PRAM Lower Bound for Element Distinctness Revisited

Petr Kolman

Department of Applied Mathematics, Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic
kolman@kam.ms.mff.cuni.cz

Abstract. This paper considers the problem of element distinctness on CRCW PRAMs with unbounded memory. A complete proof of the optimal lower bound of $\Omega\left(n \log n / \left(p \log(\frac{n}{p} \log n + 1)\right)\right)$ steps for n elements problem on p processor COMMON PRAM is presented. This lower bound has been previously correctly stated by Boppana, but his proof was not complete. Its correction requires some additional observations and some not straightforward changes.

1 Introduction

This paper considers the PRAM model with unbounded memory. A *PRAM* consists of p processors $P_1, \cdots, P_p$ and shared memory with cells indexed by integers N. Initially the contents of all shared memory cells are 0 and processor P_i, $1 \leq i \leq n$, has the input value x_i in it's local memory. One step of computation consists of three phases: local computation, global read, global write. On the PRIORITY model the minimal index processor (among those attempting to write to the same cell) succeeds in writing to a memory cell if a write conflict appears. On the COMMON model all processors writing to the same cell have to write the same value. Assume also that the result of the computation is known to processor P_1.

The problem of *Element Distinctness* is defined as follows: Given n integers $x_1, \cdots, x_n$ determine whether they are pairwise distinct. This problem has been studied for some time as a tool for separating different variants of PRAM. On n processor PRIORITY PRAM it is solvable in $O(1)$ steps [11]. For COMMON PRAM several lower bounds were proved implying the separation. Fich, Meyer auf der Heide, and Wigderson [7] showed a lower bound of $\Omega(\log \log \log n)$, Ragde, Steiger, Szemeredi, and Wigderson [11] improved it to $\Omega(\sqrt{\log n})$. Finally Boppana [1] presented a proof of the optimal lower bound $\Omega(\frac{\log n}{\log \log n})$ (resp. $\Omega\left(\frac{n \log n}{p \log(\frac{n}{p} \log n+1)}\right)$ for the case with n elements and p processors). Unfortunately there is an error in the proof of his theorem and in fact the assertion is not proved (see Appendix A). All these results require an infinite input domain size. Later on Edmonds [3, 4] proved (using a new technique) the same lower bound even for the case of much smaller input domain size (his proof requires only $2^{2^{\Omega(n)}}$). The proof is very complicated and the published version [3] gives mainly an overview of the proof, the key ideas, not the details.

The present paper gives the complete proof of the lower bound for infinite input domain size. The basic idea is the same as in the proof of Boppana – to measure the number of pairs of variables that were learned to be different by entropies of associated random variables. The difference is that the unjustly omited pairs in the previous proof are considered now. The other difference is that now the lower bound is proved directly for the COMMON PRAM.

1.1 Definitions

A pair (x, y) of vectors of variables is said to *cover* a pair (x_i, x_j) of variables, if x and y agree on all coordinates but one, and on that coordinate x is equal to x_i and y to x_j (e.g. $((x_1, x_2), (x_1, x_3))$ covers (x_2, x_3)).

Let l be a mapping of a set of n variables $V = \{x_1, \cdots, x_n\}$ into some totally ordered set. We say that a vector $a = (a_1, \cdots, a_n) \in N^n$ is *consistent with* l if for every $1 \leq i, j \leq n$, $l(x_i) < l(x_j) \Rightarrow a_i < a_j$. Let $(S^n)_l$ denotes the set $(S^n)_l = \{a \in S^n \mid a \text{ is consistent with } l\}$. Because l corresponds to some partial order on V we will sometimes speak about l as about an partial order. For l and subsets $A, B \subseteq V$ define the *comparison graph* $C_l(A, B) = (V, E)$, where $E = \{(x_i, x_j) \mid x_i \in A,\ x_j \in B,\ i \neq j,\ l(x_i) = l(x_j)\}$. The number of edges in $C_l(A, B)$ will be denoted by $|C_l(A, B)|$.

