数理解析研究所講究録
第 754 巻 1991 年 82-93

Selection Networks with $8n\log_2 n$ Size and $O(\log n)$ Depth

Shuji JIMBO and Akira MARUOKA
神保秀司　　丸岡章
Faculty of Engineering, Tohoku University

31-Jan-91, LA Symposium in Kyoto

Abstract Selection networks composed of comparators that select the smallest $n/2$ elements from n inputs are investigated, and such networks with $8n\log_2 n$ size and $O(\log n)$ depth are constructed. This result improves [AKS83a][AKS83b] in constant factor of size and in simplicity of construction, and [Pip90] in order of depth, in which selection networks with $2n\log_2 n$ size and $O((\log n)^2)$ depth are constructed.

1 Introduction

An comparator network is a network consisting of elements called comparators. A comparator is a module with two inputs and two outputs which sorts any two elements on the two inputs. A (n, k)-selector, where $1 \leq k < n$, is a comparator network with n inputs $(x_1, x_2, \ldots, x_n)$ and n outputs $(y_1, y_2, \ldots, y_n)$ such that the set $\{y_1, y_2, \ldots, y_k\}$ consists of the smallest k elements of $x_1, x_2, \ldots, x_n$. A sorting network with n inputs is a comparator network with n inputs $(x_1, x_2, \ldots, x_n)$ and n outputs $(y_1, y_2, \ldots, y_n)$ such that $y_1 \leq y_2 \leq \ldots \leq y_n$. A sorting network with n inputs is also called an n-sorter.

Since n-sorters are also (n,k)-selectors, the existence of n-sorters with $O(n\log n)$ size and $O(\log n)$ depth, given in [AKS83a][AKS83b], immediately implies the existence of (n,k)-selectors with the same size and depth. Main concern in [AKS83a][AKS83b] seems to prove just the existence of n-sorters with the size and depth, so the construction of soters is of some intricacy, and the constant factors in the depth and size bound are enormous. In fact, in spite of efforts in [Pat] to improve the previous construction, the numerical constant in the size bound have not been brought below 1000. Since selectors don't do as much as sortors do, it is natural to ask whether we can obtain much simpler construction of (n,k)-selectors with smaller constant factors. Based on the same fundamental idea as their sorters, Pippenger[Pip90] constructed (n, $n/2$)-selectors of approximate $2n\log_2 n$ size and $O((\log n)^2)$ depth. In the same spirit, we aslo investigate the construction, obtaining relatively simple (n, $n/2$)-selectors of approximate $8n\log_2 n$ size and $O(\log n)$ depth.

In Section 2 we explain notations and definitions. In Section 3 we give some genaral properties of comparator networks. In Section 4, we give some types of comparator subnetworks which are used to construct selectors. In Section 5, we explain how to assemble the subnetworks to obtain selectors. Moreover, the justification of the construction and the size and depth bound of the selectors are discussed.

2 Preliminaries

In the following, basic notations and definitions need for constructing (n, n/2)-selectors are explained.

Notation 1 (The number of the elements of a finite set) For a finite set X, $|X|$ denotes the number of the elements of X. □

Notation 2 (A Cartesian product of mappings) Let $f : A \to B$ and $g : C \to D$ be mappings. $f \times g$ denotes the *Cartesian product* of f and g. $f \times g : A \times C \to B \times D$ is defined by

$$(f \times g)(x,\ y) = (f(x),\ g(y))$$

for all $x \in A$ and $y \in C$.

The n times Cartesian product of f,

$$\overbrace{f \times f \times \ldots \times f}^{n},$$

is denoted by $f^{\times n}$. □

Definition 1 (A comparator network) A comparator network is a directed graph $G = (V, E)$ satisfying the following conditions:

1. G has no cycles.
2. If the in-degree of a vertex $v \in V$ is 0 then the out-degree of v is 1. We call such a vertex an *input terminal.*
3. If the out-degree of a vertex $v \in V$ is 0 then the in-degree of v is 1. We call such a vertex an *output terminal.*
4. The in-degree and the out-degree of a vertex $v \in V$ except input terminals and output terminals are both 2. We call such a vertex a *comparator.* Only one of two labels, called MAX and MIN, is placed on each of the two edges incident out of each comparator so that if label MAX is placed on one of the two edges then label MIN is placed on the other. In this paper, we call an edge on which the label MAX is placed a *MAX edge*, and also call an edge on which the label MIN is placed a *MIN edge.*

From these conditions, we can easily deduce that the number of the input terminals of G is equal to the one of the output terminals. Let n denote the number of the input terminals of comparator networks G. Moreover, it is easy to see that there exist a set of n paths from the input terminals of G to the output terminals of G such that, for every two paths p, q of the n paths, the intersection of the edges on p and the edges on q is empty and every edge or vertex of G belongs to one of the n paths, namely the edge disjoint n paths cover graph G.

Assume that n paths covering comparator network G are taken to be fixed. These n paths are denoted by distinct integers from 1 to n. We call such a path a *register.* The input terminal on register i is called input terminal i or the i-th input terminal. Similarly, the output terminal on register i is called output terminal i or the i-th output terminal. □

We show an example of a comparator network in Figure 1.

Definition 2 (The mapping associated with a comparator network) Let G be a comparator network with n registers, and S a totally ordered set. There is a unique way of assigning mappings to the edges of G. All those mappings are $S^n \to S$. Let e be an edge of G, and let f_e denote the

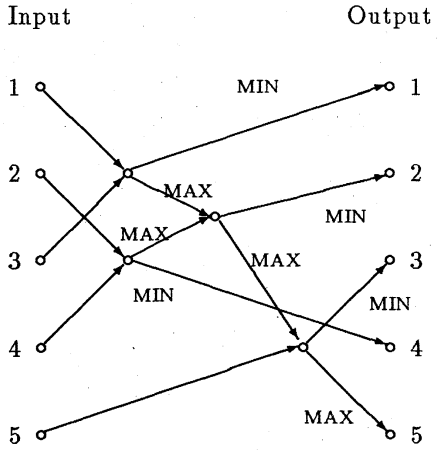

Figure 1: An example of a comparator network

mapping assigned to e. f_e is determined in the flollowing way.

1. If e is incident out of an input terminal of G then f_e is the mapping satisfying that $f_e(x_1, x_2, \ldots, x_n) = x_i$ for every $(x_1, x_2, \ldots, x_n) \in S^n$, where i is an integer denoting the register containing e.
2. If e is incident out of a comparator, the following two cases are concidered. Let e_a and e_b denote the edges incident into the comparator.
   (a) If label MAX is put on e, then f_e is the mapping satisfying that $f_e(x) = \max\{f_{e_a}(x), f_{e_b}(x)\}$.
   (b) If label MIN is put on e, then f_e is the mapping satisfying that $f_e(x) = \min\{f_{e_a}(x), f_{e_b}(x)\}$.

