write, an Extended Find-First problem of size m is defined: $A_c[i]$ contains processor P_j if P_j attempts to write i into cell c. The space required for the simulating machine is $O(Sm)$. A 'write' step of the min-CRCW(S,m) PRAM can be also reduced to S Find-First problems of size nm. Specifically, $A_c[<i,j>]$ contains processor P_j if P_j attempts to write i into cell c (here 'lowest number' is with respect to the lexicographic ordering). The space required for the simulating machine here is $O(Snm)$.

Chlebus et al. show how to solve the Find-First problem of size m on several machines:

Proposition 24 *([CDHR88]) The Find-First problem of size m can be solved as follows: (a) On arbitrary-CRCW PRAM in $O(\log\log m)$ time; (b) On common-CRCW PRAM in constant time, provided that each processor has additional $\log m$ processors.*

The algorithms in [CDHR88] solve also the Extended Find-First problem since all processors contained in the same cell act identically (independently of their index). This is enough when using the arbitrary-CRCW and the common-CRCW PRAMs. Using the above we have

Simulation Result 3 An n-processor min-CRCW(S,m) PRAM can be simulated by an n-processor arbitrary-CRCW PRAM with $O(\log\log m)$ slow-down, using $O(mS)$ space.

Simulation Result 4 An n-processor min-CRCW(S,m) PRAM can be simulated by an $n\log m$-processor common-CRCW PRAM in $O(1)$ time, using $O(mS)$ space.

4. If for some i, $i = 1, .., l$, $b_i = 1$ and $1 < b_{i-1} < n - 1$ then q is "composite".

If the q was declared "composite" then it is indeed composite, otherwise q is prime with probability $> 1/2$ (i.e., the probability that a composite number will be considered as "possibly prime" is $< 1/2$).

The algorithm involves $O(\log q)$ modular exponentiations that can all be computed in parallel. Therefore, using $O(\log q)$ processors, the $O(\log q)$ time (sequential) algorithm for exponentiation can be employed. Since the algorithm for finding a prime performs in parallel $O(\log m)$ primality tests, the time complexity is $O(\log m)$ using $O(\log^2 m)$ processors.

In Section 3, a parallel time bound of $O(\log n)$ dominates all steps, but the one in which a prime is to be found. Finding a prime in $O(\log m)$ expected time meets this time bound only where m is bounded by a polynomial in n. Finally, we refer the reader to [AK88] for some further improvements.

C Simulation Results 3 and 4

Consider some CRCW machine. We say that a memory cell *contains* a processor if this processor has the address of this cell written in a special local register. Each processor is contained in at most one cell. A cell that contains at least one processor is said to be *non-empty*, otherwise it is said to be *empty*. The *Find-First* problem of size n is defined as follows: Given is an array $A[1..n]$, each cell of which is empty or contains exactly one processor, find the lowest-numbered non-empty cell of A. We similarly define the *Extended Find-First* problem of size n: Given is an array $A[1..n]$, each cell of which is empty or contains one or more processors, find the lowest-numbered non-empty cell of A.

Chlebus, Diks, Hagerup and Radzik [CDHR88] show how to simulate priority-CRCW PRAM on weaker CRCW PRAMs. Their simulations are based on solving the *Find-First* problem[2]. Specifically, a 'write' step of n-processor priority-CRCW is done as follows. For each memory cell c to which there is at least one processor that attempts to write, a Find-First problem of size n is defined: $A_c[i]$ contains processor P_i if P_i attempts to write into cell c. The space required for the simulating machine is $O(Sn)$ where S is the size of memory being used by the simulated priority-CRCW PRAM. Time requirements are discussed later.

Let *min-CRCW*(S, m) be a min-CRCW PRAM with space S and m being an upper bound on the values that can be written into the memory cells. A 'write' step of min-CRCW(S, m) PRAM can be done, similarly to the above, by using S Extended Find-First problems of size m. For each memory cell c to which there is at least one processor that attempts to

[2]Fich, Ragde and Wigderson [FRW88] also used the Find-First problem (there called "leftmost prisoner problem") to simulate priority-CRCW on common-CRCW PRAM.

Lemma 22 *([RS62]) For all $u \geq 17$, $\frac{u}{\ln u} \leq \pi(u) \leq 1.25506\frac{u}{\ln u}$.*

Corollary 23 *For all $u \geq 17$ there are at least $\frac{u}{2.28368 \ln(2u)}$ primes in the range $[(u+1)..2u]$.*

Proof: Let $\beta = 1.25506$. Following Lemma 22, $\pi(2u) - \pi(u) \geq \frac{2u}{\ln(2u)} - \beta\frac{u}{\ln u} = \frac{u(2\ln u - \beta\ln(2u))}{\ln u \ln(2u)} = \frac{u(\ln u(2-\beta) - \beta\ln 2)}{\ln u \ln(2u)} \geq \frac{u(\ln u(2-\beta-\beta\ln 2/\ln 17))}{\ln u \ln(2u)} > \frac{0.43788889u}{\ln(2u)} > \frac{u}{2.28368 \ln(2u)}$. ∎

Overview of the algorithm for finding a prime in the range $[(m+1)..2m]$.

Corollary 23 implies that our strategy for finding p may be as follows. Repeatedly select at random a number x from $[(m+1)..2m]$ and test x for primality. By Corollary 23 The expected number of x's to be tested is $\leq 2.28368 \ln(2m)$. Thus, $O(\log m)$ numbers from $[(m+1)..2m]$ can be randomly selected and independently (in parallel) be tested for primality. With high probability, at least one of these numbers will be detected prime.

Later, we go into some details of primality testing. Below, we backtrack and discuss the relevance of the above algorithm for finding a prime in the context of Section 3. The primality testing algorithm can be of a Monte Carlo type; i.e. we allow the output of the primality testing to be incorrect with constant fraction probability. Assume that some primality testing procedure PT is employed and detects (possibly falsely) a given number p' to be a prime. We use p' in our hash function scheme, assuming that it is a prime. If nothing goes wrong then we are done. (Note that this does not imply that p' is indeed a prime.) If, on the other hand, the hashing scheme (in some phase) takes longer than some predetermined time limit, then it is stopped. A new number p'' is then supplied by PT (p'' again is assumed to be prime), and a new hashing scheme is constructed (for that phase), based on p'' as the 'prime'. (Note that a failure in the hashing scheme construction may result from p' being a composite number; however, a failure may also occur when p' is a prime, because a success in the hashing construction depends also on the random choices of the parameters k and k'.) The expected number of times that the hashing scheme is reconstructed for either reason (i.e. selection of a composite number or selection of inappropriate parameters) in each phase is constant.

We show which primality testing algorithms are adequate for our purpose. For the serial algorithm many primality testing algorithms are available, see [AH87] [APR83] [GK86] [Mil76] [Rab80] [SS77]. Given an integer q, we give a short description of Rabin's algorithm for testing whether q is a prime:

1. Randomly pick b, $1 < b < q$.
Let $q - 1 = 2^l r$, where r is odd.

2. Compute residues mod q: for $i = 0, .., l$, compute $b_i = b^{2^i r} \bmod q$.

3. If $b^{q-1} \not\equiv 1 \bmod q$ then q is "composite".

$x_l[i] \in L_k$ and $x_r[j] \in R_{k'}$ for some k and k'. If $x_l[i]$ was selected into GL, i.e. $x_l[i]$ is the smallest element in $L_k \bigcup R_k$, then $x_r[j]$ was selected into GR, i.e. $x_r[j]$ is the largest element in $L_{k'} \bigcup R_{k'}$. Otherwise, we have from the inductive hypothesis on (a) and (c) that $x_r[j] < b_{k'} < x_l[i]$ (before $b_{k'}$ was changed in set GR) which contradicts the inductive hypothesis on (d). Similarly, if $x_r[j]$ was selected into GR then $x_l[i]$ was selected into GL, otherwise we have from the inductive hypothesis on (a) and (c) that $x_r[j] < a_k < x_l[i]$, which contradicts the inductive hypothesis on (d). If both $x_l[i]$ and $x_r[j]$ were not selected into GL and GR, respectively, then $k = k'$ otherwise by the inductive hypothesis on (a) and (c) we have $x_r[j] < a_k < x_l[i]$ which contradicts the inductive hypothesis on (d). Thus, $x_l[i]$ and $x_r[j]$ are in GL and GR, respectively, or in L_k and R_k, respectively.

(c): Following from the inductive hypothesis on (b), if $x_l[i]$ and $x_r[j]$ are in L_k and R_k, respectively, then their values are unchanged. If they are in GL and in GR, respectively, then after step 2 $x_l[i] = k$ and $x_r[j] = k'$ (where after step 1 $x_l[i] \in L_k$ and $x_r[j] \in R_{k'}$). Following from the definition of L_k and $R_{k'}$ in step 1 and from the inductive hypothesis on (c) we have $k < k'$.

(d): The values of all elements in sets L_k and R_k are unchanged. Thus, following from the inductive hypothesis on (b) and (d), if $x_l[i] \in L_k$ and $x_r[j] \in R_k$ then $x_r[j]$ is the left neighbor of $x_r[j]$. We only need to deal with the case that $x_l[i] \in GL$ and $x_r[j] \in GR$. Assume, by negation, that there is an element $y \in GR$ such that $x_r[j] < y < x_l[i]$. Clearly, after step 1 we had $x_l[i] \in L_k$, $x_r[j] \in R_{k'}$ and $y \in R_{k''}$ with $k' < k'' < k$, contradicting the inductive hypothesis on (d).

(e): Following from the inductive hypothesis on (e), in step 2 each element $x_l[i]$ is either in L_k for some k or in GL. Similarly, each element $x_r[j]$ is either in $R_{k'}$ for some k' or in GR. Thus, in step 3 each element is represented in exactly one recursive sub-problem.

(f): Following from the inductive hypothesis on (b). ∎

B Finding a prime in a given range

In Section 3 it is assumed that $m + 1$ is a prime. If we want m to be part of the input (either explicitly or implicitly) then we should give a procedure that, given some m, finds a prime $p > m$ such that $\log\log p = O(\log\log m)$; i.e. $p \in [(m+1)..m^{\log^k m}]$, for some constant $k > 0$. We show below how to find p with an expected number of $O(\log^3 m)$ operations. The expected parallel time is $O(\log m)$.

It is first shown that the density of primes in $[(m+1)..2m]$ is asymptotically similar to their density in $[1..m]$. Let $\pi(u)$ denote the number of primes $\leq u$. The following lemma is due to Rosser and Schoenfeld:

[Vis84] U. Vishkin. Randomized speed-ups in parallel computations. In *Proc. of the 16th Ann. ACM Symp. on Theory of Computing*, pages 230–239, 1984.

[Vis90] U. Vishkin. A parallel blocking flow algorithm for acyclic networks. Technical Report UMIACS-TR-90-11, University of Maryland Inst. for Advanced Computer Studies, 1990.

[vKZ77] P. van Emde Boas, R. Kaas, and E. Zijlstra. Design and implementation of an efficient priority queue. *Math. Systems Theory*, 10:99–127, 1977.

A Proof of Proposition 1

Proposition 1 Let $x[j]$ be the left neighbor of $x[i]$. Then for each level of the recursion the following properties hold:

(a) The values of all elements in L are distinct and the values of all elements in R are distinct.

(b) $x_l[i]$ and $x_r[j]$ are both represented in the same recursive sub-problem.

(c) $x_r[j] < x_l[i]$.

(d) $x_r[j]$ is the left neighbor of $x_l[i]$.

(e) Each element is represented in exactly one recursive sub-problem.

(f) Set L is nonempty if and only if set R is nonempty.

Proof:

The proof is by induction on the level of the recursion.

Inductive Base: Trivial.

Induction step:

(a): After step 2 the values of elements in L_k and in R_k are unchanged and therefore, by the inductive hypothesis on (a), we only need to look at the sets GL and GR. In step 2, for each k at most one element from L_k is selected into GL, and at most one element from R_k is selected into GR. These (possibly) selected elements are the only ones that are assigned with the value k.