A D*-function* is a function f whose domain is of the form D^V for $D \subseteq N$ and for some finite set V. A function $f|_I$, where $f|_I$ denotes the restriction of f to $I \subseteq D^V$, is said to *depend on the variable* x_i if there are $a = (a_1, \cdots, a_i, \cdots, a_n) \in I$ and $\hat{a} = (a_1, \cdots, \hat{a}_i, \cdots, a_n) \in I$ such that $f(a) \neq f(\hat{a})$ (a and $\hat{a}$ agree on all coordinates but the i^{th}).

Let f, g be S-functions and let $I \subseteq (S^n)_l$ be such a set that the set of variables which $f|_I$ (resp. $g|_I$) depends on is lineary ordered in l. Suppose $f|_I$ and $g|_I$ are indentical when seen as functions just of those variables they depend on and when these variables are ordered according to l. Then we say that $f|_I$ and $g|_I$ are *weakly indentical* (e.g. if $l(x_1) = 1,\ l(x_2) = 2,\ l(x_3) = 2,\ f(x_1, x_2, x_3) = x_1 + x_2^3$, $g(x_1, x_2, x_3) = x_1 + x_3^3$ and $I \subseteq (S^3)_l$, then we would say that $f|_I$ and $g|_I$ are weakly indentical).

Given a random variable X with range $\{c_1, \cdots, c_m\}$, its *entropy* is $H(X) = \sum_{j=1}^{m} -Pr[X = c_j] \log_2 Pr[X = c_j]$. The *entropy of a function* f with a finite domain is $H(f) = H(f(v))$, where v is a random variable with uniform distribution on the domain of f. Given two random variables X and Y, the notation $H(X, Y)$ will be used for the entropy of a random variable (X, Y). The most useful property of entropy for us is subaddivity: $H(X, Y) \leq H(X) + H(Y)$.

Finally let L denotes the function $L(z) = (z + 1) \log_2(z + 1) - z \log_2 z$.

2 Proof

In this section a proof of the lower bound will be given. It is based on those of Boppana [1] and Ragde, Steiger, Szemeredi, Wigderson [11]. The proof makes crucial use of Ramsey theory. The following theorem states the results we shall need.

Theorem 1. *Let F be a finite set of S-functions of n variables $\{x_1, x_2, \cdots, x_n\}$, for infinite $S \subseteq N$, let l be a mapping of $\{x_1, x_2, \cdots, x_n\}$ into some totally ordered set and let $I \subseteq (S^n)_l$ be such a set that for every $f \in F$ the set of variables which $f|_I$ depends on is lineary ordered in l. Then there exists an infinite $\bar{S} \subseteq S$ such that for $I' = I \cap \bar{S}^n$*

$$\forall f \in F \ : \ f|_{I'} \text{ is one-to-one on variables it depends on,}$$
$$\forall f, g \in F \ : \ f|_{I'} \text{ and } g|_{I'} \text{ either have disjoint ranges or are weakly identical.}$$

Proof. The theorem follows from Lemma 1 [10], which is based on Erdös-Rado Theorem [5].

Theorem 2. *Every COMMON PRAM with p processors that solves the problem of element distinctness of size $n, n \leq p$, requires $\Omega\left(\frac{n \log n}{p \log(\frac{n}{p} \log n + 1)}\right)$ steps.*

Proof. The given algorithm defines for each processor P_i and for each time step t two *addressing functions* R^i_t, $W^i_t \ : \ N^n \to N$, where $R^i_t(x)$ specifies the number of a cell of the global memory, that the processor P_i at time step t for input x is reading from. Similarly with W^i_t for writing. By doubling the amount of steps of the algorithm we may assume that $R^i_t = W^i_t$ for each i and t.