Let $e_1, \ldots, e_n$ denote the n edges incident into output terminals of G. Π_G^S denote the function, $f_{e_1} \times f_{e_2} \times \ldots \times f_{e_n} : S^n \to S^n$. Π_G^S is called the *mapping associated with* G. $y \in S^n$ is called the *output from* G *corresponding to* $x \in S^n$ if $y = \Pi_G^S(x)$. In this case, x is called an *input to* G. □

Definition 3 (Size and depth of a comparator network) Let G be a comparator network. The size of G is the number of comparators belonging to G, and is denoted by size(G). The *depth* of G is the maximum length paths from input terminals of G to output terminals of G, and is denoted by depth(G) □

Definition 4 (A selector) Let k, n be integers with $1 \leq k \leq n-1$. Let S be a totally ordered set.

A *(n, k)-selector* is a comparator network with n registers and distinguished k output terminals such that, for every input in S^n, the elements appearing on the distinguished output terminals are all smaller than or equal to each elements appearing on the output terminals not distinguished. □

Definition 5 (A sorting network) Let S be a totally ordered set. A *sorting network* with n registers is a comparator network such that, for every input in S^n, the output $y = (y_1, y_2, \ldots, y_n)$ corresponding to the input satisfies the condition $y_1 \leq y_2 \leq \ldots \leq y_n$. □

Note that for every $1 \leq k \leq n-1$ a sorting network with n registers is also an (n, k)-selector.

The largest $n-k$ elements in the n input elements of an (n, k)-selector, appear on the $n-k$ output terminals other than the distinguished ones. It is easy to see that an (n,k)-selector becomes an $(n,n-k)$-selector by letting the output terminals not distinguished be distinguished, letting the output terminals distinguished be not distinguished and interchanging the labels, MAX and MIN, on the pair of edges incident out of each comparator. So without loss of generality, we can assume that $k \leq \lfloor n/2 \rfloor$.

Notation 3 Let $G = (A, B, E)$ be a bipartite graph and X be a subset of A. $\Gamma_G(X)$ denotes the subset of B,

$$\{y \in B \mid \exists x \in X((x, y) \in E)\} .$$

□

Definition 6 (An expander) Let $0 < \alpha \leq 1$ and $\beta \geq 1$. Let $G = (A, B, E)$ be a bipartite graph with left vertices A, right vertices B and edges E. G is an *(α, β)-expander* if every subset $X \subseteq A$ with $|X| \leq \alpha|A|$ satisfies $|\Gamma_G(X)| \geq \beta|X|$. □

To construct selectors, we utilize linear size expanders G such that the degree of each vertex of G is at most a constant.

Pinsker[Pin73] first proved the existence of linear size expanders. There are several results to improve that of [Pin73]. In this paper, we employ one of these results due to Bassalygo[Bas81]. We note here that, in contrast with these existence results, Margulis[Mar73] first gave an explicit construction of linear size comparators. After that, several explicit constructions are also given in literature.

3 Properties of comparator networks

The following Lemma 1 and Lemma 2 can be proved by induction on the size of comparator network G.

Lemma 1 *Let S be a totally ordered set and $f : S \to \{0,1\}$ be a function such that for all $i, j \in S$ with $i \leq j$, $f(i) \leq f(j)$. Let G be a comparator network. Then for all $x \in S^n$,*

$$\Pi_G^{\{0,1\}}(f^{\times n}(x)) = f^{\times n}(\Pi_G^S(x))$$

Lemma 2 (Monotonicity) *Let G be a comparator network with n registers and S a totally ordered set. Let $P = (p_1, p_2, \ldots, p_n) \in S^n$, $Q = (q_1, q_2, \ldots, q_n) \in S^n$, $U = (u_1, u_2, \ldots, u_n) \in S^n$, $V = (v_1, v_2, \ldots, v_n) \in S^n$. Assume that*

$$\Pi_G^S(P) = Q$$

and

$$\Pi_G^S(U) = V .$$

If $u_1 \geq p_1, u_2 \geq p_2, \ldots u_n \geq p_n$ then $v_1 \geq q_1, v_2 \geq q_2, \ldots v_n \geq q_n$.

Notation 4 For $x \in \{0,1\}^n$, $\#x$ denotes the number of entries of x equal to 1. □

Proposition 3 can be proved by Lemma 1 and Lemma 2. For a set N and a set K, $N \setminus K$ denotes the complement of K with respect to N.

Proposition 3 *A comparator network G with n registers and distinguished k output terminals is an (n, k)-selector if G satisfies the following conditions:*

Let N denote the set of all the output terminals of G and K the set of the k distinguished output terminals of G. Let $x \in \{0,1\}^n$ be such that $\#x = n - k$. If x is an input to G then the elements appearing on K are all 0 and the elements appearing on $N \setminus K$ are all 1.

Proposition 3 justifies our assumption employed in what follows that the totally ordered set S is taken to be set $\{0,1\}$.

4 Comparator subnetworks obtained from expanders

$(n,n/2)$-selectors given in this paper are composed of several kinds of modules. Construction and

function of those modules are explained in this section.

Definition 7 (A compressor) Let n, m be positive integers and let α, β be real numbers with $0 < \alpha < 1$ and $\beta > 1$. We shall define two types of comparator networks with $n+m$ registers. Let $x = (x_1, x_2, \ldots, x_{n+m})$ be an input to such a comparator network, and $y = (y_1, y_2, \ldots, y_{n+m})$ denote the output corresponding to x.

An *(n, m, α, β)-compressor of type 1* is a comparator network with $n+m$ registers satisfying that if $x \in \{0,1\}^{n+m}$ and $\#x \leq \lfloor \alpha n \rfloor + \lceil \beta \lfloor \alpha n \rfloor \rceil$ then $\beta \cdot \#(y_1, y_2, \ldots, y_n) \leq \#(y_{n+1}, y_{n+2}, \ldots, y_{n+m})$. The registers $1, 2, \ldots, n$ are called *upper registers* and the registers $n+1, n+2, \ldots, n+m$ are called *lower registers.*

An (n, m, α, β)-compressor of type 0 is a comparator network with $n+m$ registers satisfying that if $x \in \{0,1\}^{n+m}$ and $(m - \#x) \leq \lfloor \alpha m \rfloor + \lceil \beta \lfloor \alpha m \rfloor \rceil$ then $\beta(m - \#(y_{n+1}, y_{n+2}, \ldots, y_{n+m})) \leq n - \#(y_1, y_2, \ldots, y_n)$. The registers $1, 2, \ldots, m$ are called *upper registers* and the registers $m+1, m+2, \ldots, n+m$ are called *lower registers.* □

It is easy to see that an (n, m, α, β)-compressor of type 1 becomes an (m, n, α, β)-compressor of type 0 by interchanging register 1 and register $n+m$, register 2 and register $n+m-1$, ... and interchanging the labels, MAX and MIN, on the pair of edges incident out of each comparator.