(b): Following from the inductive hypothesis on (b), before step 1 elements $x_l[i]$ and $x_r[j]$ are both represented in the same recursive sub-problem. Assume that after step 1

[PVW83] W. Paul, U. Vishkin, and H. Wagener. Parallel dictionaries on 2-3 trees. In *Proc. of 10th ICALP, Springer LNCS 154*, pages 597–609, 1983.

[Rab80] M. Rabin. Probabilistic algorithms for testing primality. *J. Number Theory*, 12:128–138, 1980.

[Ran87] A.G. Ranade. How to emulate shared memory. In *Proc. of the 28th IEEE Annual Symp. on Foundation of Computer Science*, pages 185–194, 1987.

[RR89] S. Rajasekaran and J.H. Reif. Optimal and sublogarithmic time randomized parallel sorting algorithms. *SIAM J. Comput.*, 18:594–607, 1989.

[RS62] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.

[RS85] L. Rudolph and W. Steiger. Subset size in parallel. In *Proc. International Conference on Parallel Processing*, pages 11–13, 1985.

[Ruz80] W.L. Ruzzo. Tree-size bounded alterations. *JCSS*, 22:218–235, 1980.

[Sch87] B. Schieber. *Design and analysis of some parallel algorithms.* PhD thesis, Dept. of Computer Science, Tel Aviv Univ., 1987.

[Spi88] P.G. Spirakis. Optimal parallel randomized algorithms for sparse addition and identification. *Information and Computation*, 76:1–12, 1988.

[SS77] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM J. Computing*, 6:84–85, 1977.

[SV81] Y. Shiloach and U. Vishkin. Finding the maximum, merging, and sorting in a parallel computation model. *J. Algorithms*, 2:88–102, 1981.

[SV82a] Y. Shiloach and U. Vishkin. An $O(\log n)$ parallel connectivity algorithm. *J. Algorithms*, 3:57–67, 1982.

[SV82b] Y. Shiloach and U. Vishkin. An $O(n^2 \log n)$ parallel Max-Flow algorithm. *J. Algorithms*, 3:128–146, 1982.

[SV84] L. Stockmeyer and U. Vishkin. Simulation of parallel random access machines by circuits. *SIAM J. Comput.*, 13:409–422, 1984.

[Vis83a] U. Vishkin. On choice of a model of parallel computation. Technical Report TR 61, Dept. of Computer Science, Courant Institute, New York University, 1983.

[Vis83b] U. Vishkin. Synchronous parallel computation - a survey. Technical Report TR 71, Dept. of Computer Science, Courant Institute, New York University, 1983. Also: Annual Paper Collection of "Datalogforeningen" (The Computer Science Association of Aarhus, Denmark), 1987, 76-89.

[Joh82] D.B. Johnson. A priority queue in which initialization and queue operations take $O(\log\log D)$ time. *Math. Systems Theory*, 15:295–309, 1982.

[KLP89] Z.M. Kedem, G.M. Landau, and K.V. Palem. Optimal parallel prefix-suffix matching algorithm and applications. In *Proc. 1st ACM Symposium on Parallel Algorithms and Architectures*, pages 388–398, 1989.

[KMR72] R.M. Karp, R.E. Miller, and A.L. Rosenberg. Rapid identification of repeated patterns in strings, trees and arrays. In *Proc 4th ACM STOC*, pages 125–136, 1972.

[Knu73] D.E. Knuth. *The art of computer programming*, volume 3, Sorting and searching. Addison-Wesley, Reading, 1973.

[KP88] Z.M. Kedem and K.V. Palem. Optimal parallel algorithms for forest and term matching. *Theoretical Computer Science*, 1988. to appear.

[KR84] D. Kirkpatrick and S. Reisch. Upper bounds for sorting integers on random access machines. *Theoretical Computer Science*, 28:263–276, 1984.

[KR88] R.M. Karp and V. Ramachandran. A survey of parallel algorithms for shared-memory machines. Technical Report UCB/CSD 88/408, Computer Science Division (EECS) U. C. Berkeley, 1988.

[KRS88] C.P. Kruskal, L. Rudolph, and M. Snir. A complexity theory of efficient parallel algorithms. In *Proc. of 15th ICALP, Springer LNCS 317*, pages 333–346, 1988.

[KSSS86] A. Kalvin, E. Schonberg, J.T. Schwartz, and M. Sharir. Two dimensional, model-based, boundary matching using footprints. *The Int. J. of Robotics Research*, 5(4):38–55, 1986.

[KU86] A. Karlin and E. Upfal. Parallel hashing - an efficient implementation of shared memory. In *Proc. of the 18th Ann. ACM Symp. on Theory of Computing*, pages 160–168, 1986.

[LW88] Y. Lamdan and H.J. Wolfson. Geometric hashing: a general and efficient model-based recognition scheme. In *Proc. 2nd Int'l Conf. on Computer Vision, Tampa, FL*, pages 238–249, 1988.

[Mil76] G. Miller. Riemann's hypothesis and tests for primality. *JCSS*, 13:300–317, 1976.

[MV84] K. Mehlhorn and U. Vishkin. Randomized and deterministic simulations of PRAMs by parallel machines with restricted granularity of parallel memories. *Acta Informatica*, 21:339–374, 1984.

[PS80] W.J. Paul and J. Simon. Decision trees and random access machines. In *Symp. uber Logic und Algorithmik*, 1980.

[CW79] J.L. Carter and M.N. Wegman. Universal classes of hash functions. *J. Computer and System Sciences*, 18:143–154, 1979.

[DM89] M. Dietzfelbinger and F. Meyer auf der Heide. An optimal parallel dictionary. In *Proc. 1st ACM Symposium on Parallel Algorithms and Architectures*, pages 360–368, 1989.

[EG88] D. Eppstein and Z. Galil. Parallel algorithmic techniques for combinatorial computation. *Ann. Rev. Comput. Sci.*, 3:233–283, 1988.

[FKS84] M. L. Fredman, J. Komlós, and E. Szemerédi. Storing a sparse table with $O(1)$ worst case access time. *J. of the Association for Computing Machinery*, 31:538–544, 1984.

[FRW88] F.E. Fich, P.L. Ragde, and A. Wigderson. Simulations among concurrent-write PRAMs. *Algorithmica*, 3:43–51, 1988.

[GG88] Z. Galil and R. Giancarlo. Data structures and algorithms for approximate string matching. *J. of Complexity*, 4:33–72, 1988.

[GGK$^+$83] A. Gottlieb, R. Grishman, C.P. Kruskal, K.P. McAulife, L. Rudolph, and M. Snir. The NYU Ultracomputer - designing an MIMD shared memory parallel machine. *IEEE Trans. on Comp*, C-32:175–189, 1983.

[GK86] S. Goldwasser and J. Kilian. Almost all primes can be quickly certified. In *Proc. 18th ACM Symposium on Theory of Computing*, pages 316–329, Berkeley, 1986. ACM.

[Gol82] L.M. Goldschlager. A universal interconnection pattern for parallel computers. *J. Assoc. Comput. Mach.*, 29:1073–1086, 1982.

[Hag87] T. Hagerup. Towards optimal parallel bucket sorting. *Information and Computation*, 75:39–51, 1987.

[Hag88] T. Hagerup. On saving space in parallel computation. *Information Processing Letters*, 29:327–329, 1988.

[Has86] J. Hastad. Almost optimal lower bounds small depth circuits. In *Proc. of the 18th Ann. ACM Symp. on Theory of Computing*, pages 6–20, 1986.

[HN89] T. Hagerup and M. Nowak. Parallel retrieval of scattered information. In *Proc. of 16th ICALP, Springer LNCS 372*, pages 439–450, 1989.

[IK88] J. Illingworth and J. Kittler. A survey of the Hough transform. *Computer Vision, Graphics, and Image Processing*, 44:87–116, 1988.

[AS83] B. Awerbuch and Y. Shiloach. New connectivity and MSF algorithms for Ultracomputer and PRAM. In *Proc. International Conference on Parallel Processing*, pages 175–179, 1983.

[BDH$^+$89] P.C.P. Bhatt, K. Diks, T. Hagerup, V.C. Prasad, T. Radzik, and S. Saxena. Improved deterministic parallel integer sorting. Technical Report TR 15/1989, Fachbereich Informatik, Universität des Saarlandes, D-6600 Saarbrücken, W. Germany, November 1989.

[Bea89] P. Beame. A general sequential time-space tradeoff for finding unique elements. In *Proc. of the 21st Ann. ACM Symp. on Theory of Computing*, pages 197–203, 1989.

[BH87] P. Beame and J. Hastad. Optimal bounds for decision problems on the CRCW PRAM. In *Proc. of the 19th Ann. ACM Symp. on Theory of Computing*, pages 83–93, 1987.

[Bop89] R.B. Boppana. Optimal separations between concurrent-write parallel machines. In *Proc. of the 21st Ann. ACM Symp. on Theory of Computing*, pages 320–326, 1989.

[Bre74] R.P. Brent. The parallel evaluation of general arithmetic expressions. *J. Assoc. Comput. Mach.*, 21:302–206, 1974.

[BSV88] O. Berkman, B. Schieber, and U. Vishkin. Some doubly logarithmic parallel algorithms based on finding all nearest smaller values. Technical Report UMIACS-TR-88-79, Univ. of Maryland Inst. for Advanced Computer Studies, 1988.

[CDHR88] B.S. Chlebus, K. Diks, T. Hagerup, and T. Radzik. Efficient simulations between concurrent-read concurrent-write PRAM models. In *Mathematical Foundations of Computer Science '88*, 1988.

[Col86] R. Cole. Parallel merge sort. In *Proc. of the 27th IEEE Annual Symp. on Foundation of Computer Science*, pages 511–516, 1986.

[CV86] R. Cole and U. Vishkin. Approximate and exact parallel scheduling with applications to list, tree and graph problems. In *Proc. of the 27th IEEE Annual Symp. on Foundation of Computer Science*, pages 478–491, 1986.

[CV88] R. Cole and U. Vishkin. Approximate parallel scheduling. Part I: the basic technique with applications to optimal parallel list ranking in logarithmic time. *SIAM J. Comput.*, 17:128–142, 1988.

[CV89] R. Cole and U. Vishkin. Faster optimal parallel prefix sums and list ranking. *Information and Computation*, 81:334–352, 1989.

A third topic of independent interest is the efficient simulations of strong models of CRCW PRAM by more acceptable ones, and the methodology of designing parallel algorithms for the strong models with automatic simulations on acceptable models. We expect to see more applications of this approach in the design of parallel algorithms.

Acknowledgment: Torben Hagerup pointed out to us that the hashing scheme (Steps (a) and (b) in Section 3.1) works only when the input elements are distinct, and suggested the idea of repeatedly using different hash functions for proving Lemma 15. His comments are gratefully acknowledged.

We wish to thank Yehuda Afek, Noga Alon, Eli Gafni, Zvi Galil and Hanoch Levy for stimulating discussions.

References

[AH87] L. M. Adleman and M. A. Huang. Recognizing primes in random polynomial time. In *Proc. 19th ACM Symposium on Theory of Computing*, pages 462–469, New York City, 1987. ACM.

[AHU74] A. V. Aho, J. E. Hopcroft, and J. D. Ullman. *The design and analysis of computer algorithms*. Addison-Wesley Publishing Company, 1974.

[AIL+88] A. Apostolico, C. Iliopoulos, G.M. Landau, B. Schieber, and U. Vishkin. Parallel construction of a suffix tree. *Algorithmica*, 3:347–365, 1988.

[AK88] L.M. Adleman and K. Kompella. Using smoothness to achieve parallelism. In *Proc. of the 20st Ann. ACM Symp. on Theory of Computing*, pages 528–538, 1988.

