Algorithms and datastructures II

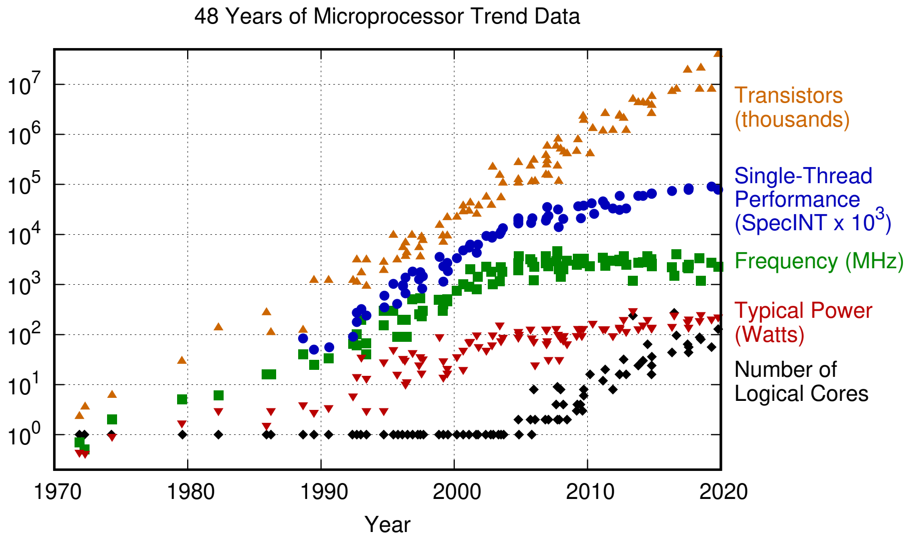
Lecture 6: circuit complexity 2/2

Jan Hubička

Department of Applied Mathematics
Charles University
Prague

Nov 9 2020

Parallel computing



Original data up to the year 2010 collected and plotted by M. Horowitz, F. Labonte, O. Shacham, K. Olukotun, L. Hammond, and C. Batten
New plot and data collected for 2010-2019 by K. Rupp

Computational model

Definition (Circuit)

Circuit is defined by:

1. Alphabet Σ.
2. Pairwise disjoint set of vertices I (input), O (output) and H (gate).
3. Acyclic directed multi-graph (V, E) with $E = I \cup O \cup H$.
4. Mapping F which assign every gate $g \in H$ of arity $a(g)$ a function $F(h) : \Sigma^{a(g)} \to \Sigma$.
5. Mapping $z : E \to \mathbb{N}$ which maps every edge to a gate to index which argument it represents.

Satisfying:

1. In-degree of vertices in I is 0.
2. In-degree of vertices in O is 1 and out-degree is 0.
3. In-degree of every gate corresponds to its arity. Out-degree of every gate is at least 1.
4. Every input of every gate is assigned.

Computational model: computation

Definition (Computation)

Computation happens in steps (clocks):

1. step 0: All inputs and constants gets assigned value.
2. step $i + 1$: Assign value to all gates and outputs for which all inputs are determined at step i.

Computation ends once all vertices have value assigned.

Definition (Layer)

Layer i consist of all vertices whose value is determined in step i.

Layer is also maximal distance from some input.

Definition (Time complexity)

Time of the computation of a given circuit is determined by the number of layers.

Definition (Space complexity)

Space of the computation is determined by the number of gates in the circuit.

Computational model: program

Definition (Program)

Program is a sequence of circuits for individual sizes of inputs.

Remarks:

1. It is necessary to restrict types of allowed gates (or their arity) and Σ. Otherwise every problem can be solved by a single gate.
2. Typically we want network for a given size to be generated by an effective non-parallel algorithm.

We will typically consider boolean circuits where $\Sigma = \{0, 1\}$ and arity is at most 2.

Comparator networks: An example

Σ consists of values being sorted.
Comparators are "gates" with two inputs and two outputs.

