LECTURE NOTES ON THE NEW AKS SORTING NETWORK

V. Chvátal

Computer Science Department,

Rutgers University

New Brunswick, NJ 08903, USA

Abstract

Ajtai, Komlós, and Szemerédi constructed sorting networks with N wires of depth $O(\log N)$. They were not concerned with the value of the proportionality constant implicit in the O-notation; subsequently Paterson replaced the $O(\log N)$ by $c \log_2 N$ with c under 6100. We describe an implementation of a more recent, and as yet unpublished, proposal of Ajtai, Komlós, and Szemerédi, that yields a smaller value of c: for every integer N such that $N \geq 2^{78}$ there is a sorting network on N wires whose depth is at most $1830 \log_2 N - 58657$.

The basic units in this new construction are sorting networks on M wires such that M is relatively small; these may be thought of as indivisible hardware elements (rather than networks made from comparators); following Knuth, we call them *M-sorters*. For every choice of positive integers M and N such that $N \geq M$, the construction yields a sorting network on N wires, made from M-sorters, whose depth is at most $(48 + o(1)) \log_M N + 115$ as $M \to \infty$. (It is worth emphasizing that the asymptotic $o(1)$ here is relative to M rather than N.)

1 INTRODUCTION

We assume familiarity with the notion of a sorting network ([5], Section 5.3.4). Ajtai, Komlós, and Szemerédi [1,2] constructed sorting networks with N wires of depth $O(\log N)$. They were not concerned with the value of the proportionality constant implicit in the O-notation; subsequently Paterson [7] replaced the $O(\log N)$ by $c \lg N$ with c under 6100. (We write *lg* for the logarithm to the base 2 and *ln* for the natural logarithm.) The purpose of these lecture notes is to describe an implementation of a more recent, and as yet unpublished, proposal of Ajtai, Komlós, and Szemerédi, that yields a smaller value of c.

THEOREM 1.1 *For every integer N such that $N \geq 2^{78}$ there is a sorting network on N wires whose depth is at most* $1830 \lg N - 58657$. □

The basic units in this new construction are sorting networks on M wires such that M is relatively small; these may be thought of as indivisible hardware elements (rather than networks made from comparators); following Knuth ([5], Exercise 44 in Section 5.3.4), we call them *M-sorters*.

THEOREM 1.2 *For every choice of positive integers M and N such that $N \geq M$ there is a sorting network on N wires, made from M-sorters, whose depth is at most*
$(48 + o(1)) \log_M N + 115$ *as $M \to \infty$.* □

It is worth emphasizing that the asymptotic $o(1)$ in Theorem 1.2 is relative to M rather than N. (In particular, a special case of the theorem asserts that, for all M, there are sorting networks on M^2 wires, made from M-sorters, whose depth is constant. Knuth asked whether such networks exist for all M. An earlier affirmative answer is implicit in a work of Leighton [6]; his algorithm *columnsort* provides a sorting network om $2s^3$ wires, made from $2s^2$-sorters, whose depth is four; applying this result twice in a recursive fashion yields a sorting network on $2s^{9/2}$ wires, made from $2s^2$-sorters, whose depth is 16.)

2 THE TREE PARADIGM AND SEPARATORS

To motivate the construction, we define a *perfect separator* as a network with output wires split into k blocks of equal sizes such that, given any input consisting of a distinct keys, the network places the a/k smallest keys in the first block, the next a/k smallest keys in the next block, and so on. Perfect separators may be used as modules to construct a sorting network with N wires such that $N = k^d$ for some positive integer d. This network is a series composition of networks $N_0, N_1, \ldots, N_{d-1}$ such that each N_t is a parallel composition of k^t perfect separators of equal sizes; the k^{d-t} output wires of each perfect separator in N_t are split into k blocks of equal sizes and each of these blocks forms the input of a perfect separator in N_{t+1}.

We shall find it useful to interpret this construction in different terms. The k^d addresses of the input keys will be thought of as the leaves of a complete k-ary tree of depth d; each module (a perfect separator) in N_t will be assigned to a node on the t-th level of the tree. Thus, at each time $t = 0, 1, \ldots, d-1$, the k^d wires are distributed throughout the t-th level of the tree. At this time, each node x on the t-th level contains k^{d-t} wires; these wires are used as inputs of a perfect separator whose output wires are split into k blocks of equal sizes; between times t and $t+1$, the wires from the j-th output block are sent down to the j-th child of x. At time d, each leaf of the tree contains a single wire and this wire holds a key addressed to the leaf.

Unfortunately, this scheme yields sorting networks of depth $\Omega((\log_k N)(\log_M N))$: every perfect separator with a wires made from M-sorters must have depth greater than $\log_M(\frac{k-1}{k}a)$. (To see this, note that for each output y, there must be more than $\frac{k-1}{k}a$ inputs x such that a key can travel from x to y.) Fortunately, the scheme can be modified to yield sorting networks of depth $O(\log_M N)$: the perfect separators are replaced by weaker modules of constant depth, whose weakness is made up for by a more complicated movement of the N registers through the tree.

The weaker modules will be called *separators*. Each of them has its a output wires split

into blocks $F_1, B_1, B_2 \ldots, B_k, F_2$ such that

$$\mid F_1 \mid = \mid F_2 \mid \qquad \text{and} \qquad \mid B_1 \mid = \mid B_2 \mid = \ldots \mid B_k \mid;$$

typically, the "fringe blocks" F_1 and F_2 are far smaller than the remaining blocks $B_1, B_2, \ldots, B_k$. In a sense, the separator approximates a perfect separator; the quality of the approximation is measured by certain numbers δ_F, ε_F, and ε_B. A sorting network with the same output wires as the separator would, given any input I consisting of a distinct keys, place some set I_j of keys into each output block B_j. The separator distributes I through the output wires in such a way that

(i) for each $j = 1, 2, \ldots, k$, at most $\varepsilon_B a$ of the keys in I_j are placed outside B_j,

(ii) for each integer j such that $1 \leq j \leq \delta_F \mid F_i \mid$, at most $\varepsilon_F j$ of the j smallest keys are placed outside F_1 and at most $\varepsilon_F j$ of the j largest keys are placed outside F_2.

As for the movement of the wires through the tree, all the k^d wires are placed in the root at time $t = 0$. Between times t and $t + 1$, each node x that contains any wires at all uses these a wires as the input of a separator with judiciously chosen sizes of the output blocks; the wires from each output block B_j are sent down to the j-th child of x and the wires from $F_1 \cup F_2$ are sent back up to the parent of x. (If x is the root then F_1 and F_2 are both empty.) Since F_1 and F_2 are relatively small, most of the wires trickle down towards the leaves of the tree; since the separator is not perfect, some keys may be sent down in a wrong direction; property (i) guarantees that only a relatively few keys go astray with each iteration; property (ii) guarantees that most of these stray keys will back up again, so that they may correct the wrong turn later on.

In the next section, we specify the sizes of the output blocks in each of the separator modules; in the section following the next, we prove that the resulting network sorts, provided that the separators are of a good enough quality. Construction of the separators will be taken up later on.