[AKS83] M. Ajtai, J. Komlós, and E. Szemerédi. An $O(n \log n)$ sorting network. In *Proc. of the 15th Ann. ACM Symp. on Theory of Computing*, pages 1–9, 1983.

[AM88] R.J. Anderson and G.L. Miller. Optimal parallel algorithms for list ranking. In *3rd Aegean workshop on computing, Lecture Notes in Computer Science 319, 1988, Springer-Verlag*, pages 81–90, 1988.

[Apo84] A. Apostolico. The myriad virtues of subword trees. *in "Combinatorial Algorithms on Words" (A. Apostolico and Z. Galil, Eds.), NATO ASI Series F, Vol. 12,*, pages 85–96, 1984.

[APR83] L. M. Adleman, C. Pomerance, and R. S. Rumely. On distinguishing prime numbers from composite numbers. *Ann. Math.*, 117:173–206, 1983.

done, using Simulation Result 1, in $O(\log n)$ expected time and $O(n)$ expected number of operations, using $O(n)$ space. There are $O(\log\log m)$ phases by Lemma 4.

For the other implementations we use Algorithm DNN, where at each phase we implement a step of min-CRCW PRAM with memory size $S = O(m)$, each memory cell containing a $\log m$-bit word. We use Simulations Results 2, 3 and 4 to implement the second, third and forth implementations, respectively. ∎

Recall that after running Algorithm DNN, the Sorting algorithm can be finished by using the List Ranking procedure. The latter takes $O(\log n)$ time, $O(n)$ operations and $O(n)$ space on EREW PRAM. Thus, sorting distinct integers can be implemented with the same complexities as stated in Corollary 21 except for an increase in time to $O(\log n)$ in the last two cases.

In particular, the first item in Corollary 21 implies the following parallel sorting result.

Theorem 3 *Sorting n integers from the range $[1..m]$ can be done on a randomized arbitrary-CRCW in $O(\log n \log\log m)$ expected time, $O(n \log\log m)$ expected number of operations and $O(n)$ space.*

We finally note that the last three items in Corollary 21 can be used to derive deterministic implementations of the sorting algorithm that use reduced space. The fact that the sorting algorithm is stable will be used in a way similar to the proof of Theorem 1,

5 Conclusion

We gave an $o(n \log n)$ time randomized algorithm for sorting integers drawn from a superpolynomial range. Our algorithm takes $O(n \log\log m)$ expected time and $O(n)$ space. A parallel version of the algorithm achieves optimal speed up.

An open question is whether a space efficient deterministic integer sorting algorithm in $o(n \log n)$ time can be found, for integers drawn from a superpolynomial range $[1..n^{polylog(n)}]$.

We presented a parallel hashing technique that achieves optimal speed up and takes expected logarithmic time. It enables drastic reduction of space requirements for the price of using randomness and some increase in time, but no change in the expected number of operations. The technique was used in the parallel sorting algorithm and in the simulation results; its applicability to other problems was demonstrated.

An open question: design an optimal parallel speed up hashing scheme $F : W \mapsto [1..O(n)]$ that takes sublogarithmic time.

Chlebus, Diks, Hagerup and Radzik [CDHR88] show how to simulate an n-processor priority-CRCW by an n-processor arbitrary-CRCW PRAM with $O(\log \log n)$ slow-down. They also show how to simulate an n-processor priority-CRCW by an $n \log n$-processor common-CRCW PRAM in $O(1)$ time. Both simulations use $O(nS)$ space, where S is the size of memory being used by the simulated priority-CRCW PRAM. Using similar techniques we have the following simulations (proofs can be found in Appendix C).

Simulation Result 3 An n-processor min-CRCW that uses memory of size S, where each memory cell contains a $\log m$-bit word, can be simulated by an n-processor arbitrary-CRCW PRAM with a slow-down of $O(\log \log m)$, using $O(mS)$ space.

Simulation Result 4 An n-processor min-CRCW that uses memory of size S, where each memory cell contains a $\log m$-bit word, can be simulated by an $n \log m$-processor common-CRCW PRAM in $O(1)$ time, using $O(mS)$ space.

4.1 Applications

In this section we apply some of the simulations to the parallel DNN and Sorting algorithms and derive complexity results for standard CRCW PRAM models.

Recall that in Algorithm DNN there are $O(\log \log m)$ phases. Each phase takes $O(1)$ time for n min-CRCW processors. Following Simulation Results 1, 2, 3 and 4 we have

Corollary 21 *Let the input consist of n distinct integers from the range $[1..m]$, then Algorithm DNN can be implemented as follows:*

- *On arbitrary-CRCW in $O(\log n \log \log m)$ expected time, $O(n \log \log m)$ expected number of operations and $O(n)$ space.*
- *On priority-CRCW in $O(\log n \log \log m)$ time, $O(n \log \log m \log \log n)$ operations and $O(m + n^{1+\epsilon})$ space, for any fixed $\epsilon > 0$.*
- *On arbitrary-CRCW in $O((\log \log m)^2)$ time, $O(n(\log \log m)^2)$ operations and $O(m^2)$ space.*
- *On common-CRCW in $O(\log \log m)$ time, $O(n \log m \log \log m)$ operations and $O(m^2)$ space.*

Proof: The first implementation is as follows. At each phase of Algorithm DNN, Theorem 2 is used to map $O(n)$ variables (from $O(m)$ range) into $O(n)$ space in $O(\log n)$ expected time and $O(n)$ expected number of operations. The step of the min-CRCW PRAM is then the prefix $[1..l]$ provides the minimum needed for Step (c). For finding prefix minima in $O(\log\log n)$ time using $n/\log\log n$ processors, see [BSV88], or [Sch87].

The space complexity is dominated by the array BB whose size is m. The values written in the memory locations $BB[t_i]$ in Step (a) are from the range $[1..n]$. Therefore, the sorting problem of Step (b) is indeed of elements from this range only. The Lemma follows. ∎

A major drawback of the above reduction is the potentially large space that it might require. (Recall that this space is in addition to the memory which is as in the simulated min-CRCW.) However, the space consuming array BB is only used in Step (a). It is easy to see that the parallel hashing scheme from Section 3 can be applied here. As a result the additional space which is used by the reduction is reduced to $O(n)$ while the time complexity becomes expected $O(\log n)$, using the same number of operations (up to a constant factor).

We are ready to derive Simulation Result 1: It follows from Lemma 19, Lemma 9 and Theorem 2.

Comments:
1. Simulation Result 1 improves a similar theorem in the survey of Eppstein and Galil [EG88] (the min-CRCW is called there strong-CRCW), where it is assumed that addresses can be written in at most $O(\log n)$ bits. Recall that Simulation Result 1 does not impose any size restriction on the memory to be used by the simulated machine.

2. Lemma 19 can be extended to hold in $O(\log n/\log\log n)$ time for a fetch&add step of a fetch&add-CRCW PRAM. This extension, Lemma 9 and Theorem 2 imply the following extensions of Simulation Result 1: A single fetch&add step of n processors on a fetch&add-CRCW PRAM can be simulated by $\frac{n}{\log n}$ arbitrary-CRCW PRAM processors in $O(\log n)$ expected time (optimal speed-up) and $O(n)$ additional space.

Simulation Result 1 states that a single step of an n-processor min-CRCW can be simulated with $\Theta(n)$ expected number of operations by an arbitrary-CRCW PRAM. To see what can be done deterministically we first state the following lemma due to Hagerup:

Lemma 20 *([Hag87]) For any fixed $\epsilon > 0$, n integers of size polynomial in n can be sorted in $O(\log n)$ time by a priority-CRCW PRAM using $O(\frac{n\log\log n}{\log n})$ processors and $O(n^{1+\epsilon})$ space.*

Following Lemma 19 and Lemma 20 we have

Simulation Result 2 A single step of n processors on a min-CRCW PRAM with memory size S can be simulated by $\frac{n\log\log n}{\log n}$ priority-CRCW PRAM processors in $O(\log n)$ time and $O(S + n^{1+\epsilon})$ space (for any fixed $\epsilon > 0$).

Comment 3. Simulation Result 2 can be extended for a fetch&add-CRCW PRAM similarly to Comment 2 above.

Lemma 19 *Consider the problem of simulating a single 'write' stage of an n-processor min-CRCW PRAM on an arbitrary-CRCW PRAM. This problem can be reduced in $O(\log\log n)$ time and $O(n)$ operations (on an arbitrary-CRCW PRAM), to the problem of sorting n integers from the range $[1..n]$. The reduction uses $O(m)$ space, where m is the size of the memory in the simulated min-CRCW PRAM.*

Proof: Suppose the memory of the min-CRCW PRAM is an array $M[1..m]$ of size m. We denote the processors of the simulated min-CRCW PRAM by $MP_i, 1 \leq i \leq n$. As usual we will refer to the computation on the simulating arbitrary-CRCW PRAM in terms of operations, and suppress the issue of allocation of these operations to processors of the simulating machine. We will make one exception to this, in a case where such allocation requires special care. A typical 'write' stage of n min-CRCW PRAM processors can be viewed as follows. Processor $MP_i, 1 \leq i \leq n$, attempts to write value v_i into target address $M[t_i]$. Let S_i be the set of elements j such that $t_j = t_i$. The definition of the min-CRCW PRAM implies that v_i is written into $M[t_i]$ if $v_i = \min\{v_j : j \in S_i\}$.

The simulation makes use of a *bulletin board* $BB[1..m]$ that enables direct communication between all elements with the same target address. It works as follows:

a. For each processor MP_i, write its index i into memory location $BB[t_i]$. Arbitrarily, some index $i' \in S_i$, succeeds and i' is written into $BB[t_i]$.

The main idea is to "label" each processor in S_i by the same label i' and group all processors in S_i together into a successive subarray (Step (b)). The simulation of the min-CRCW PRAM is carried out by determining the minimum value v_i over each such successive subarray (Step (c)).

b. Sort the list $BB[t_1], .., BB[t_n]$ into an array $G[1..n]$.

We view each entry of G as a pair $< BB[t_i], v_i >$. The pairs are sorted by their first component; namely, identical $BB[t_i]$ values occupy successive subarrays of G. The beginning and end of each such subarray can be easily determined.

c. For each such successive subarray in G, find the minimum v_i over $\{v_j : BB[t_j]$ is in the subarray$\}$, and write v_i into memory location $M[t_i]$.

Step (a) can be done in $O(1)$ time and $O(n)$ operations using the arbitrary-CRCW PRAM. Step (c) can be done in time $O(\log\log n)$ and $O(n)$ operations.

We comment on how to implement Step (c) using $n/\log\log n$ processors within $O(\log\log n)$ time. The idea is to perform a prefix minima computation with respect to the vector of pairs G. That is, for each prefix $[1..i]$ we find the lexicographic minimum over its pairs. Given a successive subarray $[k..l]$ of identical $BB[t_i]$ values, we observe that the minimum over

Hagerup's algorithm for sorting integers from polynomial range [Hag87] has the drawback of using $O(n^{1+\epsilon})$ space (for any fixed $\epsilon > 0$). By using the parallel hashing scheme its space complexity decreases to $O(n)$. The expected number of operations remains the same and the time increases from $O(\log n)$ to expected $O(\log n \log\log n)$.

Finally, the parallel hashing scheme is used to get a space efficient optimal randomized simulation of the min-CRCW PRAM by arbitrary-CRCW PRAM, as given in Section 4.

Comment on finding a prime in a given range.
We assumed above that $m + 1$ is a prime. To withdraw this assumption we should give a procedure that, given some m, finds a prime $p > m$ such that $\log\log p = O(\log\log m)$. We have some preliminary results on this. Appendix B shows how to find a prime p in the range $[(m+1)..2m]$ in $O(\log m)$ expected time; the expected number of operations is proportional to a polynomial in $\log m$. To see the significance of such a procedure we should refer to the way in which the sorting algorithm is viewed. If the algorithm is for a fixed range $[1..m]$ then finding p is just a preprocessing which may be done only once (p can then be part of the input). We may, however, use the sorting algorithm as an *input sensitive* algorithm with no a priori knowledge about the range. Specifically, after reading the input values the actual range may be found by using a maximum finding procedure. In this case, an efficient procedure for finding a prime p is desired.