Proposition 4 ([AKS83a][AKS83b]) *Let G be an (α, β)-expander with n left vertices and m right vertices. Let N be a comparator network with $n+m$ registers. N is a (n, m, α, β)-compressor if N satisfies the following two conditions:*

1. *If there is a comparator of N which is an intersecting vertex of two registers i and j with $i < j$, then $i \in \{1, 2, \ldots, n\}$, $j \in \{n+1, n+2, \ldots, n+m\}$, the edge on i incident out of the comparator is labeled MIN and the edge on j incident out of the comparator is labeled MAX.*
2. *If there is an edge of G incident from the i-th left vertex to the j-th right vertex then there is a comparator of N which is an intersecting vertex of register i and register $n+j$.*

Proposition 5 *Assume that there exists an (α, β)-expander with n left vertices and m right vertices. Let s and k denote the number of edges and the maximum degree of a vertex of the expander, respectively. Then there exists a (n, m, α, β)-compressor of type 1 such that its size is s and its depth is k.*

Proof: This proposition is obvious by the fact that a bipartite graph G with the maximum degree k can be coloured with just k colours so that no two adjacent edges have the same colour. □

The following Lemma 6 and Lemma 7 are obtained directly from the results of Bassalygo[Bas81].

Lemma 6 ([Bas81]) *There exists an integer $n_0 > 0$ such that for every $n \geq n_0$, there exists a $(10^{-5}, 6)$-expander with n left vertices and n right vertices such that its maximum degree of a vertex is at most 8.*

Lemma 7 ([Bas81]) *Let μ and η be real numbers with $0 < \mu < 1$ and $7/8 \leq \eta < 1$. There exist positive integers m_0 and s such that for every $m \geq m_0$, there exists a $\left(\mu, \left\lfloor \frac{1}{\mu}\left(\frac{2\eta}{1-\eta} - 1\right)\right\rfloor\right)$-expander with m left vertices and $\left\lfloor \frac{2\eta}{1-\eta} \right\rfloor m$ right vertices such that its maximum degree of a vertex is at most $s\left\lfloor \frac{2\eta}{1-\eta} \right\rfloor$.*

Lemma 8 *Let n_0 be as in Lemma 6. For every $n \geq n_0$, there exists a $(10^{-10}, 18)$-expander with $2n$ left vertices and n right vertices such that the maximum degree of a vertex over its left vertices is at most 64 and the maximum degree of a vertex over its right vertices is at most 128.*

Proof: Let $G_1 = (A_1, B_1, E_1)$ and $G_2 = (A_2, B_2, E_2)$ be $(10^{-5}, 6)$-expanders with n left vertices and n right vertices such that the maximum degree of a vertex of G_1 and the maximum degree of a vertex of G_2 are both at most 8. Let $G_3 = (V, E)$ denote the graph by identifying the i-th right vertex of G_1 with the i-th left vertex of G_2 for each $i \in \{1, 2, \ldots, n\}$. We can devide V, the set of vertices of G_3, into three subsets V_1 originating in A_1, V_2 originating in B_1 or A_2 and V_3 originating in B_2. Identify V_1 with A_1 and V_3 with B_2.

Let $H = (A, B, F)$ denote the bipartite graph such that

$$F = \{(a, b) \in A \times B \mid \text{There exists a path of length 2 from } a \text{ to } b \text{ on } G_3.\}$$

Then, it is obvious that $|A| = |B| = n$, the degree of each vertex in $A \cup B$ is at most $8^2 = 64$ and that H is a $(10^{-10}, 36)$-expander.

Next, we construct a bipartite graph G with $2n$ left vertices and n right vertices as follows. Let

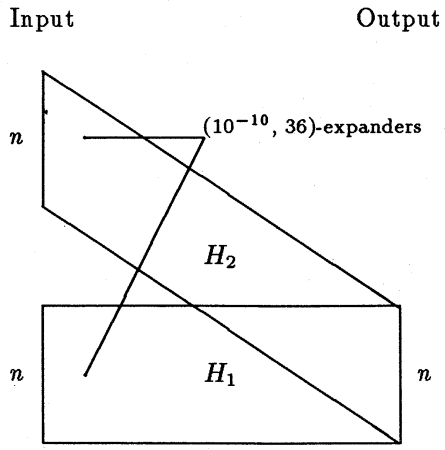

Figure 2: Construction of a $(10^{-10}, 18)$-expander

H_1 and H_2 be $(10^{-10}, 36)$-expanders isomorphic to H. G is constructed by identifying the i-th right vertex of H_1 with the i-th right vertex of H_2 for each $i = 1, 2, \ldots, n$ as shown in Figure 2. Thus, the degree of each left vertex of G is at most 64 and the degree of each right vertex of G is at most 128. Moreover, it is easy to show that G is a $(10^{-10}, 18)$-expander. □

The following Lemma 9 is deduced from Lemma 6 and Lemma 8.

Lemma 9 *For every $\varepsilon > 0$, there exist positive integers n_1, k_0 and a real number α_0 with $0 < \alpha_0 < 1$ such that for every integer $n \geq n_1$, there exists an $(\alpha_0, 6)$-expander with n left vertices, at most $(1 - (\varepsilon/28))n - 4$ right vertices and at most $8(1+\varepsilon)n$ edges such that the degree of each vertex of the expander is at most k_0.*

Proof: Note that we can assume that $\varepsilon < 1$ to prove the lemma. For $\varepsilon > 0$, we determin α_0, n_1 and k_0 as follows:

$$n_1 = \max\{\left\lceil \frac{140}{\varepsilon} \right\rceil, \left\lceil \frac{14}{\varepsilon}(n_0 + 1) \right\rceil\},$$

$$\alpha_0 = \frac{27}{70} \cdot 10^{-10}\varepsilon$$

and

$$k_0 = 128\,.$$

For every $n \geq n_1$, we construct the bipartite graph G as shown in Figure 3. The bipartite graph A and B in the figure are the $(10^{-10}, 18)$-expander stated in Lemma 8 and the $(10^{-5}, 6)$-expander

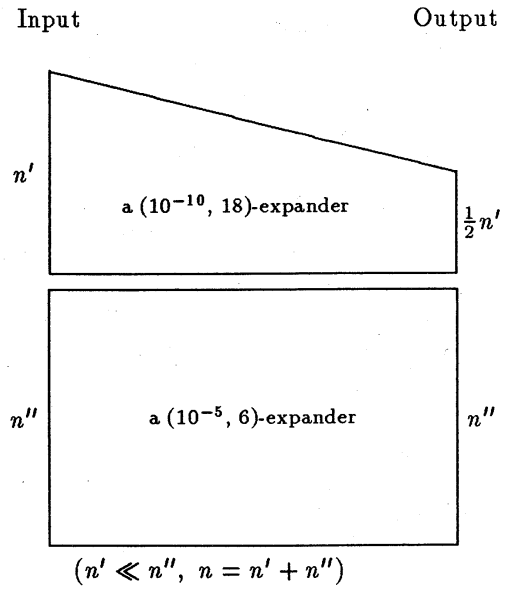

Figure 3: Construction of an $(\alpha_0, 6)$-expander

stated in Lemma 6, respectively. The number of the left vertices of A is $n' = 2\lfloor(\varepsilon/14)n\rfloor$ and the number of the right vertices of A is $n'/2$. n'' denotes the number of left vertices of B, namely, $n'' = n - n'$. It is not hard to see that the bipartite graph, G, is an $(\alpha_0, 6)$-expander satisfying the condition of Lemma 9. □

From Proposition 4, Proposition 5 and Lemma 9, the following Lemma 10 is proved immediately.