3 CONSTRUCTION OF THE NETWORK

We choose k, the branching factor of the tree, to be a power of two and write $N = k^d$ for the number N of input keys. At each time t, the N wires are distributed throughout the tree in such a way that the actual number of wires contained in a node x depends only on t and on the depth i of x; we let $a(i,t)$ denote this number. The values of $a(i,t)$ are controlled by two parameters, A and ν; these are powers of two such that $\nu < 1$ and $A\nu > 1$.

In the beginning, all the wires are contained in the root:

$$a(0,0) = N.$$

Between $t = 0$ and $t = 1$, the root splits the set of N wires into k equal parts and sends them down to its k children:

$$a(1,1) = N/k.$$

Between $t = 1$ and $t = 2$, each node on level 1 sends $N\nu/Ak^2$ of its N/k wires back to the root and distributes the remaining wires evenly among its children:

$$a(0,2) = \frac{\nu}{Ak}N \qquad \text{and} \qquad a(2,2) = \frac{Ak-\nu}{Ak^3}N.$$

Let $\alpha(t)$ and $\omega(t)$ denote the top and the bottom level, respectively, that contain nonempty nodes at time t: formally, $\alpha(t)$ is the smallest i with $a(i,t) \neq 0$ and $\omega(t)$ is the largest i with $a(i,t) \neq 0$. Thus

$$\alpha(0) = \omega(0) = 0; \quad \alpha(1) = \omega(1) = 1; \quad \alpha(2) = 0, \ \ \omega(2) = 2.$$

By the time $t = 2$, the top and the bottom have separated; they will remain apart until some time t_f when they meet again and the movement of the wires ceases.

Writing

$$\alpha^*(t) = \frac{t \log \frac{1}{\nu} - \log N + \log(2A\nu k^3)}{\log A}$$

and

$$\omega^*(t) = \frac{t \log \frac{1}{\nu} + \log(A\nu k)}{\log(Ak)},$$

we let $\alpha(t)$ be the smallest nonnegative integer such that

$$\alpha(t) \geq \alpha^*(t), \quad \alpha(t) \equiv t \bmod 2$$

and we let $\omega(t)$ be the smallest integer such that

$$\omega(t) \geq \omega^*(t), \quad \omega(t) \equiv t \bmod 2.$$

Since $A\nu \geq 1$, we have $\alpha^*(t+1) \leq \alpha^*(t) + 1$, $\omega^*(t+1) \leq \omega^*(t) + 1$ for all t, and so

$$\mid \alpha(t+1) - \alpha(t) \mid = 1, \quad \mid \omega(t+1) - \omega(t) \mid = 1$$

for all t. Thus the bottom descends in a zig-zag fashion at the average speed of $\log \frac{1}{\nu}$ levels per $\log(Ak)$ iterations; the top initially oscillates between levels 0 and 1 for about $\log N / \log \frac{1}{\nu}$ iterations and then it begins its own zig-zag descent at the average speed of $\log \frac{1}{\nu}$ levels per $\log A$ iterations. Let t_f denote the time when the top catches up with the bottom: t_f is the largest integer such that

$$\alpha(t) < \omega(t) \quad \text{whenever} \quad 1 < t < t_f,$$

and so $\alpha(t_f) = \omega(t_f)$. (It will follow from our subsequent exposition, and it can be checked directly, that the common value of $\alpha(t_f)$ and $\omega(t_f)$ is less than d.)

To specify the values of $a(i,t)$ with $1 < t < t_f$, we shall find it convenient to write

$$c(i,t) = \frac{N}{A\nu k} A^i \nu^t.$$

Each $c(i,t)$ may be thought of as the capacity of a node on level i at time t: for each t such that $1 < t < t_f$, we have

$$\frac{a(\alpha(t),t)}{c(\alpha(t),t)} = 1,$$

$$\frac{a(i,t)}{c(i,t)} = 1 - \frac{1}{A^2k^2} \quad \text{whenever} \quad \alpha(t) < i < \omega(t) \quad \text{and} \quad i \equiv t \bmod 2,$$

$$a(\omega(t),t) = Nk^{-\omega(t)} - \frac{c(\omega(t),t)}{A^2k^2}.$$

(If $i \not\equiv t \bmod 2$ then $a(i,t) = 0$.) Since

$$Nk^{-\omega(t)} \le c(\omega(t),t) < A^2k^2Nk^{-\omega(t)},$$

we have

$$0 < \frac{a(\omega(t),t)}{c(\omega(t),t)} \le 1 - \frac{1}{A^2k^2}.$$

Since $c(\alpha(t),t) \ge 2k^2$, we have $c(i,t) \ge 2A^2k^2$ whenever $i \ge \alpha(t)+2$; it follows that all $a(i,t)$ are even integers.

To relocate the wires between times t and $t+1$, each node on level i sends $\pi(i,t)$ wires to its parent and $\chi(i,t)$ wires to each of its k children. When $2 \le t < t_f$, we have

$$\pi(\alpha(t),t) = \begin{cases} 0 & \text{if } \alpha(t+1) > \alpha(t), \\ \dfrac{\nu}{Ak}c(\alpha(t),t) & \text{if } \alpha(t+1) < \alpha(t), \end{cases}$$

$$\pi(i,t) = \frac{A\nu k - 1}{A^2k^2}c(i,t) \qquad \text{if } \alpha(t) < i < \omega(t),$$

$$\pi(\omega(t),t) = \begin{cases} \dfrac{A\nu k - 1}{A^2k^2}c(\omega(t),t) & \text{if } \omega(t+1) > \omega(t), \\ a(\omega(t),t) & \text{if } \omega(t+1) < \omega(t), \end{cases}$$

$$\chi(\alpha(t),t) = \begin{cases} \frac{1}{k}c(\alpha(t),t) & \text{if } \alpha(t+1) > \alpha(t), \\ \dfrac{Ak - \nu}{Ak^2}c(\alpha(t),t) & \text{if } \alpha(t+1) < \alpha(t), \end{cases}$$

$$\chi(i,t) = \frac{Ak - \nu}{Ak^2}c(i,t) \qquad \text{if } \alpha(t) < i < \omega(t),$$

$$\chi(\omega(t),t) = \begin{cases} a(\omega(t+1),t+1) & \text{if } \omega(t+1) > \omega(t), \\ 0 & \text{if } \omega(t+1) < \omega(t)\ . \end{cases}$$

Note that all $\pi(i,t)$ and all $\chi(i,t)$ are even integers: in particular, if $\alpha(t+1) < \alpha(t)$ then $c(\alpha(t),t) = (A/\nu)c(\alpha(t+1),t+1) \geq 2Ak^2/\nu$.

If the separator modules used throughout the network are good enough then (as we shall prove in the next section) there is an integer γ, at most $\alpha(t_f)$ but differing from $\alpha(t_f)$ by at most a constant independent of N, such that, for each node x on level γ, all the keys located in descendants of x at time t_f are addressed to leaves that are descendants of x. Hence the network can be completed by a single layer of parallel sorting networks, each of which has $k^{d-\gamma}$ wires.

The policy of keeping $a(i,t)$ proportional to $NA^i\nu^t$ whenever $\alpha(t) < i < \omega(t)$ was advocated (in the special case $k = 2$) by Paterson [7]; the notation A, ν used in this section is his, as is the notation μ, δ used in the next section. When $k = 2, A = 4, \nu = 1/2$, and $d \equiv 0 \bmod 4$, our network reduces to that constructed by Pippenger [8] except for two minor details. (First, his network lags two steps behind ours in the sense that his $a(i,t)$ equals our $a(i,t-2)$ whenever $t \geq 3$; second, even though the top and the bottom meet when his t equals $3d - 18$, he carries on for three additional steps till the top and the bottom meet again.)