4 Simulating the min-CRCW PRAM

In this section we deal with simulations of the min-CRCW PRAM by weaker (and more acceptable) models of parallel computation. We show applications of some of these simulations for the parallel sorting algorithms.

Our most interesting simulation result is the following:

Simulation Result 1 One step of an n-processor min-CRCW PRAM can be simulated by an $\frac{n}{\log n}$-processor arbitrary-CRCW PRAM in $O(\log n)$ expected time (optimal speed-up) and $O(n)$ additional space.

Before proceeding to prove this simulation result, we make some general comments on how the result should be read and what has to be proved. These comments apply to other simulation results below, as well. The difference between the min-CRCW PRAM, being simulated, and the simulating arbitrary-CRCW PRAM lies in the way write conflicts are resolved. For this reason our proof needs to be concerned only with a 'write' stage of the min-CRCW PRAM on the arbitrary-CRCW PRAM. The space requirements for the simulating arbitrary-CRCW PRAM should be read as follows: (1) it needs as much space as the min-CRCW PRAM; in addition, (2) $O(n)$ space is needed.

space. Using the parallel hashing scheme, the space requirement decreases to $O(n \log n)$, the time increases to expected $O(\log n \log m)$ and the (expected) number of operations remains $O(n \log m)$.

An important technique for string matching algorithms was introduced by Karp, Miller and Rosenberg [KMR72]. Suppose an input string of length m is given. For each i, $0 \leq i \leq \log m$, the input string has m successive substrings of length 2^i. (Actually, there are only $m - 2^i + 1$ such substrings.) The technique partitions these substrings into equivalence classes where the substrings in each class are identical; furthermore, for each i separately, the technique labels each of the equivalence classes by a distinct integer between 1 and m. The main tool that was developed in [AIL$^+$88] was to parallelize this technique in $O(\log m)$ parallel time, $O(m \log m)$ work and $O(m^{1+\epsilon})$ space for $\epsilon > 0$. In [KP88], Kedem and Palem showed how to elegantly enhance this technique into $O(\log m)$ parallel time, and only $O(m)$ work (optimal) parallel algorithms for labeling equivalence classes of paths in labeled forests. However, the space remains superlinear. They applied this technique to solve term matching and related problems. Further advancements were given in [KLP89], where Kedem, Landau, and Palem present parallel algorithms for solving a variety of problems from pattern matching including multidimensional matching. Using our parallel hashing technique, *the space requirements in each of these algorithms can be reduced to linear, in exchange for randomization and increase in time by a logarithmic factor, but with no change in the number of operations.*

Section 2 in the approximate string matching survey of [GG88] discusses various ways for hashing many different substrings of a certain string. This is a fundamental problem that arises in some string matching automaton-like algorithms. They consider both serial and parallel computation. Given a string x, the size of the alphabet is relevant to the assignment of names to different substrings of x. In principle, different names should be assigned to different substrings of a given string x. In cases where the number of different substrings is n, a name should be a number from $[1..n]$. Name assignment is a mapping from a possibly large domain into $[1..n]$. Galil and Giancarlo propose in [GG88] an assignment procedure that takes $O(n \log n)$ operations where $|x| = n$; subsequently, it takes $O(\log n)$ time to find the name of a substring. Using our parallel hashing scheme, the assignment procedure takes $O(n)$ expected number of operations and $O(\log n)$ expected time; finding a name for a given substring takes $O(1)$ worst-case (!) time.

Following Kalvin, Schonberg, Schwartz and Sharir [KSSS86], Lamdan and Wolfson [LW88] use hashing for object recognition. Their method is parallel in a straightforward manner, except for their hash table construction. The parallel hashing scheme can be useful there. Hashing is used in implementations of the Hough Transform (HT) computations (cf. [IK88]). The HT technique has become important for many computer vision and pattern recognition applications. Parallel implementations of this technique can be efficiently done by using the parallel hashing scheme.

most $2k$. Part 1 ends before the $\log\log n$'th success, hence the expected number of phases in part 1 is $O(\log\log n)$. Part 2 ends before the $\log n$'th success, and the expected number of phases in part 2 is $O(\log n)$.

Using Brent's theorem [Bre74] as part of the WT suppression level methodology, part 1 can be implemented in $O(\log n)$ expected time, using $\frac{n}{\log n}$ processors.

Each phase of part 2 takes $O(1)$ time using $\frac{n}{\log n}$ processors. Part 2 takes a total of $O(\log n)$ expected time using $\frac{n}{\log n}$ processors. ∎

3.2 Applications

As a motivation for the previous subsection we stated Corollary 6.

Proof of Corollary 6: In algorithm DNN there are $\log\log m$ phases. In each phase, there are $O(n)$ variables a_k and b_k, each from the range $[1..nm]$. Separately for each phase we hash these variables into $O(n)$ space, using Theorem 2. Part A of Corollary 6 follows. Part B is trivial. ∎

We mention here some examples of algorithms for which the parallel hashing scheme can be used.

One application relates to the construction of *suffix trees*. Consider a string S of length n and all its n suffixes. A suffix tree is: (1) A rooted tree with n leaves. (2) Each edge of the tree is labeled by a successive substring of S. (3) Consider a path from the root to a leaf and concatenate the substrings along the path: each such path equals a different suffix of S. (4) Given any two suffixes, consider their longest common prefix. The suffix tree will have an internal node u such that the path from the root to u defines exactly this prefix. Actually, the lowest common ancestor of two leaves is the node defining the longest common prefix of their two suffixes. The ability to construct efficiently suffix trees and perform lowest common ancestor computations made suffix trees become the most important data structure for algorithms on strings. Applications of this data structure are reviewed in [Apo84]. [GG88] indicate that the space requirement of the suffix tree construction is the source of inefficiency in quite a few parallel preprocessing algorithms. The parallel algorithm by [AIL$^+$88] for constructing suffix tree requires $O(\log n)$ time, $O(n\log n)$ operations and $O(n^{1+\epsilon})$ space (for any $0 < \epsilon \leq 1$), where n is the length of the input string. Using the parallel hashing scheme, the space requirement decreases to $O(n)$, while the time increases to expected $O(\log^2 n)$ and the number of operations remains $O(n\log n)$ (as expected value rather than worst case). Suppose we have a relatively short string, whose length is m, and a long string, whose length is n. [GG88] considered instances where suffix trees are needed only for supporting queries requesting comparison among substrings of the short string and the long string. Their algorithm takes $O(\log m)$ time, $O(n\log m)$ operations and $O(n\log n + m^2)$

The following lemma will lead to the proof of Lemma 15.

Lemma 16 *Consider an active element $x \in W$ prior to some phase i. A representative for x will be found in phase i with probability $\geq \frac{1}{2}$.*

Proof: Let W' be the set defined by the multiset W, i.e., $W' = \{x \ : \ x = a_i$ for some $a_i \in W\}$ (we will refer to the elements of W' as *keys*). The *collision set* of an element $x \in W$ consists of the keys $y \in W'$, $y \neq x$, such that $g_{k_1,k_2}(y) = g_{k_1,k_2}(x)$. In Step (3) a representative is found for every element in W whose collision set is of size at most $s-1$. We show that setting $s = 3$ suffices for proving Lemma 16. The following definition and lemmas are due to Carter and Wegman [CW79]:

Definition A class H of functions from domain U to range R is *universal*$_2$ if for each pair of distinct elements x, y in U and randomly chosen $h \in H$ $\text{Prob}\,(h(x) = h(y)) \leq 1/|R|$.

Lemma 17 *(Proposition 2 in [CW79]) Given an element x in U, a subset S of U, and a function chosen randomly from a universal$_2$ class of functions, the expected number of elements in S that are in the collision set of x is at most $|S|/|R|$.*

Lemma 18 *(Proposition 7 in [CW79]) The class of functions $G = \{g_{k_1,k_2} : k_1, k_2 \in [1..m]\}$ is universal$_2$.*

Following Lemmas 17 and 18, for each element a_i in W, the expected size of its collision set is at most $|W|/n = 1$. Since the size of the collision set is non-negative, the probability of being at least twice the expected value is at most $1/2$. Therefore, the size of a_i's collision set is at most 2 with probability $\geq 1/2$. By setting $s = 3$, Lemma 16 follows. ∎

Proof of Lemma 15: Let t_k be the phase number in which element a_k becomes inactive, for $1 \leq k \leq n$. Following Lemma 16, $E[t_k] \leq 2$ for each k (same proof as for Lemma 14). The total work in all phases of part 1 (where $N_i > n/\log n$) is proportional to $\sum_i N_i \leq \sum_{k=1}^{n} t_k$. Therefore, the expected total work in all phases of part 1 is proportional to $\sum_{k=1}^{n} E[t_k] \leq 2n$.

The time in each phase in part 1 is dominated by the compaction procedure (Step 5). Using the Prefix Sums algorithm each phase takes $O(\frac{\log n}{\log\log n})$ time.

We show that the expected number of phases in part 1 is $O(\log\log n)$ and in part 2 is $O(\log n)$. Consider the following Bernoulli trials: A *success* in the i'th trial is defined to be the case that at least half of the active elements become inactive in phase i; that is, a success is when $N_{i+1} \leq \frac{N_i}{2}$. Following Lemma 16, the probability for success in each phase is $\geq \frac{1}{2}$. Therefore, as in the proof of Lemma 14, the expected number of phases before a first success occurs is at most 2, and the expected number of phases before the k'th success is at active element is found, with probability at least 1/2. The situation with implementing and analyzing the representative selection algorithm is analogous to Step (b) above. The only significant difference between the implementations is in Steps (1-3) (where elements become inactive). Lemma 16 below plays an analogous role to Lemma 8. Lemma 15 follows by simply being the analogous of Lemma 12. Details follow.

The representative selection algorithm

```
$i := 1$; $N_i := n$.

**while** $N_i > n/\log n$ **do**
    (All active elements in $W$ are in array $ACTIVE[1..N_i]$)

      Phase $i$

      1. Select at random two independent values $k_1$ and $k_2$ from the range $[1..m]$ (same
         range from which the elements of $W$ are drawn). Let $g_{k_1,k_2}(x) = 1 + ((k_1x + k_2)$
         mod $p)$ mod $n$ be a function from $[1..m]$ to $[1..n]$ (recall that $p = m+1$ is prime).
      2. For each active element $a_j$ compute $g_{k_1,k_2}(a_j)$.
      3. Repeat substeps $(i - iii)$ below $s$ times (the proof of Lemma 16 below shows that
         taking $s = 3$ is fine):
            (i) For each active element $a_j$, write $< a_j, j >$ into cell $g_{k_1,k_2}(a_j)$.
            (ii) If $< a_j, j >$ is actually written then index $j$ is selected to be the 'represen-
                 tative' of the elements $a_l = a_j$, $1 \leq l \leq n$.
            (iii) Each element that has a representative becomes inactive.
      4. Elements which are still active participate in phase number $i+1$. Their number is
         $N_{i+1}$.
      5. Using a prefix sums algorithm, compact the active elements into array $ACTIVE[1..N_{i+1}]$.
      6. $i := i + 1$.

**end** while

Denote $i' = i$. $N_{i'}$ is at most $n/\log n$.

**while** there is an active element **do**
    (All active elements in $W$ are in array $ACTIVE[1..N_{i'}]$)

      Phase $i$

      Do Steps 1-4 and 6 as above.

**end** while
```

similar to those in Lemma 13, $E[i'] \leq 2 \log \log n$ where i' is the number of phases in the first part. The expected number of phases for Part 2 is $O(\log n)$ based on Lemma 13.