Suppose, by contradiction, there is a COMMON PRAM, that solves the problem in less than $\Omega\left(\frac{n \log n}{p \log(\frac{n}{p} \log n + 1)}\right)$ steps, say in T steps. We will show there are two different inputs, one element distinct and the other not, that are indistinguishable to the given PRAM at the beginning of step T. To reach the desired goal, a sequence of input sets $I_t \subseteq N^n$ will be inductively constructed, such that for every t, $1 \leq t \leq T$, there are two inputs in I_t, one element distinct and the other not, that are indistinguishable to the PRAM at the beginning of step t. The set I_t is described by a set S_t, $S_t \subseteq N$, by a mapping l_t of the set $V = \{x_1, \cdots, x_n\}$ of input variables into some totally ordered set and by a graph DG_t on the set V, in the following way:

$$\begin{aligned} I_t = \{ \ a \mid a \in (S^n_t)_{l_t} \ \& \ a_i = a_j \Rightarrow \ (x_i, x_j) \notin DG_t \ \& \\ \text{there is at most one pair } a_i = a_j, i \neq j\}. \end{aligned}$$

Sets V^i_t, $1 \leq t \leq T$, $1 \leq i \leq p$, will help us to define the objects. The meaning of the objects is roughly as follows. If for each $x \in I_{t-1}$ the PRAM is able to recognize during the first $t-1$ steps the relative order of x_i and x_j, then $l_t(x_i) \neq l_t(x_j)$. If it is only able to recognize wheather $x_i = x_j$ or $x_i \neq x_j$, then $(x_i, x_j) \in DG_t$. If the values for all $x_j \in V^i_t$ are fixed then no matter how the other values are changed, the state of P_i at the beginning of step t will be the same, provided $x \in I_t$ (we say that only variables in V^i_t may *affect* the state of processor P_i at the beginning of step t). The restriction of inputs to a subset of $(S^n_t)_{l_t}$ ensures that the interactions among processors via the shared memory appear only in a very regular way. This enables us to bound the amount of information about the input values the algorithm is able to learn in a single step.

All the mentioned objects will be constructed inductively and will satisfy the following properties for $m = 8\log p$:

1. $S_t \subseteq S_{t-1}$ for $t \geq 1$,
2. $l_{t-1}(x_i) < l_{t-1}(x_j) \;\Rightarrow\; l_t(x_i) < l_t(x_j)$ for $t \geq 1$, and for $t \geq 0$ hold:
   (a) $H(l_t) \leq \big(L(\frac{pm}{n}) + 3\big)\, t$,
   (b) $|C_{l_t}(V_t^i, V_t^j)| \leq m$ for $1 \leq i < j \leq p$,
3. $DG_t \supseteq DG_{t-1}$ for $t \geq 1$,
4. l_t is a linear order on V_t^i (i.e. l_t is one-to-one on V_t^i) for $t \geq 0$, $\forall\, i, 1 \leq i \leq p$,
5. V_t^i contains all the variables that may affect the state of processor P_i at the beginning of step t, for all inputs in I_t.

This will make sure, besides others, that $I_t \subseteq I_{t-1}$.

According to the definition of PRAM we put $V_0^i = \{x_i\}$ for $1 \leq i \leq n$, $V_0^i = \emptyset$ for $n < i \leq p$. Let $S_0 = N$, l_0 be a constant mapping and DG_0 be an empty graph (i.e. with no edges). All desired properties are satisfied for $t = 0$.

Now the inductive step can be described. Let

$$F = \{W_{t'}^i \mid 1 \leq i \leq p, 1 \leq t' \leq t\}.$$

By applying the Theorem 1 to the set F of functions, mapping l_t and sets I_t and S_t (we have $I_t \subseteq (S_t)_{l_t}^n$) we obtain $\bar{S} \subseteq S_t$. We put $S_{t+1} = \bar{S}$ and $I_t' = I_t \cap S_{t+1}^n$. Then the set F can be divided into several disjoint subsets $F_1, \cdots, F_{m_t}$ such that

$$\forall f, g \in F_i : f|_{I_t'} \text{ is weakly identical with } g|_{I_t'},$$
$$\forall f \in F_i,\ \forall g \in F_j, i \neq j : f|_{I_t'} \text{ and } g|_{I_t'} \text{ have disjoint ranges .}$$

Let's choose the indices of F_i in such a way that F_i from the previous step is a subset of F_i from the current step, for $1 \leq i \leq m_{t-1}$. Consider processors P_j and P_k. If there is no pair of addressing functions f of P_j and g of P_k (used up to step t) such that $f, g \in F_i$ for some i, then processors P_j and P_k cannot exchange directly (i.e. without help of any other processor) any information up to step t, for inputs in I_t'.