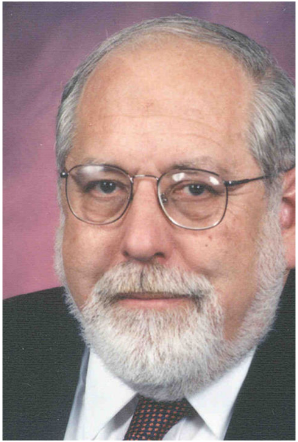
Comparator networks: An example

Σ consists of values being sorted.
Comparators are “gates” with two inputs and two outputs.
Example: Bubble sort

Comparator networks: An example

Σ consists of values being sorted.
Comparators are “gates” with two inputs and two outputs.
Example: Bubble sort
Example: Insert sort

Bitonic sorting, 1968



Ken Batcher

Bitonic sequences

Definition (Purely bitonic sequence)

Sequence $x_0, x_1, \ldots, x_{n-1}$ is purely bitonic if it can be split at some position k such that $x_0, x_1, \ldots, x_k$ is growing and $x_k, x_{k+1}, \ldots, x_{n-1}$ is decreasing.

Bitonic sequences

Definition (Purely bitonic sequence)

Sequence $x_0, x_1, \ldots, x_{n-1}$ is purely bitonic if it can be split at some position k such that $x_0, x_1, \ldots, x_k$ is growing and $x_k, x_{k+1}, \ldots, x_{n-1}$ is decreasing.

Definition (Bitonic sequence)

Sequence is bitonic if it is created as a rotation of a purely bitonic sequence.

Bitonic comparator

Definition (Bitonic separator)

An separator of degree n is a comparator network S_n with inputs $x_0, x_1, \ldots, x_{n-1}$ and outputs $y_0, y_1, \ldots, y_{n-1}$. If it is given a bitonic sequence it produces its permutation with the following properties:

1. $y_0, y_1, \ldots, y_{n/2-1}$ and $y_{n/2}, y_{n/2+1}, \ldots, y_{n-1}$ are bitonic sequences;
2. $y_i < y_j$ whenever $0 \leq i < n/2 \leq j < n$.

Bitonic comparator

Definition (Bitonic separator)

An separator of degree n is a comparator network S_n with inputs $x_0, x_1, \ldots, x_{n-1}$ and outputs $y_0, y_1, \ldots, y_{n-1}$. If it is given a bitonic sequence it produces its permutation with the following properties:

1. $y_0, y_1, \ldots, y_{n/2-1}$ and $y_{n/2}, y_{n/2+1}, \ldots, y_{n-1}$ are bitonic sequences;
2. $y_i < y_j$ whenever $0 \leq i < n/2 \leq j < n$.

Lemma (On separators)

For every n there exists a separator S_n of constant depth with $\Theta(n)$ comparators.

Will show this later

Bitonic sorter

Definition (Bitonic sorter)

Bitonic sorter of degree n is a comparator network B_n with n inputs and n outputs which sorts every bitonic sequence of length n.

Lemma (On bitonic sorter)

For every $n = 2^k$ there exists a bitonic of depth $\Theta(\log n)$ and with $\Theta(n \log n)$ comparators.

Bitonic sorter

Definition (Bitonic sorter)

Bitonic sorter of degree n is a comparator network B_n with n inputs and n outputs which sorts every bitonic sequence of length n.

Lemma (On bitonic sorter)

For every $n = 2^k$ there exists a bitonic of depth $\Theta(\log n)$ and with $\Theta(n \log n)$ comparators.

We will apply:

Lemma (On separators)

For every n there exists a separator S_n of a constant depth with $\Theta(n)$ comparators.

Merge

Definition (Merging netwok)

Merging network of degree n is a comparator network M_n with $2n$ inputs and $2n$ outputs. Given two sorted sequences on input it merges them to output.

Lemma (On merging)

For every $n = 2^k$ there exists a merging network of depth $\Theta(\log n)$ and with $\Theta(n \log n)$ comparators. If it is given two sorted sequences it produces results of their merge.

Merge

Definition (Merging netwok)

Merging network of degree n is a comparator network M_n with $2n$ inputs and $2n$ outputs. Given two sorted sequences on input it merges them to output.

Lemma (On merging)

For every $n = 2^k$ there exists a merging network of depth $\Theta(\log n)$ and with $\Theta(n \log n)$ comparators. If it is given two sorted sequences it produces results of their merge.

We will apply:

Lemma (On bitonic sorter)

For every $n = 2^k$ there exists a bitonic of depth $\Theta(\log n)$ and with $\Theta(n \log n)$ comparators.