The following facts will be used later on.

LEMMA 3.1 *If $a(i,t) \neq 0$ then*

$$\sum_{j=i}^{d} k^{j-i} a(j,t) \;=\; \begin{cases} Nk^{-i} & \text{if } i = \alpha(t), \\ Nk^{-i} - \dfrac{c(i,t)}{A^2k^2} & \text{if } i > \alpha(t). \end{cases}$$

PROOF. This follows from the identity

$$\sum_{j=0}^{d} k^j a(j,t) = N$$

directly when $i = \alpha(t)$ and by substituting

$$a(j,t) = \begin{cases} 0 & \text{if } j \not\equiv i \bmod 2 \\ c(j,t) & \text{if } j = \alpha(t) \\ (1 - \dfrac{1}{A^2k^2})c(j,t) & \text{if } \alpha(t) < j < i, \quad j \equiv i \bmod 2 \end{cases}$$

with $c(j,t) = c(i,t)A^{j-i}$ when $i \geq \alpha(t) + 2$. □

LEMMA 3.2 *If* $\alpha(t+1) > \alpha(t)$ *then* $\alpha(t) = 0$ *or* $c(\alpha(t), t) \leq Ak^2/\nu$.

PROOF. If $\alpha(t+1) > \alpha(t) > 0$ then $\alpha(t) - 1 < \alpha^*(t+1)$, and so $c(\alpha(t), t) < 2Ak^2/\nu$. Since both sides of the last inequality are powers of two, the desired conclusion follows. □

4 ANALYSIS OF THE NETWORK

This section follows the lines of Paterson [7]. An *outsider* is a key located in a node x but not addressed below x; an *outsider of order* r is an outsider that would remain an outsider even if it were moved to the ancestor of its current location that is r levels higher up in the tree. (Thus "outsider" is synonymous with "outsider of order zero".)

We aim to prove that at time t_f nodes on level $\alpha(t_f)$ contain no outsiders of order r for some constant r (depending only on k, A, ν). For this purpose, consider the following proposition,

P: For all $i = 0, 1, \ldots, d$ and for all $r = 0, 1, \ldots, d$, each node on level i contains fewer than $\mu\delta^r c(i, t)$ outsiders of order r.

Since $c(\alpha(t_f), t_f) < 2A^2k^2$, we only need prove that **P** holds at time t_f for some μ and δ (depending only on k, A, ν) such that $\delta < 1$.

We propose to use induction on t to show that **P** holds at all times $t = 0, 1, \ldots, t_f$ for some suitable choice of μ and δ (depending only on k, A, ν) such that $\delta < 1$. This can be done only if the separator modules used throughout the network are good enough; assuming that all these separators except the one used in the root at time $t = 0$ have the same parameters ε_B, δ_F, ε_F and that the exceptional separator has ε_B replaced by some ε^*, we shall derive conditions on $\mu, \delta, \varepsilon_B, \delta_F, \varepsilon_F, \varepsilon^*$ that will allow the induction on t to carry through.

The bulk of the induction step consists of showing that only a few of the keys a node u sends to its child v are not addressed below v (Lemma 4.2); this is possible only if u contains sufficiently many keys addressed below v. We begin by showing that u contains not too many keys addressed below siblings w of v.

LEMMA 4.1 *let u be a node on level i and let w be a child of u. If* **P** *holds at time t such that $\omega(t) > i$ then at this time u contains fewer than*

$$(\frac{1}{k} + \frac{\mu\delta k A^2}{1 - \delta^2 k^2 A^2})c(i,t)$$

keys addressed below w.

PROOF. Lemma 3.1 (with $i+2$ in place of i) guarantees that precisely

$$\frac{1}{k}(Nk^{-i} - c(i,t))$$

wires are located below w at time t ; since **P** holds at this time, at most

$$\sum_{j\geq 1} k^{2j-1}\mu\delta^{2j-1}c(i+2j,t)$$

of these wires holds keys addressed not below w. The desired conclusion follows by observing that

$$\begin{aligned}\sum_{j\geq 1}(k\delta)^{2j-1}c(i+2j,t) &= c(i,t)\sum_{j\geq 1}(k\delta)^{2j-1}A^{2j} \\ &< c(i,t).\frac{\delta k A^2}{1-\delta^2 k^2 A^2}\end{aligned}$$

and that precisely $\frac{1}{k}Nk^{-i}$ of the N input keys are addressed below w. □

LEMMA 4.2 *Let u be a node on level i and let v be a child of u. If* **P** *holds at time t such that $t \geq 1$ then u sends to v between times t and $t+1$ fewer than*

$$(\mu + (k-1)\frac{\mu\delta k A^2}{1-\delta^2 k^2 A^2} + \frac{A\nu k - 2A\nu + 1}{2k^2A^2} + \varepsilon_B)c(i,t)$$

keys that are not addressed below v.

PROOF. Write

$$c = c(i,t), \quad a = a(i,t), \quad \pi = \pi(i,t), \quad \chi = \chi(i,t),$$

$$\Delta_1 = \frac{\mu\delta k A^2}{1-\delta^2 k^2 A^2}c, \quad \Delta_2 = \frac{\nu}{Ak^2}c,$$

and

$$\Delta = \begin{cases} \Delta_1 & \text{if } i = \alpha(t) < \alpha(t+1) \\ \Delta_2 & \text{if } i = \omega(t) < \omega(t+1) \\ \Delta_1 + \Delta_2 & \text{if } \alpha(t) < i < \omega(t) \quad \text{or} \quad i = \alpha(t) > \alpha(t+1) \text{ with } t \geq 2. \end{cases}$$

Note that , for each child w of u,

u contains at most $\chi + \Delta$ keys addressed below w :

this follows from Lemma 4.1 if $i < \omega(t)$ and from the fact that precisely $\frac{1}{k}Nk^{-i}$ input keys are addressed below w if $i = \omega(t) < \omega(t+1)$.

Now let $F_1, B_1, B_2, \ldots, B_k, F_2$ be the output blocks of the separator module used at u between times t and $t+1$. If the module sorted then it would place in each B_j fewer than $\mu c + (k-1)\Delta - \frac{1}{2}\pi$ keys that are not addressed below the j-th child of u; since the module is only a separator, an additional $\varepsilon_B a$ keys not addressed below the j-th child of u may intrude into B_j; since $t \geq 1$, we have $a \leq c$.

Finally, we only need observe that

$$(k-1)\Delta - \frac{1}{2}\pi \leq (k-1)\Delta_1 + \frac{A\nu k - 2A\nu + 1}{2A^2k^2}c.$$

□

LEMMA 4.3 *If* **P** *holds at time* t *and if*

$$\varepsilon^* \leq \mu/k, \tag{4.1}$$

$$(\mu + (k-1)\frac{\mu\delta k A^2}{1-\delta^2k^2A^2} + \frac{A\nu k - 2A\nu + 1}{2A^2k^2} + \varepsilon_B)\frac{1}{A\nu} + \mu\delta\frac{Ak}{\nu} \leq \mu \tag{4.2}$$

then each node on level $i+1$ *contains fewer than* $\mu c(i+1, t+1)$ *outsiders at time* $t+1$.