Now we are ready to construct the objects l_{t+1}, DG_{t+1} and V_{t+1}^i. We have to ensure that properties 2, 3, 4 and 5 will hold for $t+1$. For $f \in F$ let $\mathbf{k}_f$ denote the vector of variables that $f|_{I_t'}$ depends on, ordered according to l_t. Consider one by one each F_i, $1 \leq i \leq m_t$. Let's define

$$C_t^i = \{\mathbf{k}_f \mid f \in F_i \;\&\; f = W_t^j \text{ for some } j\}.$$

At this point, in the construction of DG_{t+1} and V_{t+1}^i, the fact that a COMMON PRAM is considered will be used. An edge (x_k, x_l) is added to DG_{t+1} if there exists $\mathbf{a} \in C_{t'}^i$ for some $t' < t$ and $\mathbf{b} \in C_t^i$, such that $(\mathbf{a}, \mathbf{b})$ covers (x_k, x_l) and $\mathbf{b} \notin A_{t''}$ $\forall t'', t' \leq t'' < t$. This will make sure that the communication among processors via the shared memory in step t will be the same for all inputs in I_{t+1}. Let $R = \{P_j \mid W_t^j \in F_i\}$. For each $P_j \in R$ let t' be the last time $\tau < t$ such that there exists processor P_k with $W_\tau^k \in F_i$ and $\mathbf{k}_{W_\tau^k} = \mathbf{k}_{W_t^j}$, and let W_j be a set of all such P_k (i.e. $W_j = \{P_k \mid W_{t'}^k \in F_i \;\&\; \mathbf{k}_{W_{t'}^k} = \mathbf{k}_{W_t^j}\}$), let $W_j = \emptyset$ if no such τ

exists. W_j is the set of all processors that wrote at the last time to the memory cell that P_j is reading from in step t, for inputs in I_{t+1}. The important thing for us is that W_j is the same for all inputs in I_{t+1}. Thus the contents of the memory cell P_j is reading from in step t is determined by the same set of processors, for all inputs in I'_t. Therefore if we put $U^j_{t+1} = \bigcap_{P_i \in W_j} V^i_{t'}$ then $V^j_{t+1} = V^j_t \cup U^j_{t+1}$ has the desired property 5. After doing this for each $P_j \in R$ proceed to next F_i.

By invariant 2(b) in step t the graph $G = \bigcup_{i=1}^{p} C_{l_t}(V^i_t, U^i_{t+1})$ has at most pm edges. Thus by Lemma 3.4 [1] there is a coloring χ of graph G with entropy at most $L(\frac{pm}{n})$. Order the colors of χ arbitrarily and define $l' = (l_t, \chi)$, ordering its range in lexicographic order. Notice that for any l_{t+1} that is a refinement of l' the invariant 4 follows.

Next we shall show there is a function $f : V \to \{1, ..., 8\}$ such that for $l_{t+1} = (l', f)$ with lexicographicaly ordered range the properties 2(a)(b) hold. Choose a random function $f : V \to \{1, ..., 8\}$ (we assume a uniform distribution of the random functions from V to $\{1, ..., 8\}$, then $H(f) = 3$). Since for each i, j the graph $C_{l'}(V^i_{t+1}, V^j_{t+1})$ is a matching, the events "$f(a) = f(b)$" (i.e. the edge (a, b) remains in $C_{l_{t+1}}(V^i_{t+1}, V^j_{t+1})$) over all edges (a, b) in this graph are mutually independent. The probability of each such event is $\frac{1}{8}$. By Chernoff bound [2] we get ($C = |C_{l_{t+1}}(V^i_{t+1}, V^j_{t+1})|$ is a random variable with a binomial distribution, $E(C) \leq \frac{m}{2}$):

$$Pr[C \geq m] \leq e^{-\frac{1}{2}\left(\frac{m}{E(C)}-1\right)^2 E(C)} \leq e^{-\frac{m}{4}} = \frac{1}{p^2}.$$