Bitonic merge

Theorem

For $n = 2^k$ there exists comparator network T_n of depth $\Theta(\log^2 n)$ with $\Theta(n \log^2 n)$ comparators.

Bitonic merge

Theorem

For $n = 2^k$ there exists comparator network T_n of depth $\Theta(\log^2 n)$ with $\Theta(n \log^2 n)$ comparators.

We will apply:

Lemma (On merging)

For every $n = 2^k$ there exists a merging network of depth $\Theta(\log n)$ and with $\Theta(n \log n)$ comparators. If it is given two sorted sequences it produces results of their merge.

Bitonic merge

Theorem

For $n = 2^k$ there exists comparator network T_n of depth $\Theta(\log^2 n)$ with $\Theta(n \log^2 n)$ comparators.

We will apply:

Lemma (On merging)

For every $n = 2^k$ there exists a merging network of depth $\Theta(\log n)$ and with $\Theta(n \log n)$ comparators. If it is given two sorted sequences it produces results of their merge.

We need $\log n$ layers of merging networks. Network on layer i has depth i.

$$\Theta(1 + 2 + 3 + \cdots + \log n) = \Theta(\log_n^2)$$

.

Bitonic separator

Definition (Bitonic separator)

An separator of degree n is a comparator network S_n with inputs $x_0, x_1, \ldots, x_{n-1}$ and outputs $y_0, y_1, \ldots, y_{n-1}$. If it is given a bitonic sequence it produces its permutation with the following properties:

1. $y_0, y_1, \ldots, y_{n/2-1}$ and $y_{n/2}, y_{n/2+1}, \ldots, y_{n-1}$ are bitonic sequences;
2. $y_i < y_j$ whenever $0 \leq i < n/2 \leq j < n$.

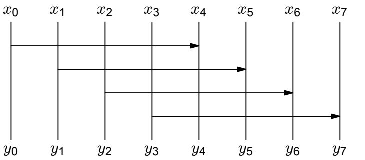
Lemma (On separators)

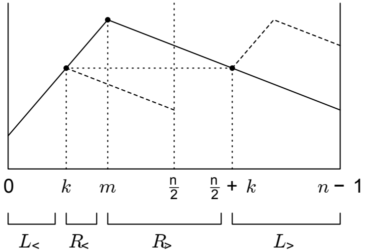
For every n there exists a separator S_n of a constant depth with $\Theta(n)$ comparators.

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.



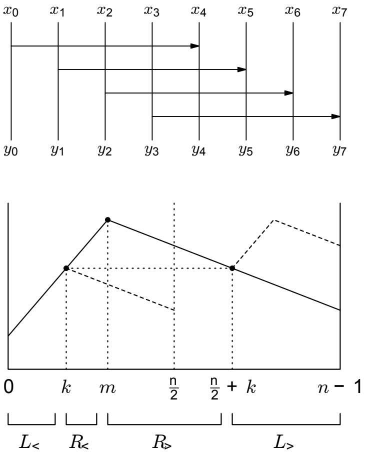


1. Denote by m the index such that x_m is maximum of the sequence. WLOG assume that $m < n/2$.

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.

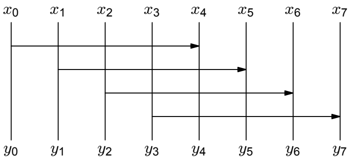


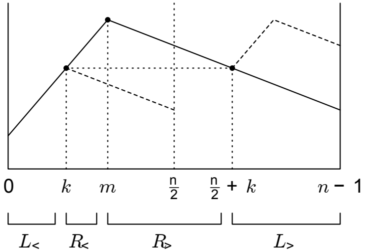
1. Denote by m the index such that x_m is maximum of the sequence. WLOG assume that $m < n/2$.
2. Let $k = min\{i : x_i > x_{n/2+i}\}$.
3. Observe that for $i = k, \ldots, n/2 - 1$ the comparators will always swap.

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.



