Parallel Algebraic Algorithm Design*

Lecture Notes for a Tutorial
ISSAC '89, Portland, Oregon, July 16, 1989

Erich Kaltofen

Department of Computer Science, Rensselaer Polytechnic Institute,
Troy, NY 12180-3590; `kaltofen@cs.rpi.edu`

Introduction

The notes following this introduction were written by students taking my graduate course 66.696 *Parallel Algorithm Design*, which I taught in the Fall of 1988. The material is largely based on the survey article by Karp and Ramachandran (1988) and the lecture notes by Leighton et al. (1988a), (1988b). However, our notes (as well as the ones by Leighton et al.) do not contain complete and up-to-date references. The following references with respect to the topics discussed in the turorial might be helpful.

Models of parallel computation
A survey of work on the complexity class $\mathcal{NC}$ is Cook's (1985) article. Von zur Gathen (1986) introduces the corresponding algebraic model. A general framework for different network designs, including a relationship between the butterfly and the deBruijn graphs, is discussed by Annexstein et al. (1989). Ranade (1987) shows how to simulate a PRAM on a butterfly network. Fault tolerant network routing on a hypercube is discussed in Hastad et al. (1989).

Workload balancing by processor rescheduling
This principle can be already found in (Brent 1974), where it is also shown that all formulas have equivalent shallow parse trees.

Parallel prefix
The original reference is to Ladner and Fischer (1980). An interesting application to parallel string matching can be found in (Karp and Rabin 1986). The prefix carry look-ahead circuit for integer addition is by (Brent and Kung 1982).

Integer arithmetic
The asymptotically best Boolean circuit for n-bit integer multiplication are still Schönhage's and Strassen's (1971). Division circuits of equivalent gate count and $O(\log(n)\log(\log\ n))$ delay are discussed by Reif and Tate (1989). With larger gate count delay $O(\log(n))$ was first accomplished by Beame et al. (1986) (see also (Shankar and Ramachandran 1988)).

List ranking
The first randomized workload balanced list ranking algorithm is by Vishkin (1984). A deterministic ruling-set based solution can be found in (Cole and Vishkin 1986). Newer solutions to this problem are in (Cole and Vishkin 1988) and (Anderson and Miller 1988).

Formula and DAG evaluation
A dynamic formula evaluation algorithm was first described by Miller and Reif (Miller and

*This material is based on work supported in part by the National Science Foundation under Grant No. CCR-87-05363 and under Grant No. CDA-88-05910.

Reif 1985). The shunting solution in the tutorial is by Kosaraju and Delcher (1988). Parallel evaluation of degree-bounded computation DAGs goes back to (Valiant et al. 1984); the dynamic scheme discussed in the tutorial is from (Miller et al. 1986). The problem of eliminating division from computation DAGs was first solved by Strassen (1973) for those that compute degree-bounded polynomials, and then by Kaltofen (1988) for the general case of degree-bounded rational functions. The latter article also contains a detailed discussion of Strassen's result.

Systolic greatest common divisors
The linear systolic array for polynomial and integer GCDs is due to Brent and Kung (1983) (see also (Yun and Zhang 1986)).

Linear systems
The first poly-log algorithm for solving linear systems was invented by Csanky (1976). The best version with respect to processor count is by Galil and Pan (1989). The solution discussed in the tutorial is Chistov's (1985). The randomized matrix rank algorithm is due to Borodin et al. (1982), while a deterministic solution was given by Mulmuley (1987). Such randomization techniques apply to matrix canonical form computations, such as the rational and Jordan normal forms; see (Kaltofen et al. 1987) and (Kaltofen et al. 1989).