PROOF: Let v be a node on level $i+1$ and let u be the parent of v. If $t = 0$ then we may assume $i = 0$; now u sends fewer than $\varepsilon^* N$ outsiders to v. If $t \geq 1$ then Lemma 4.2 provides an upper bound on the number of outsiders in v that have been sent from u between times t and $t+1$; each remaining outsider in v must have been sent from one of the k children of v, where it was an outsider of order 1. □

LEMMA 4.4 *Let r be a positive integer. If* **P** *holds at time t and if*

$$\mu \leq \frac{\nu}{Ak^2}, \tag{4.3}$$

$$\mu \leq \frac{1}{2}\delta_F \frac{A\nu k - 1}{A^2 k^2}, \tag{4.4}$$

$$\varepsilon_F \frac{1}{A\nu} + \delta^2 \frac{Ak}{\nu} \leq \delta \tag{4.5}$$

then each node on level $i+1$ contains fewer than $\mu\delta^r c(i+1, t+1)$ outsiders of order r at time $t+1$.

PROOF. Let v be a node on level $i+1$ and let u be the parent of v . Each outsider of order r in v has been sent either from u, where it was an outsider of order $r-1$, or from one of the k children of v, where it was an outsider of order $r+1$. If u contains at time t any outsiders then $c(i,t) > Ak^2/\nu$ by (4.3), and so

$$\frac{\pi(i,t)}{c(i,t)} \geq \frac{A\nu k - 1}{A^2 k^2}$$

by Lemma 3.2; in turn, (4.4) guarantees that u contains at most $\delta_F \cdot \frac{1}{2}\pi(i,t)$ outsiders of order $r-1$; hence at most $\varepsilon_F \cdot \mu\delta^{r-1} c(i,t)$ of these outsiders get sent to v. □

The findings of this section can be summarized as follows:

LEMMA 4.5 *If (4.1) - (4.5) hold and if*

$$\mu\delta^r c(\alpha(t_f), t_f) \leq 1$$

then at time t_f there are no outsiders of order r. □

5 CONSTRUCTION OF THE SEPARATORS

For each M such that

$$M \geq 32A^2k^2, \tag{5.1}$$

the separators required in Section 3 will be implemented by M-sorter networks of depth two in such a way that the quality of the separator improves as M increases (with δ_F fixed anywhere below 1/25, both ε_B and ε_F tend to zero as M tends to infinity), and so the standards set in Section 4 are met for all sufficiently large M.

Consider the separator used at time t in a node on level i; write $a = a(i,t)$, so that the separator has a wires. If $a \leq M$ then the separator can be implemented as a single M-sorter; hence we may assume that $a > M$. Under this assumption, we propose to find integers m and n such that

$$a = mn, \quad M/32 < m \leq M/16,$$

and such that the output blocks $F_1, B_1, \ldots, B_k, F_2$ have

$$\mid F_j \mid = fn, \quad \mid B_j \mid = bn$$

for some integers f and b.

For this purpose, note first that the output blocks have special sizes,

$$\mid F_j \mid = 2^s f_0 \quad \text{and} \quad \mid B_j \mid = 2^s b_0$$

with a nonnegative integer s and integers f_0, b_0 which are small in the sense that

$$2f_0 + kb_0 < 2A^2k^2 : \tag{5.2}$$

if $i = \alpha(t) < \alpha(t+1)$ then

$$f_0 = 0, \qquad b_0 = 1, \qquad 2^s = \frac{a(i,t)}{k},$$

if $i = \alpha(t) > \alpha(t+1)$ then

$$f_0 = \frac{k}{2}, \qquad b_0 = \frac{Ak}{\nu} - 1, \qquad 2^s = \frac{\nu c(i,t)}{Ak^2},$$

if $\alpha(t) < i < \omega(t)$ then

$$f_0 = A\nu k - 1, \qquad b_0 = 2A^2k - 2A\nu, \qquad 2^s = \frac{c(i,t)}{2A^2k^2},$$

if $i = \omega(t) < \omega(t+1)$ and $t \geq 2$ then

$$f_0 = A\nu k - 1, \qquad b_0 = 2A^2k\frac{Nk^{-i}}{c(i,t)} - 2A\nu, \qquad 2^s = \frac{c(i,t)}{2A^2k^2}.$$

(To see that b_0 is an integer when $i = \omega(t) < \omega(t+1)$, note that in this case $c(i,t) = c(i+1,t+1)/A\nu < AkN^{-i}/\nu$.) Next, writing $m_0 = 2f_0 + kb_0$, observe that $a = 2^s m_0$ and that (5.1), (5.2) guarantee $m_0 < M/16$; with r standing for the largest integer such that $2^r m_0 \leq M/16$, set $m = 2^r m_0$, $n = a/m$, $f = 2^r f_0$, $b = 2^r b_0$.

For future reference, note also that

$$f \geq \frac{\nu}{2Ak} \cdot \frac{A\nu k - 1}{A\nu k - \frac{\nu}{Ak}} m \qquad \text{whenever} \qquad f \neq 0. \tag{5.3}$$

The mn wires in the separator will be thought of as the mn entries of a matrix with m rows and n columns; by an $m \times n$ *scramble*, we shall mean any permutation of these mn entries that keep each entry in its row (but may move it to a different column). The *network based on a scramble* is an m-sorter network that is a series composition of networks N_1 and N_2; each N_i is a parallel composition of m-sorters N_{ij} with $j = 1, 2, \ldots, n$; the wires in each N_{1j} are the entries in the j-th column before the scramble and the wires in each N_{2j} are the entries in the entries in the j-th column after the scramble. (Each m-sorter N_{ij} places smaller keys higher up in the matrix.) The output blocks are obtained by slicing the matrix horizontally: F_1 consists of the first f rows, B_1 consists of the next b rows, and so on until F_2, which consists of the last f rows.

THEOREM 5.1 *Let m, n, b, f, k be integers such that $m \geq 100$, $n \geq 16$, $f \geq 10$, f is even and $m = 2f + kb$. Let ε_B be any positive number such that*

$$\varepsilon_B \geq \sqrt{\frac{2(1 + \ln m)}{m}};$$

let δ_F be any positive number such that

$$\delta_F \leq 1/25;$$

let ε_F be any positive number such that

$$\varepsilon_F \geq \frac{2}{f-2}\left(1 + \frac{\ln(3e^5 f)}{\ln(0.12/e\delta_F)}\right),$$

$$\varepsilon_F \geq 4e/f,$$

$1/\varepsilon_F$ *is an integer.*

Then there is a separator based on an $m \times n$ scramble with sizes of output blocks specified by $\mid F_j \mid = fn, \mid B_j \mid = bn$ and with parameters $\varepsilon_B, \delta_F, \varepsilon_F$. □

Proof of this theorem takes up the next section.