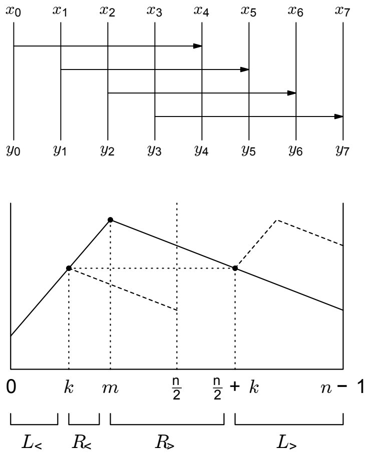


1. Denote by m the index such that x_m is maximum of the sequence. WLOG assume that $m < n/2$.
2. Let $k = min\{i : x_i > x_{n/2+i}\}$.
3. Observe that for $i = k, \ldots, n/2 - 1$ the comparators will always swap.
4. Left subsequence is increasing sequence $x_0, \ldots, x_{k-1}$ merged with decreasing sequence $x_{n/2+k}, \ldots, x_{n-1}$.

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.



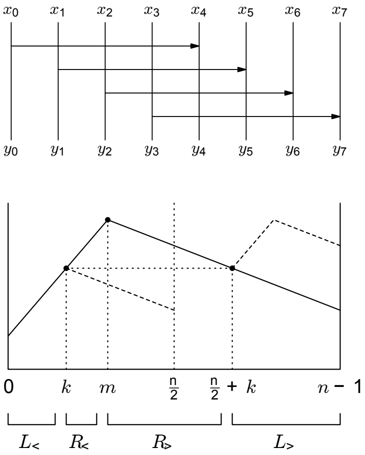
1. Denote by m the index such that x_m is maximum of the sequence. WLOG assume that $m < n/2$.
2. Let $k = min\{i : x_i > x_{n/2+i}\}$.
3. Observe that for $i = k, \dots, n/2 - 1$ the comparators will always swap.
4. Left subsequence is increasing sequence $x_0, \dots, x_{k-1}$ merged with decreasing sequence $x_{n/2+k}, \dots, x_{n-1}$.
5. Right subsequence is decreasing sequence $x_{n/2}, \dots, x_{n/2+k-1}$ merge with increasing sequence $x_k, \dots, x_{m-1}$ and decreasing sequence $x_m, \dots, x_{n/2} - 1$.

Observe that both sequences are bitonic

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.



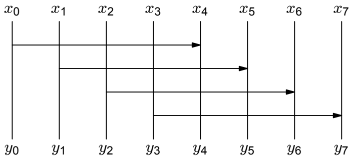
It remains to check that left sequence is smaller than right.
Put:

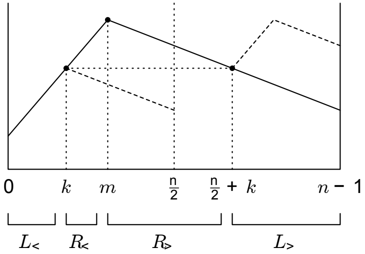
1. $L_< = (x_0, \ldots, x_{k-1})$
2. $L_> = (x_{n/2+k}, \ldots, x_{n-1})$
3. $R_< = (x_k, \ldots, x_{m-1})$
4. $R_> = (x_m, \ldots, x_{n/2+k-1})$

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.





It remains to check that left sequence is smaller than right.

Put:

1. $L_< = (x_0, \ldots, x_{k-1})$
2. $L_> = (x_{n/2+k}, \ldots, x_{n-1})$
3. $R_< = (x_k, \ldots, x_{m-1})$
4. $R_> = (x_m, \ldots, x_{n/2+k-1})$

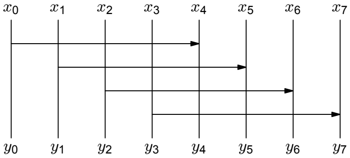
Check:

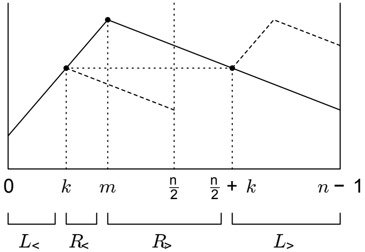
1. $L_< < R_<$:

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.