Using Brent's theorem [Bre74] as part of the WT suppression level methodology, Step (b) can be implemented in $O(\log n)$ expected time, using $\frac{n}{\log n}$ processors on an arbitrary-CRCW PRAM. This concludes the proof of Lemma 12. ∎

Withdrawing the distinctness assumption.

Above, we made the simplifying assumption that $W = \{a_1, a_2 \ldots a_n\}$ is a set. However, for proving Theorem 2, we must assume that W is a multiset, that is, several elements of W may have the same value.

Consider the *representative selection* problem, which is defined as follows.

Input: Multiset $W = \{a_1, a_2, \ldots a_n\}$.
Problem: For each element a_i in W, $1 \leq i \leq n$, select a "representative" index j , $1 \leq j \leq n$, such that: (1) $a_j = a_i$, and (2) the representative index of every element $a_k = a_i$, $1 \leq k \leq n$, is also j.

Lemma 15 *The parallel algorithm below solves the representative selection problem. Using $n/\log n$ processors and $O(n)$ space on arbitrary-CRCW, its expected running time is $O(\log n)$.*

Below, we do things in the following order: (1) finish with the proof of Theorem 2, (2) comment on an interesting corollary of Lemma 15, and (3) give an algorithm for the representative selection problem, and thereby prove Lemma 15.

For proving Theorem 2, we apply the representative selection algorithm to the multiset W, and "delete" from W each element whose index was not selected as a representative of its value. Finally, we apply the above construction of a parallel perfect hash function with respect to the set of representatives. Theorem 2 follows from Lemmas 10, 12 and 15.

Comment: Consider the following *element multiplicity (EM)* problem. Given a multiset W, as above, find for each element in W how many other elements in W have the same value. We note that the most efficient algorithms known for this problem are based on general sorting algorithms, and need a total of $O(n \log n)$ operations and $O(n)$ space. The representative selection algorithm can be used to achieve results similar to Lemma 15, for the EM problem, as follows. Replace each element of W by its representative index, and apply Rajasekaran-Reif's parallel integer sorting algorithm. We finish this comment by noting that the EM problem is more general than two known problems: *element distinctness* (see [Bop89]) and *element uniqueness* (see [Bea89]).

An element $a_i \in W$ is called *active* until its representative is found and *inactive* later. The *representative selection algorithm* works in phases. In a phase, a representative for each some abstract model of parallel computation, that is only remotedly related to any PRAM model.) This methodology is called the *Work-Time (WT) suppression level* (Work-Time, in short) methodology in [Vis90]. The second stage, i.e., application of Brent's theorem, is trivial for our algorithm.

Specifically, let VAL[1..10n] be an array. The perfect hash function F, being constructed, will map each element of the input set W into array VAL.

Less informal implementation of Step (b).

```
$i := 1$; $N'_i := n$.

while $N'_i \;>\; n/\log n$ do
    (All active elements in $W$ are in array ACTIVE[1..$N'_i$] sorted by the $B(k,j)$ to which
    they belong)

      Phase $i$
      1. The first element in an active $B(k,j)$ selects at random a $k'(j)$ value.
      2. Each active element $x$ evaluates its hashing value $F(x)$ using $f_{k'(j)}$ and writes its
         original value $x$ into VAL[$F(x)$] (using the arbitrary CRCW convention).
      3. Each active element $x$ checks whether its value is written in VAL[$F(x)$]. If not it
         "disqualifies" the $k'(j)$ for its $B(k,j)$ set.
      4. All active elements belonging to $B(k,j)$ sets whose $k'(j)$ was disqualified remain
         active in phase number $i+1$. Their number is $N'_{i+1}$.
      5. Using a prefix sums algorithm, compact them into array ACTIVE[1..$N'_{i+1}$]
      6. $i := i+1$.

end while

Denote $i' = i$. $N'_{i'}$ is at most $n/\log n$.

while there is $j$ for which good $k'(j)$ has not been found do
    (All active elements in $W$ are in array ACTIVE[1..$N'_{i'}$], sorted by the $B(k,j)$ to which
    they belong)

      Do Steps 1-4 and 6 as above.

end while
```

Complexity. Following Lemma 8, $E[N'_i] \leq \frac{n}{2^{i-1}}$. Therefore, the expected total work is $\sum_i E[N'_i] \leq 2n$. The time in each phase in part 1 is dominated by the compaction procedure (Step 5). Using the Prefix Sums algorithm each phase takes $O(\frac{\log n}{\log\log n})$ time. Using arguments

Lemma 13 $E[t] \leq 2(\lceil \log n \rceil + 1)$.

Proof: Let N_i be the number of js for which a good k' was not found in the first i trials; i.e. $N_i = |\{j : t_j > i\}|$. Consider the following Bernoulli trials: A *success* in the i'th trial is defined to be the case that the number of good k's found in the i'th trial is at least $\frac{N_i}{2}$; that is, a success is when $N_{i+1} \leq \frac{N_i}{2}$. Following Lemma 8, $Prob[success] \geq \frac{1}{2}$.

Let x be the number of trials until the $(\lceil \log n \rceil + 1)$'st successful trial. It is easy to see that t is bounded by x and therefore $E[t] \leq E[x] \leq 2(\lceil \log n \rceil + 1)$. ∎

Lemma 13 proves Fact (I). To prove Fact (II) we first show

Lemma 14 $E[t_j] \leq 2$ *for each* j.

Proof:

$$E[t_j] = \sum_{i=1}^{\infty} i \cdot Prob[t_j = i] \leq \sum_{i=1}^{\infty} \frac{i}{2^i} = \sum_{i=1}^{\infty} \sum_{k=1}^{i} \frac{1}{2^i}$$

changing the order of summation, we get

$$= \sum_{i=1}^{\infty} \sum_{k=i}^{\infty} \frac{1}{2^k} = \sum_{i=1}^{\infty} \frac{1}{2^{i-1}} = 2.$$

∎

Let op_j be the number of operations required for selecting a good k' for j. Since $op_j = t_j b(k,j)$ we have $E[op_j] = E[t_j]b(k,j) \leq 2b(k,j)$ and the total number of operations is expected to be $E[\sum_{j=1}^{n} op_j] \leq 2\sum_{j=1}^{n} b(k,j) = 2n$.

It remains to give an implementation for the processors allocation. The selection of the numbers $k'(j)$ is done in phases. A set $B(k,j)$ and its elements are called *active* if a good $k'(j)$ has not yet been found. In each phase a new number $k'(j)$ is selected and tested, for every active $B(k,j)$. Let N'_i be the number of active elements in phase i.

We use a standard idea. Initially, N'_1 is n. As long as $N'_i > n/\log n$, we simply compact all N'_i active elements of phase i into an array of length N'_i prior to the phase. Consider the first phase i' for which $N'_{i'} \leq n/\log n$. The compacted array of size $N'_{i'}$, will be used for all subsequent phases.

Our presentation of the parallel algorithm follows a methodology that was introduced in [SV82b] and became standard since then, see [KR88]: First, the algorithm is described in terms of work and time only, as was done above. Second, a theorem by Brent [Bre74] is used to guide actual assignment of processors to jobs. (The theorem formally holds only in

(1) Sort the n numbers in $\{f_k(x) : x \in W\}$ into an array $C[1..n]$.

(2) Find for each j the rightmost (resp. leftmost) index i_1 (resp. i_2) for which $C[i_1] = j$ (resp. $C[i_2] = j$). Let $b(k, j)$ be $i_1 - i_2 + 1$.

Step (2) can be trivially done in $O(1)$ time using n processors. To do Step (1), note first that the range of f_k is the integer interval $[1..n]$. Thus, we may employ the integer sorting algorithm due to Rajasekaran and Reif:

Lemma 9 *([RR89]) n keys from the range $[1..n]$ can be sorted using $\frac{n}{\log n}$ arbitrary-CRCW PRAM processors in $O(\log n)$ time, with probability $\geq 1 - \frac{1}{n^\alpha}$, for any constant $\alpha > 0$.*

Following the above we have that each iteration in Step (a) of the construction of F takes $O(n)$ expected number of operations and logarithmic expected time. We conclude

Lemma 10 *Given is a set W of n numbers from the range $[1..m]$ and some $k \in [1..m]$. Checking whether $S_k < 5n$ can be done in $O(\log n)$ expected time, using $\frac{n}{\log n}$ arbitrary-CRCW processors.*

Corollary 11 *Step (a) in the construction of F takes $O(\log n)$ expected time, using $\frac{n}{\log n}$ arbitrary-CRCW processors.*

Implementation of Step (b).

In Step (b) the procedure to check whether k' is good for j is easy when using the arbitrary-CRCW PRAM. Our goal is to select a good k' for each j within a total of $O(n)$ operations and logarithmic time. The difficulty is that Step (b) should be done independently for each j ($j = 1, ..., n$). We prove

Lemma 12 *A good $k' = k'(j)$ can be found for all j, $j = 1, .., n$, in $O(\log n)$ expected time, using $\frac{n}{\log n}$ processors.*

Proof: To prove the lemma we show three facts: (I) the expected maximum number of trials in selecting a good k' for j (over $j = 1, .., n$) is $O(\log n)$; (II) the expected total work of selecting good k's for all j ($j = 1, .., n$) is $O(n)$; and (III) the processors can be allocated according to (I) and (II) to yield an $O(\log n)$ expected time parallel procedure for Step (b) in the construction of F, using $\frac{n}{\log n}$ processors.

Let t_j be the number of *trials* before a good k' is found for j, and let $t = max\{t_j : j = 1, \ldots, n\}$.

$W : f_k(x) = j\}$. Also, let $b(k,j) = |B(k,j)|$ and $S_k = \sum_{j=1}^{n} b(k,j)^2$. For each $j = 1, \ldots, n$, define $f'_{k',r} : B(k,j) \mapsto [1..2r^2]$ as $f'_{k',r}(x) = 1 + (k'x \bmod p) \bmod 2r^2$ where $k' = k'(j)$ is a parameter from $[1..m]$ and $r = b(k,j)$. Define $k' = (k'(j))$ to be *good* if $f'_{k'(j),b(k,j)}$ is a one-to-one function (over $B(k,j)$). Construction of the hash function F will be based on two steps:

(Step a) Repeatedly select k at random until $S_k < 5n$.

(Step b) For each j, repeatedly select $k' = k'(j)$ at random until k' is good.

After all parameters k and $k'(j)$ (for all $j = 1, ..., n$) are appropriately selected, the one-to-one function F is derived by first applying f_k and then $f_{k'(j),b(k,j)}$ for a proper j. Specifically, F is constructed as follows. For each set of elements $B(k,j)$, $b(k,j)^2$ space is assigned. Let M_i be the prefix sum $\sum_{j=1}^{i} 2b(k,j)^2$. Then $[1..M_i]$ is an array assigned to the first i sets $B(k,1), ..., B(k,i)$. The function $f_{k'(j),b(k,j)}$ maps each element in $B(k,j)$ into $[(M_{j-1}+1)..M_j]$. $F(x)$ is evaluated as follows:

(1) Evaluate $j = f_k(x)$.

(2) $F(x) = M_{j-1} + f'_{k'(j),b(k,j)}(x)$.

Step (a) guarantees that the overall space $M_n = 2S_k$ is linear ($< 10n$). Step (b) guarantees that the mapping is one-to-one. It remains to show how to implement steps (a) and (b).

The following lemmas are due to Fredman, Komlós and Szemerédi (Corollaries 3 and 4 in [FKS84]).

Lemma 7 *([FKS84]) For at least one-half of the values k in $[1..m]$, $S_k < 5n$. Thus, for a randomly selected k, $S_k < 5n$ with probability $\geq \frac{1}{2}$.*

Lemma 8 *([FKS84]) For each j in $[1..n]$, at least one-half of the k's in the range $[1..m]$ are good.*

Implementation of Step (a).