Thus

$$Pr[\exists i < j, |C_{l_{t+1}}(V^i_{t+1}, V^j_{t+1})| \geq m] \leq \binom{p}{2} \frac{1}{p^2} < 1,$$

i.e. there exists f such that for $l_{t+1} = (l', f)$ the invariant 2(b) holds for time $t+1$. Invariant 2(a) follows for time $t+1$ from the subaddivity property of the entropy: $H(l_{t+1}) \leq H(l_t) + H(\chi) + H(f) \leq (t+1)\left(L\left(\frac{pm}{n}\right) + 3\right)$. This is the end of the inductive step.

It remains to show there are the two inputs in I_T, one element distinct and the other not, that are indistinguishable to the given PRAM up to step T. Suppose there is at least one pair of variables (x_j, x_k) such that (i) (x_j, x_k) is not an edge in DG_T graph and (ii) $l_T(x_j) = l_T(x_k)$. Then due to invariants 4 and 5 for every $a \in I_T$ at most one of variables x_j, x_k can affect the state of P_1 at the beginning of step T. Suppose that x_k does not affect the state of P_1. Choose $a \in I_T$ with all coordinates a_i distinct and let $\bar{a}$ be such that $\bar{a}_i = a_i$ for $i \neq k$ and $\bar{a}_k = a_j$. Surely $\bar{a} \in I_T$. Furthermore, since the state of P_1 is not affected at the beginning of step T by the variable x_k, the PRAM cannot distinguish the two inputs $\bar{a}$ and a up to step T. So it suffices to show that there exists a pair of variables (x_j, x_k) such that (i) and (ii) hold for DG_T and l_T.

Let us make some definitions first. For a function f with domain $A \subseteq V$, let $K(f)$ be a graph (V, E) such that $E = \{(a, b) \mid a, b \in A \ : \ f(a) \neq f(b)\}$. For a set F of such functions we define $K(F) = \bigcup_{f \in F} K(f)$. Let's define next

$$cost(f) = \frac{|dom(f)|}{|V|} H(f), \quad cost(F) = \sum_{f \in F} cost(f).$$

For a graph G on V define

$$content(G) = \min_{K(F) \supseteq G} cost(F).$$

The subadivity of entropy implies subadivity of content.

Let $CG = K(l_T)$. Clearly if $CG \cup DG_T$ is not complete graph K_n then the desired pair of variables (x_j, x_k) exists. A useful result by Fredman and Komlós [6] says that content of the complete graph K_n is equal to $\log_2 n$. Thus to show that $CG \cup DG_T \neq K_n$ it suffices to show that $content(CG) + content(DG_T) < \log_2 n$. By the definition of CG and by invariant 2(a) for step T we have $content(CG) \leq H(l_T) \leq \left(L\left(\frac{8p\log p}{n}\right) + 3\right) T$. Since $content(CG) > 0.1 \log n$ would imply $T = \Omega\left(\frac{n \log n}{p \log(\frac{n}{p} \log n + 1)}\right)$ let us assume that $content(CG) \leq 0.1 \log n$.

Bounding $content(DG_T)$ will be more complicated. We will describe DG_T in other way and then divide it into two parts DG_1 and DG_2 for which it is easier to bound their content. Let's define $A_t^i = \bigcup_{i=t+1}^{T} C_t^i$, for $1 \leq i \leq n_T,\ 1 \leq t \leq T$. Put

$$TS = \{(A_i^t - C_i^t, C_i^t) \mid 1 \leq i \leq n_T,\ 1 \leq t \leq T-1\}.$$

Let $E = \{(x_i, x_j) \mid \exists (A, C) \in TS\ \exists a \in A\ \exists c \in C\ :\ (a, c) \text{ covers } (x_i, x_j)\}$. Then for graph $DG' = (V, E)$ it follows $DG_T \subseteq DG'$, and $content(DG_T) \leq content(DG')$.