6 ANALYSIS OF THE SEPARATORS

Let m, n, f be integers such that $m \geq 100$, $n \geq 16$, $f \geq 10$, and f is even; let $\varepsilon_B, \delta_F, \varepsilon_F$ be as in Theorem 5.1. Each comparator network whose mn wires are associated with the mn entries of an $m \times n$ matrix may or may not have either of the following two properties:

Property B: For every choice of mn distinct input keys and for every integer $i = 1, 2, \ldots, m$, fewer than $\frac{1}{2}\varepsilon_B mn$ of the largest in keys are placed in outputs above the bottom i rows.

Property F: For every choice of mn distinct input keys and for every positive integer j such that $j \leq \delta_F fn$, fewer than $\varepsilon_F j$ of the largest j keys are placed in outputs above the bottom f rows.

We propose to prove the following two lemmas.

LEMMA 6.1 *The network based on a randomly chosen scramble fails to have Property B with probability less than* 1/100. □

LEMMA 6.2 *The network based on a randomly chosen scramble fails to have Property F with probability less than* 49/100. □

Together, Lemma 6.1 and Lemma 6.2 imply Theorem 5.1; in fact, they imply that the network based on a randomly chosen scramble fails to satisfy the conclusion of the theorem with probability less than 99/100.

We shall use the following result of Hoeffding [4]; for an easily accessible proof, see the Appendix.

LEMMA 6.3 *Let N be a set of size n and let S be its subset of size s; let $r_1, r_2, \ldots, r_k$ be nonnegative integers. Write*

$$p = \frac{1}{kn} \sum_{i=1}^{k} r_i$$

and let t be any positive number. If $R_1, R_2, \ldots, R_k$ are subsets of N chosen independently at random subject to the condition that $\mid R_i \mid = r_i$ for all i then

$$\sum_{i=1}^{k} \mid R_i \cap S \mid \geq (p+t)ks$$

happens with probability less than

$$\left(\left(\frac{p}{p+t} \right)^{p+t} \left(\frac{1-p}{1-p-t} \right)^{1-p-t} \right)^{ks}.$$

□

It will be useful to note that

$$\left(\frac{p}{p+t} \right)^{p+t} \left(\frac{1-p}{1-p-t} \right)^{1-p-t} < \exp(-2t^2) \tag{6.1}$$

and that

$$\left(\frac{p}{p+t}\right)^{p+t}\left(\frac{1-p}{1-p-t}\right)^{1-p-t} < \left(\frac{ep}{p+t}\right)^{p+t}. \tag{6.2}$$

In proving Lemma 6.1 and Lemma 6.2, it will be convenient to replace the mn distinct input keys by zeros and ones in such a way that the relevant number of largest keys are replaced by ones and the remaining keys are replaced by zeros. Now the *input* is a zero-one matrix; after the first round of sorting, the matrix becomes *monotone* in the sense that each of its columns consists of a block of zeros at the top and a block of ones at the bottom; then the scramble yields a *permuted* matrix and finally the second round of sorting yields the *output*.

PROOF OF LEMMA 6.1 First, fix a monotone matrix with in ones. If the output matrix has at least $\frac{1}{2}\varepsilon_B mn$ ones above its last i rows then, for some s, some set of s columns of the permuted matrix contains at least $is + \frac{1}{2}\varepsilon_B mn$ ones. For a fixed set of s columns, this happens with probability at most $\exp(-2t^2ms)$ by Lemma 6.3 with $k = m,\ \ p = i/m,\ \ t = \frac{1}{2}\varepsilon_B n/s$ and by (6.1); note that

$$\exp(-2t^2ms) \le (em)^{-n^2/s} \le (em)^{-n}.$$

Since there are 2^n choices of s and the s columns, it follows that the output matrix has at least $\frac{1}{2}\varepsilon_B mn$ ones above its last i rows with probability at most $(2/em)^n$.

Next, note that there are at most $(m+1)^n$ monotone matrices: each of them is determined by the sequence $s_1, s_2, \ldots, s_n$ of its column sums and each s_j is one of $0, 1, \ldots, m$. We conclude that Property B fails with probability at most $(2(m+1)/em)^n$. □

PROOF OF LEMMA 6.2 To begin, fix a positive integer j such that $j \le \delta_F fn$ and consider the following event,

E: some set S of columns of the permuted matrix contains at least $\frac{1}{2}f \mid S \mid +\varepsilon_F j$ ones above the bottom $\frac{1}{2}f$ rows.

We claim that

(i) for each monotone matrix with j ones, $\mathbf{E}$ occurs with probability at most

$$\frac{1+e^{-5}}{1-e^{-5}}\left(\left(\frac{efn}{2\varepsilon_F j}\right)^{2/f}\frac{2ej}{fn}\right)^{\varepsilon_F j}.$$

To justify this claim, let $p(s)$ denote the probability that some s columns of the permuted matrix contain at least $\frac{1}{2}fs+\varepsilon_F j$ ones above their last $\frac{1}{2}f$ rows. By Lemma 6.3 with $k=m-\frac{1}{2}f$, $p\le j/mn$, $(p+t)ks=\frac{1}{2}fs+\varepsilon_F j$, and by (6.2), we have

$$p(s)\le\binom{n}{s}\left(\frac{ejs}{(\frac{1}{2}fs+\varepsilon_F j)n}\right)^{\frac{1}{2}fs+\varepsilon_F j};$$

since $(c/x)^x$ is a decreasing function of x in the range $x>c/e$, it follows that

$$p(s)\le\binom{n}{s}\left(\frac{es}{\varepsilon_F n}\right)^{\varepsilon_F j}\quad\text{and}\quad p(s)\le\binom{n}{s}\left(\frac{2ej}{fn}\right)^{fs/2}.$$

Hence $p(s)\le g(s)$ with

$$g(x)=\begin{cases}\left(\frac{en}{x}\right)^x\left(\frac{ex}{\varepsilon_F n}\right)^{\varepsilon_F j} & \text{if } x\le\varepsilon_F\cdot 2j/f\\ \left(\frac{en}{x}\right)^x\left(\frac{2ej}{fn}\right)^{fx/2} & \text{if } x\ge\varepsilon_F\cdot 2j/f\end{cases}$$

and proving (i) reduces to proving that

$$\sum_{s=1}^{n}g(s)\le\frac{1+e^{-5}}{1-e^{-5}}g(\varepsilon_F\cdot 2j/f).$$

If $x\le\varepsilon_F\cdot 2j/f$ then

$$\frac{d}{dx}\ln g(x)=\ln\frac{n}{x}+\frac{\varepsilon_F j}{x}\ge\frac{1}{2}f\ge 5;$$

if $x\ge\varepsilon_F\cdot 2j/f$ then

$$\begin{aligned}\frac{d}{dx}\ln g(x) &= \ln\frac{n}{x}+\frac{1}{2}f\ln\frac{2ej}{fn}\\ &\le \ln\frac{e}{\varepsilon_F}+(\frac{1}{2}f-1)\ln\frac{2ej}{fn}\\ &\le \ln\frac{f}{4}+(\frac{1}{2}f-1)\ln\frac{2e}{25}\\ &< -5;\end{aligned}$$

writing $\delta = e^{-5}$, $b = \varepsilon_F \cdot 2j/f$, $a = \lfloor b \rfloor$, $c = a+1$ we conclude that

$$\begin{aligned}\sum_{s=1}^{n} g(s) &= \sum_{s=1}^{a} g(s) + \sum_{s=c}^{n} g(s) \\ &< \frac{1}{1-\delta}(g(a)+g(c)) \\ &\leq \frac{\delta^{b-a}+\delta^{c-b}}{1-\delta} g(b) \\ &\leq \frac{1+\delta}{1-\delta} g(b).\end{aligned}$$

Next, let the *top* of an $m \times n$ matrix mean the matrix without its bottom $\frac{1}{2}f$ rows. We claim that

(ii) for each positive integer j, all the monotone matrices with j ones have at most

$$\frac{90}{89}\left(\frac{e^2(f+2)^2 n}{4j}\right)^{2j/(f+2)}$$

distinct tops.