Following Lemma 7, the expected number of iterations in (a) is ≤ 2. We first show how to check whether $S_k < 5n$. Given $b(k,j)$ for all j, the evaluation of the prefix sums $M_i = 2\sum_{j=1}^{i} b(k,j)^2$ (for $i = 1, ..., n$) and of $S_k = M_n$ can be done by using the Prefix Sums algorithm of Cole and Vishkin [CV86] [CV89] in $O(\log n / \log\log n)$ time and $O(n)$ operations. The evaluation of $b(k,j)$ for each j is done as follows:

given level denote by W the set of a_k and b_k variables that are being used ($|W| = O(n)$). The deterministic implementation in Section 2 requires $O(m)$ space for the a_k and b_k variables. The key idea here is to randomly select a hash function for mapping the set W into $O(n)$ space. In order to avoid collisions, we shall use a *perfect hash* function (which is a one-to-one function).

Remark. For the serial algorithm, simpler hash functions would suffice in order to reduce the space to $O(n)$. From now on we concentrate on the parallel algorithm. Based on this, the implementation for the serial algorithm will be straightforward.

A basic procedure for constructing a perfect hash function is presented. Its expected running time is logarithmic and its expected number of operations is linear. Specifically, we prove in Section 3.1 the following theorem:

Theorem 2 *Let W be a multiset of n numbers from the range $[1..m]$, where $m + 1 = p$ is prime. Suppose we have $\frac{n}{\log n}$ processors on an arbitrary-CRCW PRAM. A one-to-one function $F : W \mapsto [1..O(n)]$ can be found in $O(\log n)$ expected time. The evaluation of $F(x)$, for each $x \in W$, takes $O(1)$ arithmetic operations (using numbers from $[1..m]$).*

We show later that Theorem 2 leads to the following:

Corollary 6 *A. Algorithm DNN takes $O(\log n \log\log m)$ expected time and $O(n)$ space, using $\frac{n}{\log n}$ processors on a min-CRCW PRAM. B. The same performance is obtained for the problem of sorting n integers drawn from a domain of size m.*

By using the optimal simulation results of Section 4, the same bounds will be shown to hold also when using the standard arbitrary-CRCW model.

3.1 Constructing a Perfect Hash Function in Palallel

In this subsection we prove Theorem 2.

Given is a multiset W of n numbers from the range $[1..m]$, where $p = m + 1$ is prime. It is first assumed that W is a set, i.e. that the numbers in W are distinct. At the end of this subsection, it is shown how to withdraw this assumption. We construct in parallel a hash function F which maps W into the range $[1..10n]$. We use the fundamental perfect hash function F that was suggested by Fredman, Komlós and Szemerédi [FKS84], as described below. An efficient parallel construction of F is presented.

Define $f_k : W \mapsto [1..n]$ as $f_k(x) = 1 + (kx \bmod p) \bmod n$ where k is a parameter from $[1..m]$. Let $B(k, j)$ be the set of values in W that are mapped by f_k into j, i.e. $B(k, j) = \{x \in$

Proof: The output of the DNN algorithm (without the distinctness assumption) gives a linked list of the elements, where the links in the list are defined by the right neighbor relation. This linked list is *stable* in the following sense: if $x[i] = x[j]$ for some $i < j$ then element i precedes element j in the linked list. A consequence is that an iterative procedure, in the spirit of Radix Sort, can be applied. Specifically, each $\log m$-bit input word is partitioned into c blocks of $(\log m)/c$ bits each. The blocks are numbered from right to left (i.e., from the the least significant bits to the most significant ones). We proceed in c phases. The input to the first phase is the original input array for the sorting problem. The input to phase k, $2 \leq k \leq c$, is the output array of phase $k-1$. In phase k, $1 \leq k \leq c$, only the k'th block of each input word is considered as the value of the word. The phase has two steps: (1) The DNN algorithm is applied to sort these values into a linked list. (2) A list ranking algorithm is applied to transform the list into an input array for the next phase; in phase c, however, this gives the output for the sorting problem.

Recall that we use the DNN algorithm for non-distinct input elements in each phase, and therefore the space needed is $O(nm^{1/c})$.

Correctness of this iterative procedure follows from the following *Inductive claim:* The output array of phase k, $1 \leq k \leq c$, gives a stable sorting of the (original) input elements if blocks $1, .., k$ together are considered as the value of each element. The theorem follows by taking $k = c$. ∎

If the input is from a range polynomial in n then we have the same complexities as in Hagerup's algorithm [Hag87]. The range for which our algorithm gives better results than the best known algorithms is for $n^{\log \log n} \ll m \ll 2^{n^{o(1)}}$, where $\ll$ denotes smaller asymptotically. Thus, for example, for $m = n^{polylog(n)}$ we have:

Corollary 5 *n integers from the range $[1..n^{\log^k n}]$ (for every constant $k > 0$) can be sorted in: (1) $O(n \log \log n)$ serial time and $O(n^{1+(\log^k n)/c})$ space, for any constant $c \geq 1$; and (2) $O(\log n)$ parallel time and $O(n^{1+(\log^k n)/c})$ space, for any constant $c \geq 1$, using $\frac{n \log \log n}{\log n}$ processors on a min-CRCW PRAM.*

3 Trading Space for Randomness

In this section we show how to use randomization in order to reduce the space complexity of the algorithms to $O(n)$. The randomization is of the "Las-Vegas" type algorithm. That is, some of the steps of the space reducing algorithm are based on randomized moves and it never errs.

Recall that in each recursive level of algorithm DNN, there are $O(m)$ variables a_k and b_k. However, in each level of the algorithm only $O(n)$ of these variables are actually used. For a

2.3 Complexity and implementation

We start by discussing the complexity of algorithm DNN and later state the sorting results.

Lemma 4 *Given are n elements with distinct values from the interval of integers $[1..m]$. (1) Algorithm DNN works serially in $O(n \log\log m)$ time and $O(m)$ space. (2) Algorithm DNN works in $O(\log\log m)$ time and $O(m)$ space, using n processors on a min-CRCW PRAM.*

Proof: The size of interval I for each recursive sub-problem is bounded by $\sqrt{m}$. Therefore, $D(m)$, the depth of the recursion, satisfies $D(m) \le D(\sqrt{m}) + O(1)$, implying $D(m) = O(\log\log m)$. For each level of the recursion we need to perform at most $O(n)$ operations and therefore the total number of operations is $O(n \log\log m)$.

To finish deriving the serial result we "remember" for each element in each level of the recursion its original index in the initial sets L and R. The space needed for all subproblems together in each level of the recursion is $O(m)$. Since we can reuse the space for the highest level of the recursion, we get a total of $O(m)$ space, as well. Item 1 of the lemma follows.

We proceed to the parallel result. Initially, we assign one processor to each copy of each element (i.e., each element of the original sets L and R). This assignment remains throughout the entire algorithm.

For Step 2, we need to have in a_k (resp. b_k), for $k = 0,..,q-1$, the minimum (resp. maximum) element's value over all the elements that belong to L_k (resp. R_k); where, a_k (resp. b_k) is the kth cell in some predesignated array $a[0..q-1]$ (resp. $b[0..q-1]$). We already argued (implicitly Item 1 of the lemma) that sequentially computatio of a_k (resp. b_k), for $k = 0, \ldots, q-1$, can be trivially done in $O(n)$ time. In parallel, Step 2 can be done in $O(1)$ time, using n processors. Here is where we take advantage of the min-CRCW PRAM, where if several processors try to write into the same memory location, only the one with the minimal value succeeds. Item 2 of Lemma 4 follows. ∎

Withdrawing the distinctness assumption. We assumed that all elements in the input sequence are distinct. It is trivial to achieve distinctness by replacing each input element $x[i]$ by the pair $<x[i], i>$. This increases the required space to $O(nm)$. However, the randomized sorting results in Section 4.1 will not be affected.

The space requirements of the sorting algorithm can be reduced deterministically, as shown in the following theorem:

Theorem 1 *Given are n elements with values from the interval of integers $[1..m]$, our sorting algorithms achieve the following results: (1) $O(n \log\log m)$ serial time and $O(nm^{1/c})$ space, where $c \ge 1$ is any fixed constant. (2) $O(\log n + \log\log m)$ parallel time and $O(nm^{1/c})$ space (for any constant $c \ge 1$), using $\frac{n \log\log m}{\log n}$ processors on a min-CRCW PRAM.*

- If the smallest (resp. largest) element of $L \bigcup R$ in I_k is in L (resp. in R) then its left (resp. right) neighbor is not in I_k. We collect the elements from L (resp. from R) whose left (resp. right) neighbor is not in I_k into the global set GL (resp. set GR).
- The algorithm advances to the deepest level of recursion and simply terminates (without any backtracking).
- All recursive calls of the algorithm are performed simultaneously in parallel.

2.2 Correctness

Proposition 1 *Let $x[j]$ be the left neighbor of $x[i]$. Then for each level of the recursion the following properties hold:*

(a) The values of all elements in L are distinct and the values of all elements in R are distinct.

(b) $x_l[i]$ and $x_r[j]$ are both represented in the same recursive sub-problem.

(c) $x_r[j] < x_l[i]$.

(d) $x_r[j]$ is the left neighbor of $x_l[i]$.

(e) Each element is represented in exactly one recursive sub-problem.

(f) Set L is nonempty if and only if set R is nonempty.

The proof of Proposition 1 is given in Appendix A.

Corollary 2 *If a problem with input L, R and I is of size 2 then $|L| = |R| = 1$ and the element in R is the left neighbor of the element in L.*

Proof: Assume that $x_l[i] \in L$ and that $x[j]$ is the left neighbor of $x[i]$. Let $I = [d, d+1]$ for some integer d. Following from property (b) in Proposition 1, $x_r[j] \in R$. Thus, from property (c) we have $x_r[j] = d$ and $x_l[i] = d+1$. If $L > 1$ then by property (a) a second element can only be $x_l[i'] = d$ (for some $i' \neq i$). However, following property (c) its left neighbor must be $< d$, contradicting property (b). Similarly, R may contain only one element. ∎

Corollary 3 *Suppose that initially m, the size of the interval from which the input elements are drawn, is 2^{2^t} for some integer $t \geq 1$ (and $t = \log\log m$). Consider a recursive problem at recursion level t. The interval I from which the input elements for such recursive problem are drawn consists of two successive integers. That is, for some integer d, $I = [d, d+1]$. Furthermore, $L = \{d+1\}$ and $R = \{d\}$ and $d+1$ is the right neighbor of d.*

a and m'. Set L will always represent a non-empty subset of the left copies and set R will always represent a non-empty subset of the right copies. Each element in set L searches for its *left neighbor* within set R. This left neighbor is defined as the largest element in R which is smaller than it. Similarly, each element in set R searches for its *right neighbor* defined as the smallest element in L which is larger than it.

Initially, the interval I is $[1..m]$ (i.e., $a = 0$ and $m' = m$), L is $\{x_l[1], ..., x_l[n+1]\}$ and R is $\{x_r[1], ..., x_r[n+1]\}$.

The recursive algorithm DNN

Input: L, R and I, where L and R are nonempty sets and $I = a + [1..m]$ is an interval of integers. We refer to $m = |I|$ as the *size* of the problem.

A processor stands by each element in L and each element in R.

if $m = 2$ (*comment:* the situation for a recursive problem for which $m = 2$ is characterized in Corollary 2.)

then Declare the element in L to be the right neighbor of the element in R and the element in R to be the left neighbor of the element in L.

else

(1) Partition set L into $q = \sqrt{m}$ subsets $L_0, L_1, ..., L_{q-1}$ where L_k contains elements (of L) from the interval $I_k = a + k \cdot q + [1..q]$, for $k = 0, ..., q-1$. Similarly, partition set R into $q = \sqrt{m}$ subsets $R_0, R_1, ..., R_{q-1}$ where R_k contains elements (of R) from the interval $I_k = a + k \cdot q + [1..q]$, for $k = 0, ..., q-1$.

(2) Let a_k be the smallest element in L_k. **If** a_k is less than or equal to the smallest element in R_k **then**: (a) Select the integer k into the new set GL (integer k represents element a_k and will be referred to as a_k). (b) Remove a_k from L_k.