Lemma 10 *For every $\varepsilon > 0$, there exist positive integers n_1, k_0 and a real number α_0 with $0 < \alpha_0 < 1$ such that for every integers n and m with $n \geq n_1$ and $(1 - \frac{\varepsilon}{28})n - 4 \leq m \leq n$ there exist an $(n, m, \alpha_0, 6)$-compressor of type 1 and an $(m, n, \alpha_0, 6)$-compressor of type 0 such that those depths are both at most k_0 and those sizes are both at most $8(1+\varepsilon)n$.*

The following Lemma 11 contributes to utilizing compressors in order to construct $(n, n/2)$-selectors.

Lemma 11 *Let X be a comparator network with n registers. Let $x = (x_1, x_2, \ldots, x_n)$ be an input to X and $y = (y_1, y_2, \ldots, y_n)$ denote the output from X corresponding to the input x. Assume that $x \in \{0,1\}^n$ and, therefore, $y \in \{0,1\}^n$. Let i, j and k be integers with $1 \leq i < j < k \leq n+1$.*

Assume that there is no comparator in intersecting vertices of any register in $\{1, 2, \ldots, i-1\}$ and any register in $\{i, i+1, \ldots, n\}$ and there is

no comparator in intersecting vertices of any register in $\{1, 2, \ldots, k-1\}$ *and any register in* $\{k, k+1, \ldots, n\}$. *(Note that this assumption implies that*

$$\#(x_1, x_2, \ldots, x_{i-1}) = \#(y_1, y_2, \ldots, y_{i-1}) ,$$

$$\#(x_i, x_{i+1}, \ldots, x_{k-1}) = \#(y_i, y_{i+1}, \ldots, y_{k-1}) \text{ and}$$

$$\#(x_k, x_{k+1}, \ldots, x_n) = \#(y_k, y_{k+1}, \ldots, y_n) .)$$

Assume that there exist constants $a > 0$ *and* $0 \leq c \leq 1$ *such that, for every* $x \in \{0,1\}^n$, *if*

$$\#(x_i, x_{i+1}, \ldots, x_{k-1}) \leq a$$

then

$$\#(y_i, y_{i+1}, \ldots, y_{j-1}) \leq c\#(x_i, x_{i+1}, \ldots, x_{k-1}) . \quad (1)$$

Let $u > 0$ *and* $v \geq u$ *be real numbers with* $\lfloor v \rfloor - \lfloor u \rfloor \leq a$. *Then,* $\#(y_1, y_2, \ldots, y_{j-1}) \leq u + c(v-u)$ *if* $\#(x_1, x_2, \ldots, x_{i-1}) \leq u$ *and* $\#(x_1, x_2, \ldots, x_{k-1}) \leq v$.

Proof: Let $w = \#(y_i, y_{i+1}, \ldots, y_{k-1})$. Let $\Delta u = u - \lfloor u \rfloor$ and $\Delta v = v - \lfloor v \rfloor$. Two cases must be considered.

Case 1: $w \geq \lfloor v \rfloor - \lfloor u \rfloor$.

Since $\#(x_1, x_2, \ldots, x_{k-1}) \leq v$ and $\#(x_1, x_2, \ldots, x_{k-1})$ is an integer,

$$\begin{aligned} \#(x_1, x_2, \ldots, x_{i-1}) &= \#(x_1, x_2, \ldots, x_{k-1}) - w \\ &\leq \lfloor v \rfloor - w . \end{aligned}$$

From Lemma 2 and assumption (1), we have

$$\#(y_j, y_{j+1}, \ldots, y_{k-1}) \geq (1-c)(\lfloor v \rfloor - \lfloor u \rfloor) ,$$

which implies

$$\#(y_i, y_{i+1}, \ldots, y_{j-1}) \leq w - (1-c)(\lfloor v \rfloor - \lfloor u \rfloor) .$$

Thus,

$$\begin{aligned} &\#(y_1, y_2, \ldots, y_{j-1}) \\ &\leq (\lfloor v \rfloor - w) + w - (1-c)(\lfloor v \rfloor - \lfloor u \rfloor) \\ &= \lfloor u \rfloor + c(\lfloor v \rfloor - \lfloor u \rfloor) \\ &= u + c(v-u) - ((1-c)\Delta u + c\Delta v) . \end{aligned}$$

Case 2: $w < \lfloor v \rfloor - \lfloor u \rfloor$.

Since $\#(x_1, x_2, \ldots, x_{i-1}) \leq u$ and $\#(x_1, x_2, \ldots, x_{i-1})$ is an integer,

$$\#(x_1, x_2, \ldots, x_{i-1}) \leq \lfloor u \rfloor .$$

On the other hand, by assumption (1), we have

$$\#(y_i, y_{i+1}, \ldots, y_{j-1}) \leq c(\lfloor v \rfloor - \lfloor u \rfloor) .$$

Therefore,

$$\begin{aligned} &\#(y_1, y_2, \ldots, y_{j-1}) \leq \lfloor u \rfloor + c(\lfloor v \rfloor - \lfloor u \rfloor) \\ &= u + c(v-u) - ((1-c)\Delta u + c\Delta v) . \end{aligned}$$

Now, $(1-c)\Delta u + c\Delta v \geq 0$ holds because $0 \leq c \leq 1$. Therefore, we conclude that

$$\#(y_1, y_2, \ldots, y_{j-1}) \leq u + c(v-u)$$

on either case. □

Definition 8 (An extractor) Let n, m be positive integers and let $0 < \mu < 1$. We shall define a class of comparator networks, called 'extractors', with $n + 2m$ registers. Let $x = (x_1, x_2, \ldots, x_{n+2m})$ be an input to an extractor and $y = (y_1, y_2, \ldots, y_{n+2m})$ denote the output corresponding to the input x.

An *(n, m, μ)-extractor* is a comparator network with $n+2m$ registers satisfying the following condition: Assume that $x \in \{0,1\}^{n+2m}$. Let $d_1 = \#x$, $d_0 = n + 2m - \#x$, $c_1 = \#(y_1, y_2, \ldots, y_m)$ and $c_0 = m - \#(y_{n+m+1}, y_{n+m+2}, \ldots, y_{n+2m})$. The condition is that

$$\text{if } d_1 \leq \frac{3}{4}n + m \text{ then } c_1 \leq \mu m$$

and

$$\text{if } d_0 \leq \frac{3}{4}n + m \text{ then } c_0 \leq \mu m .$$

Note that $d_1 \leq \frac{3}{4}n + m$ or $d_0 \leq \frac{3}{4}n + m$ must hold because $d_1 + d_0 = n + 2m$.

The registers $1, 2, \ldots, m$ of an (n, m, μ)-extractor are called *upper registers*. The registers $m+1, m+2, \ldots, n+m$ of the extractor are called *middle registers*. The registers $n+m+1, n+m+2, \ldots, n+2m$ of the extractor are called *lower registers*. □

The following Lemma 12 states another type of modules utilized to construct $(n, n/2)$-selectors.

Lemma 12 *For every* $7/8 \leq \eta < 1$ *and* $0 < \mu < 1$, *there exist positive integers* n_2, k_1 *and a positive real number* δ *such that for every integer* $n \geq n_2$ *and for every integer* m *with* $|\eta(n+2m) - n| \leq 5$ *there exist an* (n, m, μ)*-extractor of depth at most* k_1 *and size at most* $\delta(n+2m)$.