To justify this claim, observe that the top is determined by the position of its nonzero columns and by the sequence $s_1, s_2, \ldots, s_k$ of the column sums in these k columns. Since s_1, s_1+s_2, $s_1+s_2+s_3$, $\ldots$, $s_1+s_2+s_3+\ldots+s_k$ are distinct positive integers and since

$$\sum_{i=1}^{k}(s_i + \frac{1}{2}f) \leq j,$$

it follows that the number of distinct tops is at most

$$\sum_{k=0}^{n} \binom{n}{k}\binom{j-fk/2}{k}.$$

If $k \geq 1$ then

$$\binom{n}{k}\binom{j-fk/2}{k} \leq \binom{n}{k}\binom{j}{k} < \left(\frac{e^2 nj}{k^2}\right)^k;$$

hence proving (ii) reduces to verifying that

$$1 + \sum \left(\frac{e^2 nj}{k^2}\right)^k < \quad \frac{90}{89}\left(\frac{e^2(f+2)^2 n}{4j}\right)^{2j/(f+2)} \tag{6.3}$$

with the summation running through all the positive integers k such that $j - fk/2 \geq k$. Note that $e^2nj \geq e^2n > 90$; in addition, if $x \leq 2j/(f+2)$ then

$$\frac{d}{dx}\ln\left(\left(\frac{e^2nj}{x^2}\right)^x\right) = \ln\frac{nj}{x^2} \geq \ln\frac{n(f+2)^2}{4j} \geq \ln\frac{25(f+2)^2}{4f} \geq \ln 90;$$

hence the left-hand side summands in (6.3) increase at least as fast as a geometric progression with quotient 90 and (6.3) follows.

Now observe that the occurrence of event **E** depends only on the top of the monotone matrix just before the scramble and on the scramble itself: the bottom $\frac{1}{2}f$ rows are irrelevant. Hence (i) and (ii) imply that the probability of Property F failing on at least one input with precisely j ones is at most

$$\frac{90}{89}\left(\frac{e^2(f+2)^2n}{4j}\right)^{2j/(f+2)} \cdot \frac{1+e^{-5}}{1-e^{-5}}\left(\left(\frac{efn}{2\varepsilon_F j}\right)^{2/f} \cdot \frac{2ej}{fn}\right)^{\varepsilon_F j},$$

which is at most $1.025x^{\varepsilon_F j}$ with

$$x = \left(\frac{e^2(f+2)^2n}{4j}\right)^{2/\varepsilon_F f} \cdot \left(\frac{efn}{2\varepsilon_F j}\right)^{2/f} \cdot \frac{2ej}{fn};$$

we propose to show that $x < 0.32$ for all j. For this purpose, note first that

$$(e^2/\varepsilon_F)^{2/f} = ((e^2/\varepsilon_F)^{\varepsilon_F})^{2/\varepsilon_F f} \leq (e^2)^{2/\varepsilon_F f},$$

and so

$$x \leq \left(\frac{e^4(f+2)^2n}{4j}\right)^{2/\varepsilon_F f}\left(\frac{2ej}{fn}\right)^{(f-2)/f}.$$

Writing $t = \varepsilon_F(f-2)/2$, observe that

$$\begin{aligned} x^{f/(f-2)} &\leq 0.24\left(\frac{e^5(f+2)^2}{0.48f}\left(\frac{ej}{0.12fn}\right)^{t-1}\right)^{1/t} \\ &\leq 0.24\left(3e^5 f\left(\frac{e\delta_F}{0.12}\right)^{t-1}\right)^{1/t}. \end{aligned}$$

Since

$$t - 1 \geq \frac{\ln(3e^5 f)}{\ln(0.12/e\delta_F)},$$

we have $x^{f/(f-2)} \leq 0.24$, and so $x < 0.32$.

Finally, if Property F fails at all then (since ε_F is the reciprocal of an integer) it fails for some j such that $\varepsilon_F j$ is a positive integer. We conclude that Property F fails with probability at most

$$1.025 \sum_{i \geq 1} 0.32^i,$$

which is less than 0.49. □

7 PUTTING THE PIECES TOGETHER

Throughout this section, we shall keep

$$A = k^2 \quad \text{and} \quad \nu = 1/k;$$

now

$$t_f = 3d - 20 \quad \text{and} \quad \alpha(t_f) = \omega(t_f) = d - 6$$

with $d = \log N / \log k$. In addition, we shall set

$$\mu = k^{-5}, \quad \delta = \frac{1}{4}k^{-5}, \quad \delta_F = \frac{2k}{k^2 - 1};$$

now (4.2) reduces to

$$\varepsilon_B \le \frac{1}{4}k^{-4} \cdot \frac{16k^6 - 32k^4 - 2k^2 + k + 2}{16k^6 - k^2}, \tag{7.1}$$

(4.3) and (4.4) are satisfied, and (4.5) reduces to

$$\varepsilon_F \le \frac{1}{4}k^{-4} \cdot \frac{4k - 1}{4k}. \tag{7.2}$$

PROOF OF THEOREM 1.1 For each integer N such that $N \ge 2^{84}$ and N is a power of 64, we shall describe a sorting network on N wires of depth at most $1830 \lg N - 69637$; it will follow that for each integer N such that $N \ge 2^{78}$ there is a sorting network on N wires of depth at most $1830(6 + \lg N) - 69637$.

The network is as in Section 3 with $k = 64$ (and with $A = 4096$, $\nu = 1/64$). The separator used in the root at time $t = 0$ is based on an $m \times n$ scramble with $m = 2^{79}$; Theorem 5.1 allows us to assume that this separator has $\varepsilon_B = \varepsilon^*$ with

$$\varepsilon^* = 2^{-39}\sqrt{1 + 79 \ln 2} < 2^{-36}.$$

Each remaining separator is either an m-sorter (if it has at most 2^{64} wires) or based on an $m \times n$ scramble with $2^{59} < m \le 2^{60}$ (if it has more than 2^{64} wires); in the latter case, (5.3) guarantees that the separator has either $f = 0$ or

$$f > 2^{34} \cdot \frac{1 - 2^{-12}}{1 - 2^{-36}} > 1.7 \times 10^{10};$$

hence Theorem 5.1 allows us to assume that its parameters $\varepsilon_B, \delta_F, \varepsilon_F$ are specified by

$$\varepsilon_B = 2^{-29}\sqrt{1 + 59\ln 2} < 1.25 \times 10^{-8},$$

$$\delta_F = 128/4095,$$

$$\varepsilon_F = 1/(8 \times 10^7) = 1.25 \times 10^{-8}.$$

Now (4.1), (7.1), and (7.2) are satisfied; hence Lemma 4.5 (with $r = 1$) guarantees that the network can be completed by a parallel composition of 2^{42}-sorters.