It remains to check that left sequence is smaller than right.
Put:

1. $L_< = (x_0, \dots, x_{k-1})$
2. $L_> = (x_{n/2+k}, \dots, x_{n-1})$
3. $R_< = (x_k, \dots, x_{m-1})$
4. $R_> = (x_m, \dots, x_{n/2+k-1})$

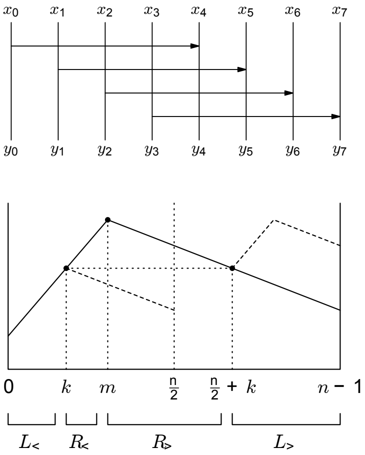
Check:

1. $L_< < R_<$: Formerly increasing sequence

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.



It remains to check that left sequence is smaller than right.
Put:

1. $L_< = (x_0, \dots, x_{k-1})$
2. $L_> = (x_{n/2+k}, \dots, x_{n-1})$
3. $R_< = (x_k, \dots, x_{m-1})$
4. $R_> = (x_m, \dots, x_{n/2+k-1})$

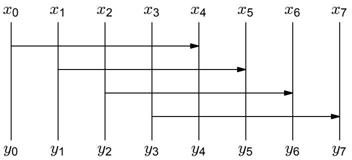
Check:

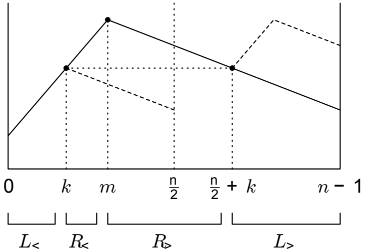
1. $L_< < R_<$: Formerly increasing sequence
2. $L_< < R_>$:

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.





It remains to check that left sequence is smaller than right.
Put:

1. $L_< = (x_0, \dots, x_{k-1})$
2. $L_> = (x_{n/2+k}, \dots, x_{n-1})$
3. $R_< = (x_k, \dots, x_{m-1})$
4. $R_> = (x_m, \dots, x_{n/2+k-1})$

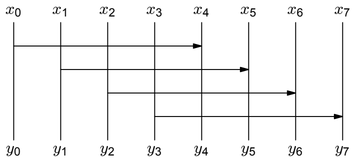
Check:

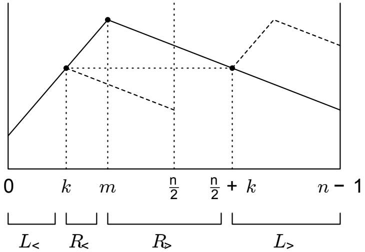
1. $L_< < R_<$: Formerly increasing sequence
2. $L_< < R_>$: $\max L_< = x_{k-1} < x_{n/2+k-1} = \min P_>$

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.





It remains to check that left sequence is smaller than right.
Put:

1. $L_< = (x_0, \ldots, x_{k-1})$
2. $L_> = (x_{n/2+k}, \ldots, x_{n-1})$
3. $R_< = (x_k, \ldots, x_{m-1})$
4. $R_> = (x_m, \ldots, x_{n/2+k-1})$

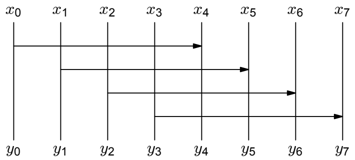
Check:

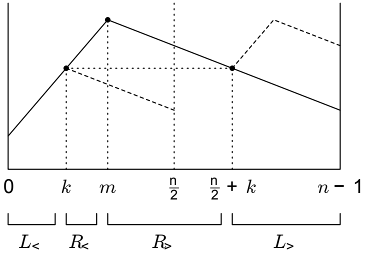
1. $L_< < R_<$: Formerly increasing sequence
2. $L_< < R_>$: $\max L_< = x_{k-1} < x_{n/2+k-1} = \min P_>$
3. $L_> < R_<$:

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.