Proof: The proof is omitted due to lack of space. □

5 Construction of $(n,\ n/2)$-selectors

In this section, we show the procedure to construct $(n,\ n/2)$-selectors and its justification. For simplicity, we assume that n is even. First we define a comparator network called a layer.

Notation 5 Let n and j be positive integers. For each integer i, let

$$x_i = \lceil (n/2)(1-\eta^i) \rceil \quad \text{and} \quad y_i = (n+1) - x_i \ ,$$

where η is as in Lemma 12. □

In what follows, we take the parameters η, μ in Lemma 12 so that $\mu \leq \alpha_0/100$ and $\eta = 1-(\varepsilon/28)$, where parameter ε is as in Lemma 10.

Notation 6 Let $j_{\max}$ denote the integer,

$$\min\{i \in \boldsymbol{Z} \mid i \geq 1 \text{ and } x_i - x_{i-1} < \max\{n_1, n_2, 100/\mu\}\} \ ,$$

where n_1 is as in Lemma 10 and n_2 is as in Lemma 12. Then, the existence of a $(y_i - x_i - 1,\ x_i - x_{i-1},\ \mu)$-extractor is gurantee by Lemma 12 for $i = 1, 2, \ldots, j_{\max}$. The existence of an $(x_{i-1} - x_{i-2},\ x_i - x_{i-1},\ \alpha_0,\ 6)$-compressor of type 1 and a $(y_{i-1} - y_i,\ y_{i-2} - y_{i-1},\ \alpha_0,\ 6)$-compressor of type 0 is also guaranteed by Lemma 10 for $i = 2, 3, \ldots, j_{\max}$. Note that $y_i - x_i - 1 = n - 2x_i$, $y_{i-1} - y_i = x_i - x_{i-1}$ and $y_{i-2} - y_{i-1} = x_{i-1} - x_{i-2}$.

For conciseness, we abbreviate the $(n - 2x_i,\ x_i - x_{i-1},\ \mu)$-extractor, the $(x_{i-1} - x_{i-2},\ x_i - x_{i-1},\ \alpha_0,\ 6)$-compressor of type 1 and the $(x_i - x_{i-1},\ x_{i-1} - x_{i-2},\ \alpha_0,\ 6)$-compressor of type 0 to $\mathrm{E}(i)$, $\mathrm{C1}(i)$ and $\mathrm{C0}(i)$, respectively. □

Notation 7 For an positive integer $i \geq 1$, $X(i)$ denotes set $\{x_{i-1}+1, x_{i-1}+2, \ldots, x_i\}$ and $Y(i)$ denotes set $\{y_i, y_i+1, \ldots, y_{i-1}-1\}$. If $x_i - x_{i-1} = y_{i-1} - y_i$ then $X(i) = Y(i) = \emptyset$. □

Definition 9 For each $j = 1, 2, \ldots, j_{\max}$, we define the *layer* of *rank* j with n registers, denoted by $\mathrm{L}(j)$, as follows.

1. If $j_{\max} = 1$ then $\mathrm{L}(1)$ is a sorting network, for example, the one constructed by Batcher's odd-even merge. In the following part of this definition, we assume that $j_{\max} > 1$.
2. $\mathrm{L}(1)$ is $\mathrm{E}(1)$.
3. If $j < j_{\max}$ then $\mathrm{L}(j)$ is constructed from $\mathrm{E}(j)$, $\mathrm{C1}(j)$, $\mathrm{C1}(j-1)$, ..., $\mathrm{C1}(2)$, $\mathrm{C0}(j)$, $\mathrm{C0}(j-1)$, ..., $\mathrm{C0}(2)$ as follows.
   (a) Join the output terminals on the upper registers of $\mathrm{E}(j)$ to the input terminals on the lower registers of $\mathrm{C1}(j)$, the output terminals on the upper registers of $\mathrm{C1}(j)$ to the input terminals on the lower registers of $\mathrm{C1}(j-1)$, ... and the output terminals on the upper registers of $\mathrm{C1}(3)$ to the input terminals on the lower registers of $\mathrm{C1}(2)$ in any way.
   (b) join the output terminals on the lower registers of $\mathrm{E}(j)$ to the input terminals on the upper registers of $\mathrm{C0}(j)$, the output terminals on the lower registers of $\mathrm{C0}(j)$ to the input terminals on the upper registers of $\mathrm{C0}(j-1)$, ... and the output terminals on the lower registers of $\mathrm{C0}(3)$ to the input terminals on the upper registers of $\mathrm{C0}(2)$ in any way.
4. $\mathrm{L}(j_{\max})$ is the comparator network obtained by exchanging $\mathrm{E}(j_{\max}-1)$ in $\mathrm{L}(j_{\max}-1)$ for a sorting network with the same number of registers as $\mathrm{E}(j_{\max}-1)$.

□

Note: In this paper, to join an output terminal of a comparator network to an input terminal of another comparator network means to identify the two terminals and then replace the identified vertex and the two edges incident to it with one edge.

Now, we express a procedure to construct $(n,\ n/2)$-selectors. In the following procedure, boldfaced letters represent variables in the procedure in order to distinguish those variables from general variables. The meanings of the variables in the procedure are as follows:

1. $\mathbf{N}$ is a variable to which a comparator network with n registers is assigned. An $(n,\ n/2)$-selector is to be assigned to $\mathbf{N}$ when the procedure terminates.
2. In progress of the procedure, layers are joined to $\mathbf{N}$. $\mathbf{j}$ is a variable indicating the rank of the joined layer.
3. For each $i = 1, 2, \ldots, j$, $\mathbf{l}(i)$ is a variable assigned a positive number.

[Procedure 1]

1. (Initial setting)

   $$\mathbf{N} \leftarrow \mathrm{L}(1),\ \mathbf{j} \leftarrow 1,\ \mathbf{l}(1) \leftarrow 3\mu|X(1)|$$

   Note: The symbol $\leftarrow$ means assignment.

2. If $j_{\max} = 1$ then terminate the procedure.

3. join either L(**j**) or L(**j** + 1) to the comparator network assigned to **N**, say G, so that the i-th output terminal of G is joined to the i-th input terminal of the joined layer (either L(**j**) or L(**j** + 1)) for each $i = 1, 2, \ldots, n$.

   The joint of the layer is the left side in Figure 4.

   (a) If $\mathbf{j} < j_{\max}$ and $\mathbf{l}(\mathbf{j}) < 7\mu|X(\mathbf{j})|$ then

   join L(**j** + 1) to G,
   $\mathbf{l}(i) \leftarrow \frac{24}{49}\mathbf{l}(i)$ for each $i = 1, 2, \ldots, \mathbf{j}$,
   $\mathbf{l}(\mathbf{j}+1) \leftarrow \frac{7}{2}\mathbf{l}(\mathbf{j})$ and
   $\mathbf{j} \leftarrow \mathbf{j} + 1$.

   (b) Otherwise,

   join L(**j**) and
   $\mathbf{l}(i) \leftarrow \frac{24}{49}\mathbf{l}(i)$ for each $i = 1, 2, \ldots, \mathbf{j}$.