The various m-sorters featured in this description can be implemented as the sorting networks constructed by Batcher [3]; these have depth $p(p+1)/2$ when $m = 2^p$ for a positive integer p. Then the network has depth at most $6320 + (t_f - 1)3660 + 903$, which comes to $1830 \lg N - 69637$. □

The argument we have just used to prove Theorem 1.1 can be also used (with $k = 64$ replaced by $k \approx M^{1/8}$) to prove Theorem 1.2; the only problem comes from the high standard set for the quality of the exceptional separator used in the root at time $t = 0$. This problem is only technical; one of the several ways of getting around it consists of running through the same argument twice. The first round (with $k \approx M^{1/12}$) yields a weaker version of Theorem 1.2 (with 48 replaced by 72); this intermediate result is used in the second round to provide the exceptional separator of constant depth.

LEMMA 7.1 *For each choice of positive integers M and N such that $N \geq M$ there is a sorting network on N wires, made from M-sorters, whose depth is at most*

$$(72 + o(1)) \log_M N - 33 \qquad \text{as } M \to \infty.$$

PROOF. Let k be the largest power of two such that

$$\sqrt{\frac{2(1 + \ln m)}{m}} \leq k^{-6} \qquad \text{whenever } M/32 < m \leq M/16;$$

note that

$$\log k = (\frac{1}{12} + o(1)) \log M \qquad \text{as } M \to \infty.$$

For each integer N such that $N \geq M$ and N is a power of k, we shall describe a sorting network on N wires, made from M-sorters, of depth at most $(72 + o(1)) \log_M N - 39$ as $M \to \infty$; it will follow that for each integer N such that $N \geq M$, there is a sorting network on N wires, made from M-sorters, of depth at most $(72 + o(1))(\frac{1}{12} + \log_M N) - 39$.

The network is as in Section 3 (with $A = k^2, \nu = 1/k$). Each separator is either an M-sorter (if it has at most M wires) or based on an $m \times n$ scramble with $M/32 < m \leq M/16$ (if it has more than M wires); in the latter case, (5.3) guarantees that the separator has either $f = 0$ or

$$f \geq (1 + o(1)) \frac{m}{2k^4} \geq (1 + o(1)) k^8 \ln k \qquad \text{as } M \to \infty;$$

hence Theorem 5.1 allows us to assume that its parameters $\varepsilon_B, \delta_F, \varepsilon_F$ are specified by

$$\varepsilon_B = k^{-6}, \quad \delta_F = \frac{2k}{k^2 - 1}, \quad \varepsilon_F = k^{-8}.$$

Now (4.1) with $\varepsilon^* = \varepsilon_B, \mu = k^{-5}$ and (7.1), (7.2) are satisfied for all sufficiently large k; hence Lemma 4.5 (with $r = 1$) guarantees that the network can be completed by a parallel composition of k^7-sorters. The network has depth at most $2t_f + 1$, which comes to $(72 + o(1)) \log_M N - 39$ as $M \to \infty$.

PROOF OF THEOREM 1.2 Let k be the largest power of two such that

$$\sqrt{\frac{2(1 + \ln m)}{m}} \leq \frac{1}{5} k^{-4} \qquad \text{whenever } M/32 < m \leq M/16;$$

note that

$$\log k = (\frac{1}{8} + o(1)) \log M \qquad \text{as } M \to \infty.$$

For each integer N such that $N \geq M$ and N is a power of k, we shall describe a sorting network on N wires, made from M-sorters, of depth at most $(48 + o(1)) \log_M N + 109$ as

$M \to \infty$; it will follow that for each integer N such that $N \geq M$, there is a sorting network on N wires, made from M-sorters, of depth at most $(48+o(1))(\frac{1}{8}+\log_M N)+109$ as $M \to \infty$.

The network is as in Section 3 (with $A = k^2, \nu = 1/k$). The separator used in the root at time $t = 0$ is either a sorting network (if it has at most $16M^{3/2}$ wires) or based on an $\lfloor M^{3/2} \rfloor \times n$ scramble (if it has more than $16M^{3/2}$ wires) with each of the $\lfloor M^{3/2} \rfloor$-sorters implemented as a sorting network; since

$$\sqrt{\frac{2(1+\ln\lfloor M^{3/2} \rfloor)}{\lfloor M^{3/2} \rfloor}} \leq k^{-6},$$

Theorem 5.1 allows us to assume that this separator has $\varepsilon_B = k^{-6}$; Lemma 7.1 keeps its depth down to at most 150 for all sufficiently large M. Each remaining separator is either an M-sorter (if it has at most M wires) or based on an $m \times n$ scramble with $M/32 < m \leq M/16$ (if it has more than M wires); in the latter case, (5.3) guarantees that the separator has either $f = 0$ or

$$f \geq (1+o(1))\frac{m}{2k^4} \geq (1+o(1))k^4 \ln k \qquad \text{as } M \to \infty;$$

hence Theorem 5.1 allows us to assume that its parameters $\varepsilon_B, \delta_F, \varepsilon_F$ are specified by

$$\varepsilon_B = \frac{1}{5}k^{-4}, \quad \delta_F = \frac{2k}{k^2-1}, \quad \varepsilon_F = \frac{1}{5}k^{-4}.$$

Now (4.1) with $\varepsilon^* = k^{-6}, \mu = k^{-5}$ and (7.1), (7.2) are satisfied for all sufficiently large k; hence Lemma 4.5 (with $r = 1$) guarantees that the network can be completed by a parallel composition of k^7-sorters. The network has depth at most $150 + 2(t_f - 1) + 1$, which comes to $(48 + o(1)) \log_M N + 109$ as $M \to \infty$. □

8 IMPROVEMENTS AND LIMITATIONS

It is not difficult to adjust the parameters in our proof of Theorem 1.2 so as to bring the constant 48 down to $24 + 16\sqrt{2}$ (≈ 46.627): let k be the largest power of two such that

$$\sqrt{\frac{2(1+\ln m)}{m}} \le \frac{1}{5}k^{-2(1+\sqrt{2})} \quad \text{whenever } M/32 < m \le M/16,$$

let A be the largest power of two such that $A < k^{1+\sqrt{2}}$, and let ν be the smallest power of two such that $A\nu \ge k$. The analysis goes through with

$$\varepsilon_B = \frac{1}{5}k^{-2(1+\sqrt{2})}, \quad \delta_F = \frac{2A\nu}{A\nu k - 1}, \quad \varepsilon_F = \frac{1}{5}A^{-2}, \quad \mu = \frac{\nu}{Ak^2}, \quad \delta = \frac{1}{4}\mu.$$