It remains to check that left sequence is smaller than right.
Put:

1. $L_< = (x_0, \ldots, x_{k-1})$
2. $L_> = (x_{n/2+k}, \ldots, x_{n-1})$
3. $R_< = (x_k, \ldots, x_{m-1})$
4. $R_> = (x_m, \ldots, x_{n/2+k-1})$

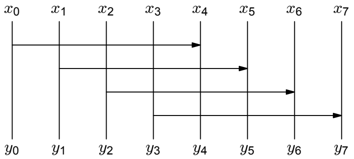
Check:

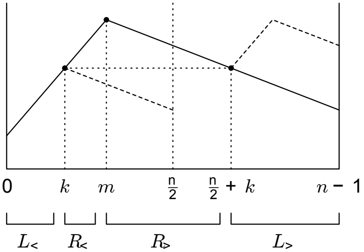
1. $L_< < R_<$: Formerly increasing sequence
2. $L_< < R_>$: $\max L_< = x_{k-1} < x_{n/2+k-1} = \min P_>$
3. $L_> < R_<$: $\max L_> = x_{n/2+k} < x_k = \min P_<$

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.





It remains to check that left sequence is smaller than right.
Put:

1. $L_< = (x_0, \ldots, x_{k-1})$
2. $L_> = (x_{n/2+k}, \ldots, x_{n-1})$
3. $R_< = (x_k, \ldots, x_{m-1})$
4. $R_> = (x_m, \ldots, x_{n/2+k-1})$

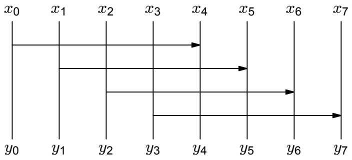
Check:

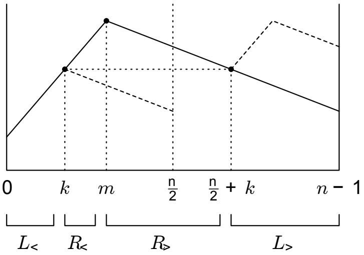
1. $L_< < R_<$: Formerly increasing sequence
2. $L_< < R_>$: $\max L_< = x_{k-1} < x_{n/2+k-1} = \min P_>$
3. $L_> < R_<$: $\max L_> = x_{n/2+k} < x_k = \min P_<$
4. $L_> < R_>$:

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.





It remains to check that left sequence is smaller than right.
Put:

1. $L_< = (x_0, \ldots, x_{k-1})$
2. $L_> = (x_{n/2+k}, \ldots, x_{n-1})$
3. $R_< = (x_k, \ldots, x_{m-1})$
4. $R_> = (x_m, \ldots, x_{n/2+k-1})$

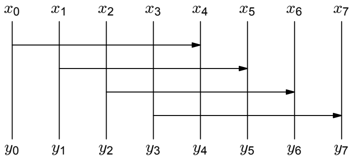
Check:

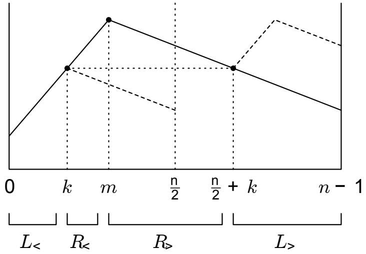
1. $L_< < R_<$: Formerly increasing sequence
2. $L_< < R_>$: $\max L_< = x_{k-1} < x_{n/2+k-1} = \min P_>$
3. $L_> < R_<$: $\max L_> = x_{n/2+k} < x_k = \min P_<$
4. $L_> < R_>$: Formerly decreasing sequence

Bitonic separator on purely bitonic sequence

Observation

Separator works on purely bitonic sequences.





It remains to check that left sequence is smaller than right.

Put:

1. $L_< = (x_0, \ldots, x_{k-1})$
2. $L_> = (x_{n/2+k}, \ldots, x_{n-1})$
3. $R_< = (x_k, \ldots, x_{m-1})$
4. $R_> = (x_m, \ldots, x_{n/2+k-1})$

Check:

1. $L_< < R_<$: Formerly increasing sequence
2. $L_< < R_>$: $\max L_< = x_{k-1} < x_{n/2+k-1} = \min P_>$
3. $L_> < R_<$: $\max L_> = x_{n/2+k} < x_k = \min P_<$
4. $L_> < R_>$: Formerly decreasing sequence

Bitonic separators

Lemma (On separators)

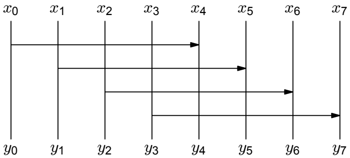
For every n there exists a separator S_n of a constant depth with $\Theta(n)$ comparators.