4. If there exists an integer i such that

$$2 \leq i \leq \mathbf{j} \text{ and } \sum_{k=1}^{i} \mathbf{l}(k) < 1$$

   then let

$$i_{\max} = \max\{i \in \boldsymbol{Z} \mid \sum_{k=1}^{i} \mathbf{l}(k) < 1\}$$

   and remove the comparator networks C1(2), ..., C1($i_{\max}$) and C0(2), ..., C0($i_{\max}$) from the layer L(**j**) joined in step 3

5. If $\mathbf{j} = j_{\max}$ and $\sum_{k=1}^{\mathbf{j}} \mathbf{l}(k) < 1$ then terminate the procedure.

6. Go to the step 3.

□

Procedure 1 progresses as step 1 → step 2, first. Next, if the execution does not terminate at step 2 then the loop, step 3 → step 4 → step 5 → step 6 → step 3, is executed 0 or more times, step 3 → step 4 is executed and the execution terminates at step 5, at last.

If the execution of Procedure 1 terminates at step 2 then the value of **N** at the termination is a n-sortor, namely an $(n, n/2)$-selector. In what follows, therefore, we assume that the execution of Procedure 1 terminates at step 5, namely $j_{\max} > 1$.

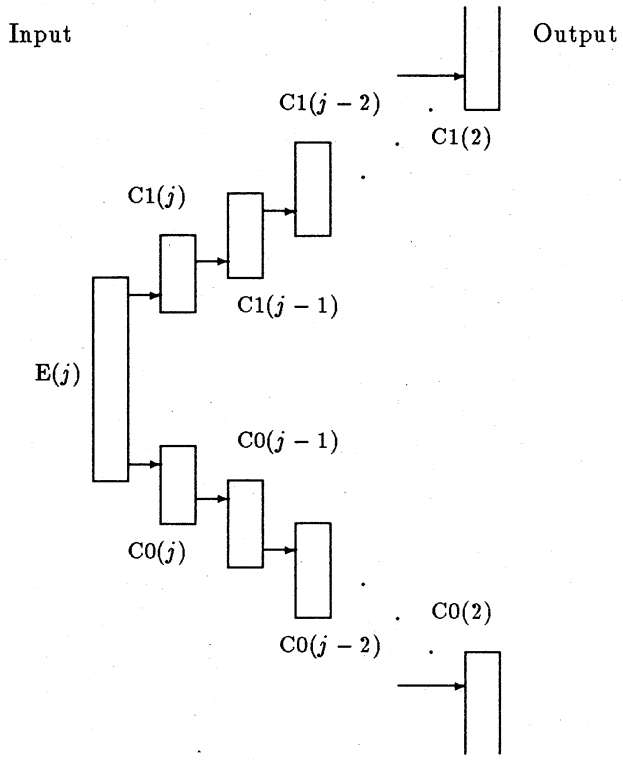

Figure 4: The structure of the layer L(j)

Variable **j**, **l**(i) are modified only in step 3 except step 1. And variable **N** is modified only in step 3 and step 4 except step 1.

Now, We shall define some notations in order to make proof of simple.

For any variable **v** in Procedure 1, $i \in \{3, 4\}$ and non-negative integer j, $V[\mathbf{v}|i, j]$ denotes the value of **v** just after step i has been executed j times if $j > 0$ and . $V[\mathbf{v}|i, 0]$ denotes the value of **v** just before the first execution of step i. For positive integer j, $A(j)$ is defined as follows: If step 3 is executed less than j times then $A(j) = 0$. If step 3a is executed in the j-th execution of step 3 then $A(j) = 1$. Otherwise, $A(j) = 0$.

We shall prove that the comparator network obtained by executing Procedure 1, denoted by $N(n)$, is a $(n, n/2)$-selector. $k_{\max}(n)$ denotes the number of times step 4 is executed in the execution of Procedure 1. Therefore, step 3 is also executed $k_{\max}(n)$ times. We abbreviate $k_{\max}(n)$ to $k_{\max}$ when n is obvious. Thus, $N(n) = V[\mathbf{N}|4, k_{\max}(n)]$. Let $i \in \{3, 4\}$ and $j \in \{0, 1, \ldots, k_{\max}(n)\}$. Let s and t be positive integers with $1 \leq s \leq t \leq n$. Then, letting f denote the function, $\Pi^{\{0,1\}}_{V[\mathbf{N}|i,j]} : \{0,1\}^n \to \{0,1\}^n$, we can decompose f as

$$f = f_1 \times f_2 \times \ldots \times f_n .$$

$N(i,j;s,t)$ denotes the function,

$$f_s \times f_{s+1} \times \ldots \times f_t : \{0,1\}^n \longrightarrow \{0,1\}^{t-s+1} .$$

Let k be a positive integer and $u \in \{0,1\}^n$. $\nu_1(i,j,k;u)$ and $\nu_0(i,j,k;u)$ denotes the integers,

$$\#(N(i,j;1,x_k)(u)),\ x_k - \#(N(i,j;y_k,n)(u)) ,$$

respectively. For an integer k with $0 \leq k \leq k_{\max}(n)$, $\xi(k)$ denotes the integer, $V[\mathbf{j}|3,k] = V[\mathbf{j}|4,k]$. For an integer k with $0 \leq k \leq k_{\max}(n)$ and an integer i with $1 \leq i \leq \xi(k)$, $\lambda(i,k)$ denotes the real number, $V[\mathbf{l}(i)|3,k] = V[\mathbf{l}(i)|4,k]$.

Observing Procedure 1, the following lemma is obvious.

Lemma 13 *Let k be an integer with $0 \leq k \leq k_{\max}$. For each $h = 1,2,\ldots\xi(k)$,*

$$\lambda(h,k) = \frac{49}{24}\lambda(h,k+1) .$$

For each $h = 1,2,\ldots\xi(k)-1$,

$$\lambda(h,k) = \frac{2}{7}\lambda(h+1,k) .$$

Lemma 14 *Let k be an integer with $1 \leq k \leq k_{\max}$. Then*

$$\lambda(\xi(k)-1,k-1) < 7\mu|X(\xi(k)-1)| \qquad (2)$$

and if $\xi(k) < j_{\max}$ then

$$2\mu|X(\xi(k))| \leq \lambda(\xi(k),k) . \qquad (3)$$

Proof: First, we shall prove (2). Assume that $A(k) = 1$. Observing Procedure 1, it is easy to see that For every $j = 1,2,\ldots,k_{\max}$, if $A(j) = 1$ then

$$\lambda(\xi(j-1),j-1) < 7\mu|X(\xi(j-1))| \qquad (4)$$

and

$$\xi(j) = \xi(j-1)+1 . \qquad (5)$$

Therefore, by Lemma 13, (4) and (5),

$$\lambda(\xi(k)-1,k-1) < 7\mu|X(\xi(k)-1)|$$

holds.