Implementations
I am aware of three Ph.D. theses written on implementation issues of algebraic algorithms on parallel machines, Watt's (1985), Johnson's (1988), and Ponder's (1988). Efforts to-date are still scattered, among them the Reduce implementation on the CRAY X-MP at the Zuse Center (ZIB) in Berlin (Melenk and Neun 1986), the PAC project at the University of Grenoble (Roch et al. 1988), and efforts at Rensselaer Polytechnic Institute (Hitz 1988) and the University of Delaware (Saunders et al. 1989). Lenstra and Manasse are successfully using a loosely coupled network of workstations for running the Pomerance quadratic sieve integer factoring algorithm, and the implementation of the black box polynomial factorization algorithm (Kaltofen and Trager 1988) on such a distributed network of processors is underway at Rensselaer Polytechnic Institute.

Further results not discussed
There is a flurry of $\mathcal{NC}$-style parallel algebraic algorithms: polynomial factorization over finite fields (von zur Gathen 1984); element powering (Fich and Tompa 1988) and inversion (Litow and Davida 1988) in algebraic extensions of finite fields; polynomial arithmetic (Eberly 1984); absolute polynomial irreducibility (Kaltofen 1985); sparse multivariate polynomial interpolation (Ben-Or and Tiwari 1988), (Grigoryev et al. 1988); sign sequences of real roots of polynomials (Ben-Or et al. 1986); this list is by far incomplete. Also an area of activity is iterative methods for solving linear systems started by Pan and Reif (1985). The recently discovered processor efficient solution to the polynomial GCD problem by Kaltofen (1989) is the last chapter of these notes. Combinatorical algorithms are also surveyed by Eppstein and Galil (1988).

References

Anderson, R. J. and Miller, G. L., "Deterministic parallel list ranking," *Proc. AWOC 88, Springer Lec. Notes Comp. Sci.* **319**, pp. 81–90 (1988).

Annexstein, F., Baumslag, M., and Rosenberg, A. L., "Group action graphs and parallel architectures," *SIAM J. Comput.* **19**/3, pp. 544–569 (1990).

Beame, P. M., Cook, S. A., and Hoover, H. J., "Log depth circuits for division and related problems," *SIAM J. Comput.* **15**, pp. 994–1003 (1986).

Ben-Or, M., Kozen, D., and Reif, J., "The complexity of elementary algebra and geometry," *J. Comp. Sys. Sci.* **32**/2, pp. 251–264 (1986).

Ben-Or, M. and Tiwari, P., "A deterministic algorithm for sparse multivariate polynomial interpolation," *Proc. 20th Annual ACM Symp. Theory Comp.*, pp. 301–309 (1988).

Borodin, A., von zur Gathen, J., and Hopcroft, J. E., "Fast parallel matrix and GCD computations," *Inf. Control* **52**, pp. 241–256 (1982).

Brent, R. P., "The parallel evaluation of general arithmetic expressions," *J. ACM* **21**, pp. 201–208 (1974).

Brent, R. P. and Kung, H. T., "A regular layout for parallel adders," *IEEE Trans. Computers* **c-31**/3, pp. 260–264 (1982).

Brent, R. P. and Kung, H. T., "Systolic VLSI arrays for linear-time GCD computation," *Proc. VLSI '83*, pp. 145–154 (1983).

Chistov, A. L., "Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic," *Proc. FCT '85, Springer Lec. Notes Comp. Sci.* **199**, pp. 63–69 (1985).

Cole, R. and Vishkin, U., "Deterministic coin tossing with applications to optimal parallel list ranking," *Information and Control* **70**, pp. 32–53 (1986).

Cole, R. and Vishkin, U., "Optimal parallel algorithms for expression tree evaluation and list ranking," *Proc. AWOC 88, Springer Lec. Notes Comp. Sci.* **319**, pp. 91–100 (1988).

Cook, S. A., "A taxonomy of problems with fast parallel algorithms," *Inf. Control* **64**, pp. 2–22 (1985).

Csanky, L., "Fast parallel matrix inversion algorithms," *SIAM J. Comput.* **5**/4, pp. 618–623 (1976).

Eberly, W., "Very fast parallel polynomial arithmetic," *SIAM J. Comput.* **18**/5, pp. 955–976 (1989).