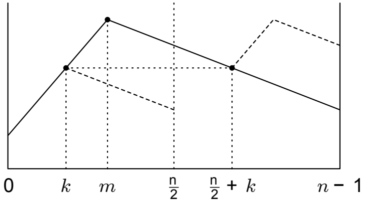
Bitonic separators

Lemma (On separators)

For every n there exists a separator S_n of a constant depth with $\Theta(n)$ comparators.

We proved Lemma for purely bitonic sequences. To see that separator works on bitonic sequence observe that it is symmetric for rotation. If input sequence is rotated by r to right, still same values are compared. Output bitonic sequences will also be rotated by r.





Bitonic separators: alternative proof

Lemma (On separators)

For every n there exists a separator S_n of a constant depth with $\Theta(n)$ comparators.

Lemma

If a comparison network transforms the input sequence $x_0, \ldots, x_{n-1}$ into the output sequence $y_0, \ldots, y_{n-1}$, then for any nondecreasing function f, the network transforms the input sequence $f(x_0), \ldots, f(x_{n-1})$ into the output sequence $f(y_0), \ldots, f(y_{n-1})$.

Bitonic separators: alternative proof

Lemma (On separators)

For every n there exists a separator S_n of a constant depth with $\Theta(n)$ comparators.

Lemma

If a comparison network transforms the input sequence $x_0, \ldots, x_{n-1}$ into the output sequence $y_0, \ldots, y_{n-1}$, then for any nondecreasing function f, the network transforms the input sequence $f(x_0), \ldots, f(x_{n-1})$ into the output sequence $f(y_0), \ldots, f(y_{n-1})$.

Corollary (Zero-one principle)

If a sorting network works correctly when each input is drawn from the set $\{0, 1\}$, then it works correctly on arbitrary input numbers.

Bitonic separators: alternative proof

Lemma (On separators)

For every n there exists a separator S_n of a constant depth with $\Theta(n)$ comparators.

Lemma

If a comparison network transforms the input sequence $x_0, \ldots, x_{n-1}$ into the output sequence $y_0, \ldots, y_{n-1}$, then for any nondecreasing function f, the network transforms the input sequence $f(x_0), \ldots, f(x_{n-1})$ into the output sequence $f(y_0), \ldots, f(y_{n-1})$.

Corollary (Zero-one principle)

If a sorting network works correctly when each input is drawn from the set $\{0, 1\}$, then it works correctly on arbitrary input numbers.

Observation

$\{0, 1\}$-sequence is bitonic if it contains at most two changes between 0 and 1.

Bitonic separators: alternative proof

Lemma (On separators)

For every n there exists a separator S_n of a constant depth with $\Theta(n)$ comparators.

Lemma

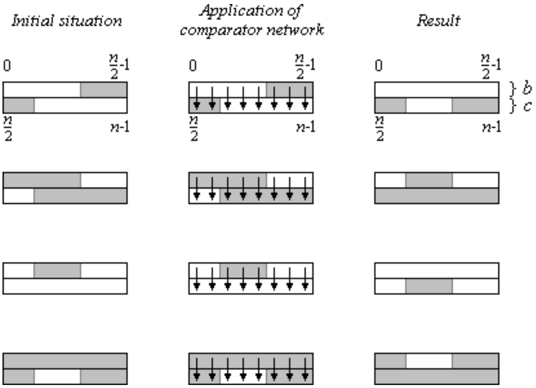
If a comparison network transforms the input sequence $x_0, \ldots, x_{n-1}$ into the output sequence $y_0, \ldots, y_{n-1}$, then for any nondecreasing function f, the network transforms the input sequence $f(x_0), \ldots, f(x_{n-1})$ into the output sequence $f(y_0), \ldots, f(y_{n-1})$.

Corollary (Zero-one principle)

If a sorting network works correctly when each input is drawn from the set $\{0, 1\}$, then it works correctly on arbitrary input numbers.

Observation

$\{0, 1\}$-sequence is bitonic if it contains at most two changes between 0 and 1.



Bitonic sort