Next, assume that $A(k) = 0$. For every $j = 1,2,\ldots,k_{\max}$, if $A(j) = 0$ then the following expressions hold: If $\xi(j-1) < j_{\max}$ then

$$\lambda(\xi(j-1),j-1) \geq 7\mu|X(\xi(j-1))| \qquad (6)$$

and

$$\xi(j) = \xi(j-1) . \qquad (7)$$

Since $A(1) = 1$, there is a positive integer $k_0 < j$ such that $A(k_0) = 1$ and $A(k_0+1) = A(k_0+2) = \ldots A(k) = 0$. Therefore, by Lemma 13, (4), (5) and (7),

$$\begin{aligned} \lambda(\xi(k),k) &< \lambda(\xi(k_0),k_0) \\ &< 12\mu|X(\xi(k_0-1))| \\ &= 12\mu|X(\xi(k)-1)| \end{aligned}$$

On the other hand, by Lemma 13,

$$\lambda(\xi(k)-1,k-1) = \frac{7}{12}\lambda(\xi(k),k)$$

holds. Thus, we have (2).

Next, we shall prove (3). We assume that $\xi(k) < j_{\max}$. If $A(k) = 0$ then (3) obviously holds. If $A(k) = 1$ then either of the following two cases holds:

1. There exists a positive integer $k_0 < k$ such that $A(k_0) = 0$ and $A(k_0+1) = A(k_0+2) = \ldots = A(k) = 1$. In this case, by Lemma 13 and (6), we have

$$\begin{aligned} \lambda(\xi(k),k) &> \lambda(\xi(k_0),k_0) \\ &\geq \frac{24}{7}\mu|X(\xi(k_0))| \\ &> 2\mu|X(\xi(k))| . \end{aligned}$$

2. $A(1) = A(2) = \ldots = A(k) = 1$. In this case, we have

$$\begin{aligned} \lambda(\xi(k),k) &> \lambda(\xi(0),0) \\ &> 2\mu|X(\xi(k))| . \end{aligned}$$

Thus, we conclude (3). □

Lemma 15 *Let k be an integer with $0 \leq k \leq k_{\max}(n)$. Let $u \in \{0,1\}^n$ be an input to N with $\#u = n/2$. Let $\tau_1(i,k)$ and $\tau_0(i,k)$ denote the integers, $\nu_1(4,k,i;u)$ and $\nu_0(4,k,i;u)$, respectively, for each $i = 1,2,\ldots,\xi(k)$. Then, for each $i = 1,2,\ldots,\xi(k)$,*

$$\tau_1(i,k) \leq \sum_{h=1}^{i} \lambda(h,k) \qquad (8)$$

and

$$\tau_0(i,k) \leq \sum_{h=1}^{i} \lambda(h,k) \qquad (9)$$

hold.

Proof: We shall prove the lemma by induction on k. Observing the initial setting of Procedure 1, we have

$$\xi(k) = 1,\ \lambda(1,0) = 3\mu x_1 .$$

Since

$$\#u = \frac{n}{2} \le x_i + \frac{3}{4}(n - 2x_i)$$

and $\mathrm{L}(1) = \mathrm{E}(1)$ is an $(n - 2x_1,\ x_1,\ \mu)$-extractor, we also have

$$\tau_1(1,0) \le \mu x_1 < 3\mu x_1 = \lambda(1,0)$$

and

$$\tau_0(1,0) \le \mu x_1 < 3\mu x_1 = \lambda(1,0) .$$

Thus, if $k = 0$ then the inequalities (8) and (9) hold for $i = 1 = \xi(k)$.

Assume that $0 \le k \le k_{\max} - 1$ and the inequalities, (8) and (9), hold for each $i = 1, 2, \ldots, \xi(k)$, by induction.

In the $(k+1)$-st execution of step 3, the layer, $\mathrm{L}(\xi(k+1))$ is joined to the comparator network, $V[\mathbf{N}|4,k]$.

From the assumption of induction and $\#u = n/2$,

$$\begin{aligned} &\frac{n}{2} - (x_{\xi(k+1)-1} - \tau_0(\xi(k+1)-1,k)) \\ &\quad \le \frac{1}{2}(n - 2x_{\xi(k+1)-1}) + \sum_{h=1}^{\xi(k+1)-1} \lambda(h,k) \end{aligned}$$

$$\tau_1(\xi(k+1)-1,k) \le \sum_{h=1}^{\xi(k+1)-1} \lambda(h,k) .$$

Therefore, we have

$$\begin{aligned} &\left\lfloor \frac{1}{2}(n - 2x_{\xi(k+1)-1}) + \sum_{h=1}^{\xi(k+1)-1} \lambda(h,k) \right\rfloor \\ &\qquad - \left\lfloor \sum_{h=1}^{\xi(k+1)-1} \lambda(h,k) \right\rfloor \\ &\le \left\lceil \frac{1}{2}(n - 2x_{\xi(k+1)-1}) \right\rceil = \frac{1}{2}(n - 2x_{\xi(k+1)-1}) . \end{aligned}$$

Therefore, if $\xi(k+1) < j_{\max}$ then, by applying Lemma 11 to $\mathrm{E}(\xi(k+1))$ and using Lemma 14 and Lemma 13, we have

$$\begin{aligned} &\nu_1(3, k+1, \xi(k+1); u) \\ &\quad \le \mu|X(\xi(k+1))| + \tau_1(\xi(k+1)-1,k) \\ &\quad \le \mu|X(\xi(k+1))| + \sum_{h=1}^{\xi(k+1)-1} \lambda(h,k) \\ &\quad \le \frac{7}{12}\lambda(\xi(k+1),k+1) \\ &\qquad + \frac{49}{24}\sum_{h=1}^{\xi(k+1)-1} \lambda(h,k+1) . \end{aligned}$$

If $\xi(k+1) = j_{\max}$ then, observing the structure of $\mathrm{L}(j_{\max})$, we also have

$$\begin{aligned} &\nu_1(3, k+1, \xi(k+1); u) \\ &\quad = \nu_1(3, k+1, \xi(k+1)-1; u) \\ &\quad = \tau_1(\xi(k+1)-2, k) \\ &\quad \le \frac{7}{12}\lambda(\xi(k+1),k+1) \\ &\qquad + \frac{49}{24}\sum_{h=1}^{\xi(k+1)-1} \lambda(h,k+1) . \end{aligned}$$

Since, by Lemma 14 and Lemma 13,

$$\begin{aligned} &\left\lfloor \frac{7}{12}\lambda(i+1,k+1) + \frac{49}{24}\sum_{h=1}^{i} \lambda(h,k+1) \right\rfloor \\ &\qquad - \left\lfloor \frac{49}{24}\sum_{h=1}^{i-1} \lambda(h,k+1) \right\rfloor \\ &\quad \le \frac{7}{6}\lambda(i+1,k+1) + 1 \\ &\quad \le 15\mu|X(i)| \\ &\quad \le 7\lfloor \alpha_0|X(i)| \rfloor \end{aligned}$$

and

$$\begin{aligned} &\frac{1}{7}\left(\frac{7}{12}\lambda(i+1,k+1) + \frac{49}{24}\lambda(i,k+1)\right) \\ &\quad + \frac{49}{24}\sum_{h=1}^{i-1} \lambda(h,k+1) \\ &\quad = \frac{7}{12}\lambda(i,k+1) + \frac{49}{24}\sum_{h=1}^{i-1} \lambda(h,k+1) \end{aligned}$$

hold for each $i = 1, 2, \ldots, \xi(k+1)-1$, by applying Lemma 11 to $\mathrm{C1}(\xi(k+1))$ (if $\xi(k+1) < j_{\max}$), $\mathrm{C1}(\xi(k+1)-1)$, ... and $\mathrm{C1}(2)$, we have

$$\nu_1(3, k+1, i; u) \le \frac{7}{12}\lambda(i,k+1) + \frac{49}{24}\sum_{h=1}^{i-1} \lambda(h,k+1)$$

for each $i = 1, 2, \ldots, \xi(k+1)$. Note that, by the definition of $j_{\max}$,

$$\mu|X(i)| > 1$$

holds for each $i = 1, 2, \ldots, j_{\max} - 1$ and $\sum_{i=j}^{k} x_i = 0$ if $k < j$.

