n^{1+o(1)})$ processors on the CREW PRAM.

On the EREW PRAM we present a simple algorithm that generates a random permutation in time $O(\log n)$ using n processors and $O(n)$ space. This algorithm matches the running time and the number of processors used of the best previously known algorithms for the CREW PRAM, and performs better as far as the memory usage is considered.

The common and novel feature of both our algorithms is to design first a suitable random network generating a permutation and then to simulate this network on the PRAM model in a fast way.

Realistic Parallel Algorithms: Priority Queue Operations and Selection for the BSP* Model

Armin Bäumker, Wolfgang Dittrich,
Friedhelm Meyer auf der Heide, Ingo Rieping
{abk, dittrich, fmadh, inri}@uni-paderborn.de

Department of Mathematics and Computer Science
and Heinz Nixdorf Institute
University of Paderborn,
D-33095 Paderborn, Germany

In this paper, we explore parallel implementations of the abstract data type priority queue. We use the BSP* model, an extension of Valiant's BSP model, which rewards communicating few large messages instead of many small ones.

We present two randomized approaches. Both yield work optimal algorithms needing asymptotically less communication than computation time. Let N be the number of keys currently stored in the data structure, n the number of keys to be inserted or removed and p the number of processors.

The first approach works with smaller values of n/p, whereas the second one benefits from small values of N/n. We use a work optimal randomized selection algorithm as a building block, which might be of independent interest. It uses less communication than computation time, if the keys are distributed at random.

We improve upon previous work by both reducing the amount of communication and by using large messages.

Ressource-Bounded Computational Concepts versus Boolean Concepts

Bernd Borchert
Universität Heidelberg
bb@math.uni-heidelberg.de

Antoni Lozano
UPC Barcelona
lozano@lsi.upc.es

It is a well-known result that P/poly = *p-size circuits*. It is not so well-known that L/poly = *p-size branching programs*, as it was shown 1989 by C. Meinel. He also showed that NL/poly = *p-size nondeterministic branching programs*. Note that in any of these equations there is on the left side the nonuniform version of a ressource-bounded computational concept, and on the right side a p-size sequence of elements of a concept for the representation of Boolean functions. We will extend the list of the three results above by similar characterizations of PSPACE/poly, NP/poly, and ALOGTIME/poly: PSPACE/poly (NP/poly) is easily shown to be equal to *p-size (existentially) quantified Boolean formulas* which contain free variables, and ALOGTIME/poly will be shown by results of S. Buss to be equal to *p-size formulas* (which are circuits having the shape of a tree). All characterizations are no surprises because it is well-known that for every one of them the evaluation problem for the Boolean concept is complete for the corresponding uniform ressource-bounded computational complexity class. For example, the evaluation problem for circuits is P-complete. Summarizing we have the following informal correspondences between ressource-bounded computational concepts on one hand and Boolean concepts on the other:

ALOGTIME	corresponds to	formulas
L	corresponds to	branching programs
NL	corresponds to	nondeterministic branching programs
P	corresponds to	circuits
NP	corresponds to	existentially quantified Boolean formulas
PSPACE	corresponds to	quantified Boolean formulas

The main contribution of this talk will be a list of results which also witness the correspondences above. For a complexity class $\mathcal{C}$ we call a language A' *$\mathcal{C}$-uncut-bit-reducible* to a language A if there is a language $R \in \mathcal{C}$ and a polynomial q such that $x \in A' \iff R(x,0)R(x,1)\ldots R(x,2^{q(|x|)}) \in A$, where numbers are given in binary. Let for a Boolean concept $\mathcal{B}$ (like circuits) the *uncut succinct $\mathcal{B}$ version* of a language A be the language of all (encoded) elements b of $\mathcal{B}$ such that the result column of the truth-table representation of the Boolean function represented by b is in A. We will show that for every language A the uncut succinct formula (branching program, ...) version of A is log-time-complete for the class of languages ALOGTIME-uncut-bit-reducible (L-uncut-bit-reducible, ...) to A.

Programm

08.45 Imbiß

09.25 Begrüßung

09.30 Nicolo Cesa-Bianchi, Paul Fischer, Eli Shamir, Hans Ulrich Simon
Randomisierte Hypothesen helfen beim Lernen aus verrauschten Beispielen

09.55 Andreas Birkendorf, Norbert Klasner, Hans Ulrich Simon, Eli Dichterman, Jeffrey Jackson
Die Lernbarkeit Boolescher Konzepte im Restricted-Focus-of-Attention Lernmodell

10.20 Stefan Lucks
Unbalancierte Luby-Rackoff Chiffren

10.45-11.00 Pause

11.00 Claudia Bertram-Kretzberg, Hanno Lefmann
The Algorithmic Aspects of Uncrowded Hypergraphs

11.25 Manfred Kunde, Kay Gürtzig
Efficient $h - h$ Sorting and Routing on Constrained Reconfigurable Meshes

11.50 Detlef Sieling
Variablenordnungen und die Größe von OBDDs für partiell symmetrische Boolesche Funktionen

12.15-13.30 Mittagspause

13.30 Rolf Niedermeier, Peter Sanders
On the Manhattan-Distance Between Points on Space-Filling Mesh-Indexings

13.55 Jörg Rothe, Lane A. Hemaspaandra
Characterizations of the Existence of Partial and Total One-Way Permutations

14.20 Klaus Reinhardt
Strikt sequentielle P-Vollständigkeit

14.45-15.00 Pause

15.00 Klaus Schröder
Routing on Networks of Optical Crossbars

15.25 Noga Alon, Phillip G. Bradford, Rudolf Fleischer
Sortieren von Schrauben und Muttern

15.50-16.05 Pause

16.05 Artur Czumaj, Przemysława Kanarek, Mirosław Kutyłowski, Krzysztof Loryś
Fast Generation of Random Permutations via Networks Simulation

16.30 Armin Bäumker, Wolfgang Dittrich, Friedhelm Meyer auf der Heide, Ingo Rieping
Realistic Parallel Algorithms: Priority Queue Operations and Selection for the BSP* Model

16.55 Bernd Borchert, Antoni Lozano
Ressource-Bounded Computational Concepts versus Boolean Concepts

17.20 Ende