We may assume that $|V_T^i| \leq n^{0.1}$ for $1 \leq i \leq p$ since the other case would imply $T = \Omega\left(\frac{n \log n}{p \log(\frac{n}{p} \log n + 1)}\right)$. Lemma 4.1 [4], when applied to our set TS, says that there is a set $\Phi = \{(B_i, D_i) \mid 1 \leq i \leq r\}$ such that

1) $B_i \cup D_i = V$, $B_i \cap D_i = \emptyset$,
2) $|E - E_1| \leq n^{0.1}\sqrt{n} \log(|TS|)|TS| + \frac{|TS|^2}{\sqrt{n}}$
   for $E_1 = \{(x_k, x_l) \mid \exists (B_i, D_i) \in \Phi\ :\ x_k \in B_i, x_l \in D_i\}$.

where $|TS| = \sum_{i,t}(|A_i^t - C_i^t| + |C_i^t|)$. In other words it is possible to divide the graph DG' conveniently in two parts $DG_1 = (V, E_1)$ and $DG_2 = (V, E - E_1)$ such that $DG_1 \cup DG_2 = DG'$.

By Lemma 3.4 [1] every graph with n vertices and $|E - E_1|$ edges has a coloring χ with entropy $H(\chi) \leq \log_2\left(\left(\frac{|E-E_1|}{n} + 1\right) e\right)$. Since $DG_2 \subseteq K(\chi)$, it follows that $content(DG_2) \leq cost(\chi) = H(\chi)$. For $p > n \log n$ the lower bound of the main theorem is trivial, so assume $p \leq n \log n$. Remember also that we assume $T < \log n$. Then because $|TS| \leq 2pT^2$ we have

$$|E - E_1| \leq n^{0.1}\sqrt{n} \log(2pT^2) 2pT^2 + \frac{4p^2T^4}{\sqrt{n}} \leq n^{1.6} \ .$$

Thus $H(\chi) \leq 0.7 \log n$ and $content(DG_2) \leq 0.7 \log n$.

For each $(B_i, D_i) \in \Phi$ define function $h_i : V \to \{0,1\}$ in the following way: for $x \in B_i$ let $h_i(x) = 0$, for $x \in D_i$ let $h_i(x) = 1$. We put $H = \bigcup_{i=1}^{r} h_i$. Then $DG_1 \subseteq K(H)$. By definition $cost(H) = \sum_{i=1}^{r} \frac{|dom(h_i)|}{n} H(h_i)$. With the help of Lemma 4.2 [4] we have

$$cost(H) \leq \frac{2pT^2}{n} \frac{2 \log T}{T} = 4 \frac{p}{n} T \log T \ .$$

Let us assume $cost(H) \leq 0.1 \log_2 n$ since the other case would imply $T = \Omega\left(\frac{n \log n}{p \log(\frac{n}{p} \log n + 1)}\right)$. It follows that $content(DG_1) \leq 0.1 \log_2 n$ and $cost(DG') \leq 0.8 \log_2 n$.

Putting together the bounds on $content(CG)$ and $content(DG')$ we get the desired $content(CG) + content(DG) < \log_2 n$ which implies the existence of a pair of variables (x_j, x_k) that are neither an edge in DG_T neither comparable in l_T. Thus, as described earlier, there are two different inputs, one element distinct and the other not that are indistinguishable to the given PRAM through step T which is the desired contradiction.