Similarly, let b_k be the largest element in R_k. **If** b_k is greater than or equal to the largest element in L_k **then**: (a) Select the integer k into the new set GR (integer k represents element b_k and will be referred to as b_k). (b) Remove b_k from R_k.

(3) Do the following recursive calls: (a) For each pair of nonempty (local) subsets L_k and R_k solve the problem for an input consisting of L_k, R_k and I_k. (b) If (global) sets GL and GR are nonempty then solve the problem for an input consisting of $a + GL$, $a + GR$, and $J = a + [0..q-1]$, where the set $a + GR$ is defined as $\{a + k : k \in GL\}$.

Comments:

We solve the sorting problem in two steps:

(a) Compute the *domain right neighbor* of each index i.

(b) For each element $x[i]$, compute its rank r in the linked list defined by the *drn*, and let $\pi(r)$ be i.

Step (b) can be (trivially) done in $O(n)$ time or in parallel time $O(\log n)$ and optimal speed-up using a List Ranking algorithm ([AM88], [CV86], [CV88], [CV89]). Therefore, our main concern is solving the domain right neighbor problem. For simplicity we assume that $m = 2^{2^t}$ for some integer $t \geq 1$. The domain right neighbor, as defined above, is the nearest neighbor from the right. We will also need a definition of the *domain left neighbor*, $dln[i]$, of element $x[i]$: the element $x[j] = \max\{x[k] : x[k] < x[i]\}$.

2.1 Algorithm for finding Domain Nearest Neighbors

The algorithm is recursive. The main effort is in defining *precisely* the problem that is being solved recursively. The recursive algorithm will provide solutions for the problems of finding left and right domain nearest neighbors. For each element the recursive algorithm separately treats the domain right neighbor and the domain left neighbor computations. This is done by duplicating each element $x[i]$ into a *left copy* $x_l[i]$ and a *right copy* $x_r[i]$. Intuitively, copy $x_r[i]$ is "responsible" for finding the domain right neighbor and $x_l[i]$ is "responsible" for finding the domain left neighbor. Initially, $x_l[i] = x[i]$ and $x_r[i] = x[i]$.

In addition, two auxiliary copies are added: $x_r[n+1]$ and $x_l[n+1]$. Copy $x_r[n+1] = 1$ is the domain left neighbor of the smallest input element. Similarly, copy $x_l[n+1] = m$ is the domain right neighbor of the largest input element. (Note that at this stage only for $i = n+1$, $x_r[i]$ is not equal $x_l[i]$.) We assume, without loss of generality, that the input elements are from $[2..m-1]$.

Informally, our algorithm works as follows: The input elements are from an interval I. Interval I is partitioned into small intervals, defining local problems of domain nearest neighbors searches. For each subinterval I_k, at most two elements (smallest left copy and largest right copy) might not have their neighbors in I_k. Such elements are collected into the global sets GR and GL. Thus, a problem on interval I is reduced recursively into several local problems on subintervals I_k and one global problem. By choosing I_k to be of size $\sqrt{|I|}$ (for all k), we have that all local problems and the global problem are with intervals of size $\sqrt{|I|}$.

The input for the recursive algorithm includes two sets L and R, whose values belong to an interval I of integers. I is of the form $a + [1..m']$, i.e., $I = \{a+1, a+2, ..., a+m'\}$ for some within the CRCW PRAM. (2) At the same time, a dialogue between more pragmatic researchers and theoreticians should continue in order to investigate "free" strengthenings of the PRAM model; specifically, collective wisdom on what are the best approaches for various machine technologies ought to be developed. The existence of operations such as the addition of n numbers by n processors as primitive operations contradicts some fundamental intuition about what is computationally feasible in one parallel step versus what needs a more substantial computational effort. (Formally, an $\Omega(\log n/ \log\log n)$ time separation between the priority- and fetch&add-CRCW PRAMs can be derived from the lower bound of [Has86] and the simulation result of [SV84], or directly from the lower bound of [BH87].) Recognizing such partition into two separate, but related, approaches justifies studying the feasibility and power of such operations as a pragmatic line of investigation.

The contributions of the present paper fall within the first approach in the above comment.

Postscript. Recently Bhatt et al. [BDH+89] designed independently a parallel deterministic integer sorting algorithm which is related (though, not identical) to the basic construction of Section 2.1 below. Using a new list ranking algorithm they were even able to reduce the time to $O(\log n/ \log\log n + \log\log m)$ maintaining optimal speed-up. However, none of the randomized space reductions ideas of the present paper appear there.

2 The Deterministic Algorithm

We consider the following problem:

Input: Sequence $x[1], ..., x[n]$ of distinct integers drawn from the domain $[1..m]$, for some integer m. **Problem:** Sort the sequence. (Formally, compute the permutation π of $\{1, ..., n\}$ such that $x[\pi(1)], ..., x[\pi(n)]$ is sorted in non-decreasing order.)

In Section 2.3 we discuss a way for withdrawing the distinctness assumption.

For presentation purposes, we falsely assume that the sequence $x[1], ..., x[n]$ is given in the following redundant form. There is a *domain array* of bits $D[1..m]$ so that $D[i] = 1$ if the value of some element $x[j]$ is i and $D[i] = 0$ otherwise. Given bit $D[i] = 1$ we define the smallest $i_1 > i$ such that $D[i_1] = 1$ as the *right neighbor* of $x[i]$.

This neighborhood relation translates easily to the values of the input sequence: the *domain right neighbor* $drn[i]$ of $x[i]$ is the element $x[j] = \min\{x[k] : x[k] > x[i]\}$. The array drn defines a linked list, where the elements preceding $x[i]$ in the linked list are smaller than $x[i]$ and the elements succeeding $x[i]$ are larger. The distance from the beginning of the list is the *rank* of $x[i]$ relative to the input elements.

exchange for randomization and increase in time by a logarithmic factor, but with no change in the number of operations. The parallel hashing technique yields similar results when applied to parallel algorithms that build on suffix trees. Section 3.2 lists many examples, including the parallel approximate string matching algorithms mentioned in [GG88].

Parallel hashing can be useful for parallel object recognition algorithms. Hashing is used in [LW88], following [KSSS86], for object recognition. It is also used in computations of the Hough Transform (cf. [IK88]). The parallel hashing technique enables efficient parallel implementations of these algorithms.

The parallel hashing scheme may be used to reduce the space in Hagerup's sorting algorithm [Hag87] from $O(n^{1+\epsilon})$ to $O(n)$ in exchange for randomization and an $O(\log\log n)$ increase in time (but no change in number of operations). The parallel hashing scheme is also used in the optimal simulation in Section 4.

Recall that we use the non standard min-CRCW model in Section 2. Note that we do not advocate this model as an alternative for existing "acceptable" theoretical models for parallel computation (see also comment below). The methodological attitude here is: (1) design the algorithm on the min-CRCW model, and (2) show later how to simulate this model on more acceptable ones.

Comment. Since this paper refers to standard versus non standard models of parallel computation, we were asked to present our views on the following basic question. Which model should be considered as the fundamental model for parallel computation? A position on this issue is presented in the survey paper [Vis83b]. In that paper, two separate lines of justification for an answer to this question are suggested. (1) The first line of justification is *technology independent* and is based on computational equivalence among models of parallel computation. Computational equivalence among the priority-CRCW PRAM and the unbounded fan-in circuits (see Stockmeyer and Vishkin [SV84]) is used to support the choice of the priority-CRCW PRAM (and not other PRAM models) as the fundamental theoretical model for parallel computation. (2) The second line of justification is *technology dependent.* Assume that *any* parallel machine that conforms with some technological restrictions is given. [GGK+83], [Vis83a] and [Vis84], jointly advocate the choice of a most permissive abstract model of computation that can be simulated by such a parallel machine without increasing the cost of implementation (by more than a constant factor). [Vis83a] demonstrated this principle by proving (under some assumptions) the following. Consider any parallel machine which consists of processors that are connected in a fixed pattern. Then the time for simulating a step of a priority-CRCW PRAM is going to be asymptotically the same as simulating a step of a fetch&add-CRCW PRAM (and since finding the minimum is an associative and commutative binary operation, also of a min-CRCW PRAM). [Vis83b] implies also the following way for how research on parallel algorithms (and architectures) can reconcile the two approaches: (1) Theoretical computer scientists (primarily designers of parallel algorithms) should continue and search for new algorithmic patterns and ideas

Combining the optimal simulation from Section 4, the parallel hashing scheme in Section 3 and the algorithm in Section 2 we derive a randomized parallel algorithm for sorting n integers from the range $[1..m]$ on an arbitrary-CRCW that achieves $O(\log n \log\log m)$ expected time, $O(n \log\log m)$ expected number of operations and $O(n)$ space.

Not only the space efficient parallel sorting result can benefit from the simulations. Recall the original min-CRCW PRAM sorting algorithm of Section 2. Together with some of these simulations, we get the following deterministic sorting results on standard PRAM models: (1) $O(\log n \log\log m)$ time and $O(nm^{\epsilon})$ space (with any fixed $\epsilon > 0$) using $\frac{n \log\log n}{\log n}$ priority-CRCW processors; and (2) $O(\log n + (\log\log m)^2)$ time and $O(n^2 m^{\epsilon})$ space ($\epsilon > 0$) using $\frac{n(\log\log m)^2}{\log n}$ arbitrary-CRCW processors.

Some of the ideas we use in the deterministic algorithms of Section 2 go back to [vKZ77]. These ideas were inspired also by the algorithms of [Hag87] and [Joh82]. Johnson's algorithm has the same complexity as our deterministic serial algorithm. However, our sorting algorithm has two advantages: it is simpler and parallelizable.

The so called DNN algorithm of Section 2 implies efficient algorithms for the ordered chaining and for the ordered compaction problems, which are defined as follows. Given an array of size m, in which n entries are marked, the (unordered) *chaining* problem is to put the marked entries into a linked list. Assume that a processor is standing by each marked entry. The (unordered) *compaction* problem is the problem of moving the marked entries into consecutive memory locations. If the marked entries are required to remain in the same order, then the problems are called *ordered chaining* and *ordered compaction*, respectively. In [Spi88], [RS85], and [HN89] algorithms are given for the *unordered* chaining and the *unordered* compaction problems only.

The proposed parallel hashing scheme may be a useful tool for parallel algorithms that use large space. We demonstrate this with several algorithms (in addition to our sorting algorithm) for which the space requirement is large. By using the proposed parallel hashing scheme, they become efficient and possibly practical.

There are applications that relate to combinatorial algorithms on strings. If the alphabet is large then a naming assignment procedure for substrings is essential to avoid large space. Such deterministic procedure, due to [GG88], takes $O(n \log n)$ operations and evaluation of a name takes $O(\log n)$ time. (We actually referred earlier to the same procedure.) Using our parallel hashing scheme, the naming assignment takes $O(n)$ expected number of operations and evaluation of a name takes $O(1)$ time in the worst case.

An important technique for string matching algorithms was introduced by Karp, Miller and Rosenberg [KMR72]. Suppose an input string of length m is given. [AIL$^+$88] showed how to parallelize this technique and used it for parallel construction of a suffix tree in $O(\log m)$ parallel time, $O(m \log m)$ work and $O(m^{1+\epsilon})$ space for $\epsilon > 0$. Using our parallel hashing technique, *the space requirements in each of these algorithms can be reduced to linear, in*

A parallel version of this deterministic algorithm takes $O(\log n)$ time and $O(nm^{1/c})$ space, for any fixed $c \geq 1$, using $n \log\log m / \log n$ processors (optimal speed-up). This parallel algorithm is designed for the nonstandard min-CRCW PRAM.