Eppstein, D. and Galil, Z., "Parallel algorithmic techniques for combinatorial computation," in *Annual Review in Computer Science* **3**, edited by J. F. Traub; Annual Reviews Inc., Palo Alto, California, pp. 233–283, 1988.

Fich, F. E. and Tompa, M., "The parallel complexity of exponentiating polynomials over finite fields," *J. ACM* **35**/3, pp. 651–667 (1988).

Galil, Z. and Pan, V., "Parallel evaluation of the determinant and of the inverse of a matrix," *Inform. Process. Letters* **30**, pp. 41–45 (1989).

von zur Gathen, J., "Parallel algorithms for algebraic problems," *SIAM J. Comp.* **13**, pp. 802–824 (1984).

von zur Gathen, J., "Parallel arithmetic computation: A survey," *Proc. MFCS '86, Springer Lec. Notes Comp. Sci.* **233**, pp. 93–112 (1986).

Grigoriev, D. Yu., Karpinski, M., and Singer, M. F., "Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields," *SIAM J. Comput.* **19**/6, pp. 1059–1063 (1990).

Hastad, J., Leighton, T., and Newman, M., "Fast computation using faulty hypercubes," *Proc. 21st Annual ACM Symp. Theory Comput.*, pp. 251–263 (1989).

Hitz, M., "HIPREC: Long integer arithmetic for SUN workstations and for the CRAY X/MP," *Master's Project*, Dept. Comput. Sci., Rensselaer Polytechnic Institute, Troy, N.Y., December 1988.

Johnson, J. R., "Designing Algebraic Algorithms for the Cray X-MP," *M.S. Thesis*, University of Delaware, January 1988.

Kaltofen, E., "Fast parallel absolute irreducibility testing," *J. Symbolic Comput.* **1**, pp. 57–67 (1985). Misprint corrections: *J. Symbolic Comput.* **9**, p. 320 (1989). Available from `anonymous@ftp.cs.rpi.edu` in directory **`kaltofen`**.

Kaltofen, E., "Greatest common divisors of polynomials given by straight-line programs," *J. ACM* **35**/1, pp. 231–264 (1988).

Kaltofen, E., "Processor efficient parallel computation of polynomial greatest common divisors," *Manuscript*, Dept. Comput. Sci., Rensselaer Polytechnic Institute, Troy, N.Y., August 1989.

Kaltofen, E., Krishnamoorthy, M. S., and Saunders, B. D., "Fast parallel computation of Hermite and Smith forms of polynomial matrices," *SIAM J. Alg. Discrete Math.* **8**, pp. 683–690 (1987).

KALTOFEN, E., KRISHNAMOORTHY, M. S., and SAUNDERS, B. D., "Mr. Smith goes to Las Vegas: Randomized parallel computation of the Smith normal form of polynomial matrices," *Proc. EUROCAL '87, Springer Lec. Notes Comput. Sci.* **378**, pp. 317–322 (1989).

KALTOFEN, E. and TRAGER, B., "Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators," *J. Symbolic Comput.* **9**/3, pp. 301–320 (1990).

KARP, R. M. and RABIN, M. O., "Efficient randomized pattern matching algorithms," *IBM J. Res. Develop.* **31**/2, pp. 249–260 (1987).

KARP, R. M. and RAMACHANDRAN, V., "Parallel algorithms for shared-memory machines," in *Handbook of Theoretical Computer Science, Algorithms and Complexity (Volume A)*, edited by J. van Leeuwen; Elsevier Science Publ., Amsterdam, pp. 869–941, 1990.

KOSARAJU, S. R. and DELCHER, A. L., "Optimal parallel evaluation of tree-structured computations by raking," *Proc. AWOC 88, Springer Lec. Notes Comp. Sci.* **319**, pp. 101–110 (1988).

LADNER, R. E. and FISCHER, M. J., "Parallel prefix computation," *J. ACM* **27**/4, pp. 831–838 (1980).

LEIGHTON, T., LEISERSON, C. E., MAGGS, B., PLOTKIN, S., and WEIN, J., *Advanced parallel and VLSI computation*; Research Seminar Series **RSS 1**; Lab. Comp. Sci., MIT, 1988a.