However, we are about to point out that no variation on the theme presented in this report can yield a version of Theorem 1.2 with the constant 48 reduced to 23.313 unless the variation differs from the theme in a significant way. More precisely, let us take it for granted that separators based on $m \times n$ scrambles have $\varepsilon_B = \Omega(m^{-1/2})$ and that the parameter μ introduced in Section 4 satisfies

$$\frac{\varepsilon_B}{A\nu} \le \mu \le \frac{\nu}{2Ak}$$

(which is a weakening of constraints (4.2) and (4.4)); all the remaining constraints stipulated in Sections 4 and 5 will be considered irrelevant. Similarly, we shall not insist on any particular choice of α and ω as long as the movement of the wires through the tree ceases at time t such that $NA^d\nu^t$ (with $N = k^d$) is a constant independent of N. Writing

$$k = 2^x, \quad A = 2^y, \quad \nu = 2^{-z}, \quad \varepsilon_B = 2^{-w},$$

note that the network has depth $2d(x+y)/z$ plus a constant independent of N and that our assumption $\varepsilon_B = \Omega(m^{-1/2})$ implies $\lg M \ge 2w + o(1)$. Hence the constant c that replaces the 48 in Theorem 1.2 must satisfy

$$c \ge \frac{4w(x+y)}{xz};$$

our assumption $\varepsilon_B \le \nu^2/2k$ and the tacit $A\nu > 1$ imply

$$\frac{w(x+y)}{xz} > \frac{w(x+z)}{xz} > \frac{(x+2z)(x+z)}{xz} \ge 3 + 2\sqrt{2}.$$

9 AFTERWORD

Without realizing what I was getting into, I volunteered to lecture on the new Ajtai-Komlós-Szemerédi sorting network in the course 198:514 (Design and analysis of data structures and algorithms II) that I gave at Rutgers in the spring of 1991. In preparing for these lectures, I had the benefit of several conversations with Komlós and Szemerédi; in addition, Komlós gave me a preprint of Paterson's paper [7] and rudimentary notes concerning mainly the separators based on scrambles. By the end of the term, I prepared lecture notes that I handed out to the students and gave to Komlós and Szemerédi; except for misprints removed and rough spots smoothed out, these lecture notes constitute Sections 1-7 of the present report. Section 8 was added a year later in my attempt to explain the discrepancy between the constants that I have actually worked out and their more impressive counterparts that Komlós claimed (around 60 to 100 in place of the 1830 in Theorem 1.1; less than 10 in place of the 48 in Theorem 1.2): I don't know how closely the network I constructed in Section 3 corresponds to what Ajtai, Komlós, and Szemerédi had in mind.

In the classroom, I initially presented a weaker version of Theorem 1.1, with 1891 in place of the 1830; Jaikumar Radhakrishnan pointed out to me that replacing my $2^{60} < m \leq 2^{61}$ by $2^{59} < m \leq 2^{60}$ yields the better constant.

References

[1] M. Ajtai, J. Komlós, and E. Szemerédi, Sorting in $c \log n$ parallel steps, *Combinatorica* 3 (1983), 1-19.

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

[3] B.E. Batcher, Sorting networks and their applications, *Proc. 32nd Ann. AFIPS Spring Joint Comp. Conf.* 32 (1968), pp.307-314.

[4] W. Hoeffding, Probability inequalities for sums of bounded random variables, *Am. Statist. Assoc. J.* 58 (1963), 13-30.

[5] D. E. Knuth, *The Art of Computer Programming. Vol. 3. Sorting and Searching*, Addison-Wesley, Reading, MA (1973).

[6] F. T. Leighton, Tight bounds on the complexity of parallel sorting, *IEEE Transactions on Computers* C-34 (1985), 344-354.

[7] M. S. Paterson, Improved sorting networks with $O(\log n)$ depth, *Algorithmica* 5 (1990), 75-92.

[8] N. Pippenger, Communication networks, in: *Handbook Of Theoretical Computer Science, Vol. A, Algorithms and Complexity* (J. van Leeuwen, ed.) The MIT Press/ Elsevier (1990), Chapter 15, pp. 805-833.

APPENDIX: A PROOF OF LEMMA 6.3

Let p^* denote the probability bounded by the lemma; let A denote the set of all integer vectors $a = [a_1, a_2, \ldots, a_k]$ such that $0 \le a_i \le r_i$ for all i; let B denote the set of all vectors in A such that $\sum a_i \ge (p+t)ks$. Trivially,

$$p^* = \sum_{a \in B} \prod_{i=1}^{k} \frac{\binom{s}{a_i}\binom{n-s}{r_i - a_i}}{\binom{n}{r_i}}.$$

We propose to show that, for all x such that $x \ge 1$,

$$\begin{aligned}
p^* &\le x^{-(p+t)ks} \sum_{a \in B} \prod_{i=1}^{k} \frac{\binom{s}{a_i}\binom{n-s}{r_i - a_i}}{\binom{n}{r_i}} x^{a_i} \\
&\le x^{-(p+t)ks} \sum_{a \in A} \prod_{i=1}^{k} \frac{\binom{s}{a_i}\binom{n-s}{r_i - a_i}}{\binom{n}{r_i}} x^{a_i} \\
&= x^{-(p+t)ks} \prod_{i=1}^{k} \sum_{a_i=0}^{r_i} \frac{\binom{s}{a_i}\binom{n-s}{r_i - a_i}}{\binom{n}{r_i}} x^{a_i} \\
&\le x^{-(p+t)ks} \prod_{i=1}^{k} \left(\frac{r_i}{n}(x-1)+1\right)^s \\
&\le \left(x^{-(p+t)}(p(x-1)+1)\right)^{ks};
\end{aligned}$$

then the lemma will follow by setting

$$x = \frac{1-p}{p} \cdot \frac{p+t}{1-p-t}.$$

Only the last two inequalities in this chain may require explanations: we need to verify that

$$\sum_{a=0}^{r} \frac{\binom{s}{a}\binom{n-s}{r-a}}{\binom{n}{r}} x^a \le \left(\frac{r}{n}(x-1)+1\right)^s$$

and that

$$\prod_{i=1}^{k} (\frac{r_i}{n}(x-1)+1) \le (p(x-1)+1)^k.$$

To see the first point, observe that

$$\sum_{a=0}^{r} \frac{\binom{s}{a}\binom{n-s}{r-a}}{\binom{n}{r}} x^a$$
$$= \sum_{a=0}^{r} \frac{\binom{s}{a}\binom{n-s}{r-a}}{\binom{n}{r}} \sum_{j=0}^{a} \binom{a}{j} (x-1)^j$$
$$= \sum_{j=0}^{r} \sum_{a=j}^{r} \frac{\binom{s}{a}\binom{n-s}{r-a}\binom{a}{j}}{\binom{n}{r}} (x-1)^j$$

and that

$$\sum_{a=j}^{r} \frac{\binom{s}{a}\binom{n-s}{r-a}\binom{a}{j}}{\binom{n}{r}}$$
$$= \sum_{a=j}^{r} \frac{\binom{s}{j}\binom{s-j}{a-j}\binom{n-s}{r-a}}{\binom{n}{r}}$$
$$= \frac{\binom{s}{j}\binom{n-j}{r-j}}{\binom{n}{r}} = \frac{\binom{s}{j}\binom{r}{j}}{\binom{n}{j}} \leq \binom{s}{j}\left(\frac{r}{n}\right)^j.$$

To see the second point, recall that

$$f(\sum_{i=1}^{k} p_i y_i) \leq \sum_{i=1}^{k} p_i f(y_i)$$

whenever f is a convex function and $p_1, p_2, \ldots, p_k$ are positive numbers that sum to 1 (this fact is known as Jensen's inequality); then set $f(y) = -\log(y+1)$ and $y_i = r_i(x-1)/n$, $p_i = 1/k$ for all i.