The second element in our presentation is described in Section 3. A randomized parallel hashing scheme is presented. It is optimal and takes logarithmic time. Specifically, let W be a given set of n numbers from an arbitrary large domain $[1..m]$. We show how to find a one-to-one mapping $F : W \mapsto R$, where $|R| = O(n)$, by a randomized algorithm on the arbitrary-CRCW PRAM. This mapping is computed in $O(\log n)$ expected time, using $\frac{n}{\log n}$ processors. Evaluation of $F(x)$, for each $x \in W$, takes $O(1)$ worst case time. The connection to the sorting results is as follows. We show how to use these hash functions in order to reduce the space requirements in both the serial and parallel algorithms to only $O(n)$ space. The penalty is that now we have randomized algorithms rather than deterministic algorithms. For the parallel algorithm, the parallel time increases to $O(\log n \log\log m)$ while, the operation count does not increase (asymptotically) on the min-CRCW model. Thus, our parallel randomized sorting algorithm is slower by an $O(\log\log m)$ factor than standard PRAM comparison sorting algorithms; however, it is more efficient by a factor of $O(\log n / \log\log m)$.

The third element in our presentation is described in Section 4. Simulations of the min-CRCW PRAM model by weaker models are presented. Some of the simulations are randomized. Some simulations apply also to the fetch&add-CRCW model.

Denote a CRCW PRAM with a shared memory of size S as *CRCW(S)* PRAM. In the following, we list some upper bounds for simulating one step of an n-processor min-CRCW(S) PRAM:

- $O(\log n)$ expected time on an $\frac{n}{\log n}$-processor arbitrary-CRCW($S + O(n)$) PRAM (optimal speed-up).
- $O(\log n)$ time on an $\frac{n \log\log n}{\log n}$-processor priority-CRCW($O(S + n^{1+\epsilon})$) PRAM ($\epsilon > 0$).
- $O(\log\log m)$ time on an n-processor arbitrary-CRCW($O(mS)$) PRAM, where m is an upper bound for the value that can be written to a memory cell by the min-CRCW PRAM.

The first result is an improvement over a previously known result [EG88] where there was a restriction that the memory addresses being used by the simulated min-CRCW are of at most $O(\log n)$-bit size. The result can be extended to simulating one step of a fetch&add-CRCW PRAM. We are not aware of similar (i.e., optimal simulation) results even for simulation of the (relatively weaker) priority-CRCW PRAM by an arbitrary-CRCW PRAM. The last two simulations are deterministic. The third result is based on the simulation of priority-CRCW by arbitrary-CRCW in [CDHR88].

$O(\lceil(\log S(n)+1)/\log B(n)\rceil)$. For $B(n)=2$ the space is reduced to $O(P(n)T(n))$ while the time (and therefore the number of operations) is increased by a factor of $O(\log S(n))$. Note that the 2-3 tree parallel algorithm of [PVW83] can be used to get a factor of $O(\log(P(n)T(n)))$. Recently, [DM89] described a dynamic data structure (dictionary) that using randomization supports the instructions *insert*, *delete* and *lookup*, and can be implemented in parallel. Their implementation preserves optimal speed-up with time bounds of the form $O(n^\epsilon)$ using $\leq n^{1-\epsilon}$ processors, for any fixed $\epsilon > 0$. However, no time bounds of the form $O(polylog(n))$ are claimed.

Several works have been previously done on relations between PRAM models. The interested reader is referred to the surveys of [EG88] [KR88] [Vis83b]. Randomization was previously used in the context of parallel simulations by [KU86] [KRS88] [MV84] [Ran87].

1.2 More on our results

As model of computation for the parallel algorithms, we use mostly the concurrent-read concurrent-write parallel random access machine (CRCW PRAM) family. The members of this family differ by outcome of the event where several processors attempt to write simultaneously into the same shared memory location. In the common-CRCW ([SV81]) all these processors must attempt to write the same value (and this value is written). In the arbitrary-CRCW ([SV82a]) one of the processors succeeds, but we do not know in advance which one. In the priority-CRCW ([Gol82]) the smallest numbered among the processors succeeds. The above three CRCW models are considered standard. Next we mention two non standard models. In the min-CRCW PRAM ([AS83]) the processor that tries to write the minimum value succeeds. In the fetch&add-CRCW PRAM ([Vis83a]) the values are added to the value already written in the shared memory location and all sums obtained in the (virtual) serial process are recorded. Finally, in an exclusive-read exclusive-write (EREW) PRAM simultaneous access of more than one processor into the same shared memory location is not allowed.

A parallel algorithm achieves optimal speed-up if its time$\times$processor product matches the number of operations of the fastest serial algorithm for the problem. Typically, we will state our parallel results in the following form: "x operations and t time". Throughout this paper, this will always translate into "t time using x/t processors". The papers [EG88], [KRS88], [KR88] and [Vis83b] overview research directions on parallel algorithms. All of them concede that achieving optimal speed-up, or at least approaching this goal, is a crucial property for parallel algorithms that are intended to be practical. A secondary (but very important) goal is to minimize parallel time. Another critical practical concern is space requirements. These guidelines led us in designing the algorithms of the present paper.

Our algorithms are presented as follows. We first present in Section 2 a deterministic algorithm that takes $O(n \log\log m)$ time and uses $O(nm^{1/c})$ space, for any fixed $c \geq 1$.

problem, where the input consists of integers drawn from a restricted interval $[1..m]$. For $m = O(n)$ the known Bucket Sort algorithm applies. It solves the problem in $O(n)$ time. For $m = poly(n)^1$ the variant of the Bucket Sort algorithm, called Radix Sort, runs in $O(n)$ time [Knu73]. More precisely, Radix Sort runs in $O(n \log_n m)$ time. Thus, a natural extension of the Radix Sort would result with an $o(n \log n)$ time algorithm for $m \leq n^{o(\log n)}$. However, for $m = n^{\Omega(\log n)}$ Radix Sort does not improve on the $O(n \log n)$ time bound.

The second approach was studied for parallel computation as well. Rajasekaran and Reif gave an optimal randomized parallel algorithm in logarithmic time on an arbitrary-CRCW for $m = n \log^c n$, for any constant $c \geq 1$ [RR89]. The integer sorting algorithm of Rajasekaran and Reif cannot be extended for m polynomial in n. For $m = poly(n)$, Hagerup provided an $O(\log n)$ time and $O(n^{1+\epsilon})$ space (for any fixed $\epsilon > 0$) parallel algorithm, using $n \log \log n / \log n$ priority-CRCW processors [Hag87]. No optimal parallel algorithm is known for this range. Our sorting algorithm clearly belongs in the second approach.

Using data structures presented by van Emde Boas, Kaas and Zijlstra [vKZ77], Johnson [Joh82] dealt with priority queues problems, where the priorities are drawn from the integer domain $[1..m]$. A corollary of his result is an $O(n \log \log m)$ time and $O(m^{1/c})$ space algorithm for sorting, where $c > 0$ is a constant. Johnson recognizes the problem with the space requirements of the algorithm, and writes that the algorithm is not practical and only of theoretical interest.

Kirkpatrick and Reisch [KR84] presented an algorithm, based on a range reduction technique, that has the same complexity bounds as Johnson's algorithm. They state that the algorithm is of little practical value due to both large constants, that are hidden in the asymptotic bounds, and storage requirements.

The following open question, quoted from Kirkpatrick and Reisch ([KR84]), captures an important aspect of our sorting results: "For what ranges of inputs can we construct practical $o(n \log n)$ integer sorting algorithms?". The present paper provides only partial answers to this question, and more work is still needed in order to resolve this question.

The issue of trading space for randomness using random hash functions belongs in the folklore of serial algorithms. For instance, the survey paper [GG88] demonstrates such considerations for hashing large alphabets for string algorithms such as the suffix tree data structure. However, for parallel algorithms this survey mentions only deterministic methods. This immediately suggests an implicit open problem.

Hagerup considered algorithms in which the space requirement $S(n)$ is larger than the number of operations $P(n)T(n)$ [Hag88]. He provided a deterministic modification algorithm that reduces the space to $O(P(n)T(n)B(n))$, for any function $B(n) \geq 2$. In the modified algorithm the number of processors remains $P(n)$, while the time increases by a factor of

^{1}We use $poly(n)$ to denote "polynomial in n", and $polylog(n)$ to denote "polynomial in $\log n$".

1 Introduction

Consider the problem of sorting n integers drawn from a given range $[1..m]$. A new randomized algorithm for the problem is presented. Its expected running time is $O(n \log\log m)$ using $O(n)$ space. The algorithm is parallelizable. The resulting parallel algorithm achieves optimal speed-up. The result implies $o(n \log n)$ expected time and linear space for $m \leq 2^{n^{o(1)}}$. More specifically, for $m = n^{\log^k n}$ (for any constant $k \geq 1$) we have $O(n \log\log n)$ expected time and $O(n)$ space. No such result is known for deterministic sorting, suggesting the following *fundamental open problem* : Is this an instance where randomization defeats determinism for sorting?

The paper employs two *Algorithmic techniques*:

1. A first randomized parallel hashing technique, which achieves optimal speed-up and takes expected logarithmic time, is presented. The parallel hashing technique enables *drastic* reduction of space requirements in quite a few parallel algorithms for the price of using randomness. The technique is used in the parallel sorting algorithm. Such (serial) technique is also demonstrated in the serial sorting algorithm. The new parallel hashing technique, that results in trading space for randomness, is likely to have additional applications. We actually demonstrate it with a few examples.

2. The parallel sorting algorithm is designed for a strong and non standard model of parallel computation. New simulations of the strong model on a CRCW PRAM are introduced. Using one of the simulations the parallel sorting algorithm runs in optimal speed-up also on a CRCW PRAM. Designing algorithms for strong and non standard models of computation and then translate them into standard models is a traditional methodology in computer science. We expect our parallel simulations to be helpful in this respect. The simulations are efficient: one of them even preserves optimal speed-up.

1.1 Extant work

Sorting is a fundamental problem that has received much attention. [Knu73] gives several algorithms for sorting n objects drawn from an arbitrary totally ordered domain in $O(n \log n)$ time. There are also optimal parallel sorting algorithms in logarithmic time [AKS83] [Col86]. For the decision-tree model the $O(n \log n)$ time serial upper bound is best possible [AHU74].

Because of the central role that the sorting problem plays in computer science, numerous papers are devoted to study opportunities for improving this time bound to $o(n \log n)$. One approach is to consider idealized (and non standard) versions of the RAM model; as, for instance, in [KR84] and [PS80], where very large words are assumed. The practicality of such an assumption is unclear. Another approach is to focus on instances of the sorting

On Parallel Hashing and Integer Sorting[*]

Yossi Matias Uzi Vishkin[†]

Tel-Aviv University &
University of Maryland

(December 1989. Revised: August 1990)

Abstract

The problem of sorting n integers from a restricted range $[1..m]$, where m is superpolynomial in n, is considered. An $o(n \log n)$ randomized algorithm is given. Our algorithm takes $O(n \log\log m)$ expected time and $O(n)$ space. (Thus, for $m = n^{polylog(n)}$ we have an $O(n \log\log n)$ algorithm.) The algorithm is parallelizable. The resulting parallel algorithm achieves optimal speed up. Some features of the algorithm make us believe that it is relevant for practical applications.

A result of independent interest is a parallel hashing technique. The expected construction time is logarithmic using an optimal number of processors, and searching for a value takes $O(1)$ time in the worst case. This technique enables drastic reduction of space requirements for the price of using randomness. Applicability of the technique is demonstrated for the parallel sorting algorithm, and for some parallel string matching algorithms.

The parallel sorting algorithm is designed for a strong and non standard model of parallel computation. Efficient simulations of the strong model on a CRCW PRAM are introduced. One of the simulations even achieves optimal speed up. This is probably a first optimal speed up simulation of a certain kind.

[*]Appeared in *Journal of Algorithms* 12, 573–606 (1991). A preliminary version of this paper was presented at the 17th International Colloquium on Automata, Languages and Programming (ICALP), Warwick, England 1990.

[†]Partially supported by NSF grant CCR-890649 and ONR grant N00014-85-0046.