LEIGHTON, T., LEISERSON, C. E., MAGGS, B., PLOTKIN, S., and WEIN, J., *Theory of parallel and VLSI computation*; Research Seminar Series **RSS 2**; Lab. Comp. Sci., MIT, 1988b.

LITOW, B. E. and DAVIDA, G. I., "O(log(n)) parallel time finite field inversion," *Proc. AWOC 88, Springer Lec. Notes Comp. Sci.* **319**, pp. 74–80 (1988).

MELENK, H. and NEUN, W., "REDUCE user's guide for the CRAY 1 / CRAY X-MP series running COS," *Tech. Report*, K. Zuse Zentrum Berlin, September 1986.

MILLER, G. L., RAMACHANDRAN, V., and KALTOFEN, E., "Efficient parallel evaluation of straight-line code and arithmetic circuits," *SIAM J. Comput.* **17**/4, pp. 687–695 (1988).

MILLER, G. L. and REIF, J. H., "Parallel tree contraction Part 1: Fundamentals," in *Randomness in Computation*, Advances in Computing Research **5**, edited by S. Micali; JAI Press Inc., Greenwich, CT., pp. 47–72, 1989.

MULMULEY, K., "A fast parallel algorithm to compute the rank of a matrix over an arbitrary field," *Combinatorica* **7**, pp. 101–104 (1987).

PAN, V. and REIF, J., "Efficient parallel solution of linear systems," *Proc. 17th ACM Symp. Theory Comp.*, pp. 143–152 (1985).

PONDER, C. G., "Evaluation of 'Performance Enhancements' in Algebraic Manipulation Systems," *Ph.D. Thesis*, Comput. Sci. Div. (EECS Dept.), Univ. California at Berkeley, 1988.

RANADE, A. G., "How to emulate shared memory," *Proc. 28th Annual IEEE Symp. Foundations Comput. Sci.*, pp. 185–194 (1987).

REIF, J. H. and TATE, S. R., "Optimal size integer division circuits," *Proc. 21st Annual ACM Symp. Theory Comput.*, pp. 264–273 (1989).

ROCH, J.-L., SENECHAUD, P., SIEBERT-ROCH, F., and VILLARD, G., "Computer Algebra on a MIMD Machine," *Proc. ISSAC '88, Springer Lec. Notes Comput. Sci.* **358**, pp. 423–439 (1988).

SAUNDERS, B. D., LEE, H. R., and ABDALI, S. K., "A parallel implementation of the cylindrical algebraic decomposition algorithm," *Proc. ACM-SIGSAM 1989 Internat. Symp. Symbolic Algebraic Comput.*, pp. 298–307 (1989).

SCHÖNHAGE, A. and STRASSEN, V., "Schnelle Multiplikation grosser Zahlen," *Computing* **7**, pp. 281–292 (1971). In German.

SHANKAR, N. and RAMACHANDRAN, V., "Efficient parallel circuits and algorithms for division," *Information Process. Letters* **29**, pp. 307–313 (1988).

STRASSEN, V., "Vermeidung von Divisionen," *J. reine u. angew. Math.* **264**, pp. 182–202 (1973). In German.

VALIANT, L., SKYUM, S., BERKOWITZ, S., and RACKOFF, C., "Fast parallel computation of polynomials using few processors," *SIAM J. Comp.* **12**, pp. 641–644 (1983).

VISHKIN, U., "Randomized speed-ups in parallel computation," *Proc. 16th Annual ACM Symp. Theory Comp.*, pp. 230–239 (1984).

WATT, S. M., "Bounded Parallelism in Computer Algebra," *Ph.D. Thesis*, Dept. Comput. Sci., Univ. Waterloo, May 1986.

YUN, D. Y. Y. and ZHANG, C. H., "A fast carry-free algorithm and hardware design for extended integer GCD computation," *Proc. 1986 ACM Symp. Symbolic Algebraic Comp.*, pp. 82–84 (1986).