References

1. Boppana R.V.: Optimal Separations Between Concurrent-Write Parallel Machines, Proc. 21th ACM Symp. on Theory of Computing (1989) 320-326
2. Chernoff H.: A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the Sum of Observations, Annals of Math. Stat. **23** (1952) 493-509
3. Edmonds J.: Lower Bounds with Smaller Domain Size, Structures in Complexity Theory (1991) 322-331
4. Edmonds J.: Removing Ramsey Theory: Lower Bounds with Smaller Domain Size, Journal of Theoretic Computer Science, submited, available as Postscript file at `http://www.cs.yorku.ca/~ jeff/research/index.html`
5. Erdös P. and Rado R.: A Combinatorial Theorem, J. London Math. Soc. **25** (1950) 376-382
6. Fredman M., Komlós J.: On the Size of Separating Systems and Families of Perfect Hash Functions, SIAM J. Alg. Disc. Meth. **5** (1984) 61-68
7. Fich F. E., Meyer Auf Der Heide F., Wigderson A.: Lower Bounds for Parallel Random-Access Machines with Unbounded Shared Memory, Advances in Computing Research **4** (1986) 1-15
8. Fich, F . E., Ragde, P. L., Wigderson, A.: Relations Between Concurrent-Write Models of Parallel Computation, SIAM J. Comp. **17** (1988) 606-627
9. Kolman, P.: Complexity of Some Problems on COMMON PRAM, Masters Thesis, Charles University, Prague (1995), in Czech
10. Meyer Auf Der Heide F., Wigderson A.: The Comlexity of Parallel Sorting, 26th FOCS (1985) 532-540
11. Ragde P. L., Steiger W., Szemeredi E., Wigderson A.: The Parallel Complexity of Element Distinctness is $\Omega(\sqrt{\log n})$, SIAM J. Disc. Math. **1** (1988) 399-410

A Counter Example

In this part a brief description of a counter example to Lemma 4.3 [1] together with a short discussion of the problem will be given.

Let's consider a COMMON PRAM that consists of two processors P_1 and P_2 and unbounded memory. Let D be the infinite set of possible input values. The computation proceeds as follows: In the first step P_i, $1 \leq i \leq 2$, reads the contents of cell $x_i + 3$ and writes 19 to the same cell. In the second step P_1 reads the contents of cell $x_1 + 3$ and then writes 1 there, while P_2 reads the contents of cell 2 and writes 7 there. In the third and last step P_1 reads the contents of cell 1 and writes 9 there, P_2 reads from cell $x_2 + 3$ and writes 17 there. If P_2 reads 1 in this step the input numbers are not element distinct, otherwise they are (the written values have no special meaning, some of them only need to be different). Let us notice that the described PRAM fulfills the requirements of the COMMON model and that it indeed solves the element distinctness problem.

The read-index and write-index functions of the processors are easy to derive. They satisfy without any additional adjustment the assumption on identity of the read-index and write-index functions of each processor in each step as required in the proof of Lemma 4.3 [1]. For the set F of write-index functions it holds that for $C = D$, $F|_C$ is reducible to the one-to-one set $G = \{g_1(y) = y+3, g_2() = 1, g_3() = 2\}$, i.e. the set $F|_C$ is canonical.

A merging and distinctness-checking machine constructed according to the proof of Lemma 4.3 [1] has a possible path of the computation (in fact there is only one path, there is no branching in the computational tree) that ends with the pair $\{x_1, x_2\}$ neither comparable in the partial order Γ, nor an edge in the distinctness graph DG, i.e. it does *not* solve the problem whereas the original COMMON PRAM *does*. For lack of space we omit detail description of the construction, it is given in [9].

The problem is that according to the definition of merging and distinctness-checking machine every access pair may be choosen at most one time. This fact is used in the the proof of the lower bound for the merging and distinctness-checking machine in Lemma 4.6 [1]. The consequence of this limitation is that the simulating merging and distinctness-checking machine is unable to compare some pairs of variables that the original PRAM was able. It is possible to show [9] that, to make the simulation possible, it is necessary either to impose no limitation on the nuber of times an access pairs may be choosen by the merging and distinctness-checking machine, or to allow it to be choosen at least $\Omega\left(\frac{\log n}{\log\log n}\right)$ times. However, in either way it would weaken the lower bound of Lemma 4.6, if no other changes would be done in the proof of it.

This article was processed using the LaTeX macro package with LLNCS style