By using Lemma 13, we can obtain

$$\frac{7}{12}\lambda(i,k+1)+\frac{49}{24}\sum_{h=1}^{i-1}\lambda(h,k+1)$$
$$= \lambda(i,k+1)\left(\frac{7}{5}-\frac{1}{15}\left(\frac{2}{7}\right)^{i-3}\right).$$

On the other hand,

$$\sum_{h=1}^{i}\lambda(h,k+1)=\lambda(i,k+1)\left(\frac{7}{5}-\frac{8}{245}\left(\frac{2}{7}\right)^{i-3}\right).$$

Hence,

$$\nu_1(3,k+1,i;u)\le\sum_{h=1}^{i}\lambda(h,k+1)$$

for each $i=1,2,\ldots,\xi(k+1)$. In a similar way, we also have

$$\nu_0(3,k+1,i;u)\le\sum_{h=1}^{i}\lambda(h,k+1)$$

for each $i=1,2,\ldots,\xi(k+1)$.

If no compressors are removed from the joined layer in the $(k+1)$-st execution of step 4, it is obvious that

$$\tau_1(i,K+1)=\nu_1(3,k+1,i;u)$$

and

$$\tau_0(i,K+1)=\nu_0(3,k+1,i;u)$$

for each $i=1,2,\ldots,\xi(k+1)$. Otherwise, by the assumption of induction,

$$\tau_1(i_{\max},k)\le\sum_{h=1}^{i_{\max}}\lambda(h,k)<1\ .$$

Since $\tau_1(i_{\max},k)\ge 0$ and $\tau_1(i_{\max},k)\in \boldsymbol{Z}$, $\tau_1(i_{\max},k)=0$. In a similar way, $\tau_0(i_{\max},k)=0$. This shows that only 0's move through C1(2), C1(3), ..., C1($i_{\max}$) and only 1's move through C0(2), C0(3), ..., C0($i_{\max}$) in the joined layer. Thus, removed compressors above do not work at all. Therefore, in any case,

$$\tau_1(i,K+1)=\nu_1(3,k+1,i;u)$$

and

$$\tau_0(i,K+1)=\nu_0(3,k+1,i;u)$$

for each $i=1,2,\ldots,\xi(k+1)$. □

Lemma 16 *For every even integer $n>0$, $N(n)$ is a $(n, n/2)$-selector.*

Proof: The proof is obvious by Lemma 15 and the structure of L($j_{\max}$). □

Lemma 17 $\mathrm{depth}(N(n))=O(\log n)$.

Proof: By Lemma 13, we have

$$\sum_{h=1}^{\xi(k)}\lambda(h,k) = \lambda(1,0)\left(\frac{24}{49}\right)^{k}\sum_{h=1}^{\xi(k)}\left(\frac{7}{2}\right)^{h-1}$$
$$< 2^{2\log_2 n+2j_{\max}-k}\ .$$

Since, by the definition of $j_{\max}$, $n\eta^{j_{\max}}\ge 1$,

$$j_{\max}\le-\frac{1}{\log_2\eta}\log_2 n\ .$$

Therefore, $\sum_{h=1}^{\xi(k)}\lambda(h,k)<1$ holds if

$$k\ge 2\left(1-\frac{1}{\log_2\eta}\right)\log_2 n\ .$$

On the other hand, by Lemma 14, $\xi(k)=j_{\max}$ holds if

$$\lambda(\xi(k),k)<1\le 2\mu|X(\xi(k))|\ .$$

Therefore, we conclude that

$$k_{\max}(n)\le\left\lfloor 2\left(1-\frac{1}{\log_2\eta}\right)\log_2 n\right\rfloor=O(\log n)\ .$$

□

Lemma 18 *There exists a positive integer n_3 such that, for every even integer $n\ge n_3$,* $\mathrm{size}(N(n))\le 8n\log_2 n$.

Proof: For a positive integer k, let $s_1(k)$ the total size of the compressors contained by the layer, L($\xi(k)$), let $s_2(k)$ and $s_3(k)$ denote the sizes of the extractor and the sorting network contained by the layer, L($\xi(k)$), respectively. We also define $s_1(0)$, $s_2(0)$ and $s_3(0)$ as $s_1(0)=s_3(0)=0$ and $s_2(0)=$ size(E(1)). Thus,

$$\mathrm{size}(N(n))=\sum_{k=0}^{k_{\max}}(s_1(k)+s_2(k)+s_3(k))\ .$$

From Lemma 17 and the definition of $j_{\max}$, it is easy to see that $\sum_{k=0}^{k_{\max}}s_3(k)=O(\log n)$.

If $\xi(k)\le j_{\max}$ then $A(k-2)=A(k-1)=A(k)=0$ does not hold, for the following reason. Let k be an positive integer with $\xi(k)\le j_{\max}$. Assume that $A(k)=A(k+1)=0$. Since $\xi(k-1)=$

$\xi(k+1)$, by using Lemma 14 and Lemma 13, we have

$$\lambda(\xi(k+1), k+1) \leq \frac{288}{49}|X(\xi(k+1)-1)| .$$

On the other hand, by the definition of $j_{\max}$, we have

$$|X(\xi(k+1)-1)| \leq \frac{101}{99} \cdot \frac{8}{7}|X(\xi(k+1))| .$$

Thus, $\lambda(\xi(k+1), k+1) < 7\mu|X(\xi(k+1))|$ and $A(k) = 1$ hold. Moreover, by Lemma 11, we have $s_2(k) \leq \eta^{\xi(k)-1}\delta n$. Therefore, we have

$$\sum_{k=0}^{k_{\max}} s_2(k) \leq 3\delta \left(\sum_{i=1}^{j_{\max}} \eta^{i-1} \right) n = O(n) .$$

We already showed that $\sum_{k=0}^{k_{\max}}(s_2(k)+s_3(k)) = O(n)$ and hence it suffices to show that there exists a $f = O(n)$ such that $\sum_{k=0}^{k_{\max}(n)} s_1(k) \leq 8n\log_2 n + f(n)$. Let $k_0 = \lfloor \log_2 n / \log_2(49/24) \rfloor$. We have

$$\sum_{k=0}^{k_0} s_1(k) \leq \frac{8(1+\varepsilon)}{\log_2(49/24)} n\log_2 n + 16(1+\varepsilon)n .$$

Since $\log_2(49/24) > 1$ and we may take ε as arbitrarily small, it suffices to show that $\sum_{k=k_0+1}^{k_{\max}} s_1(k) = O(n)$. Since $\sum_{h=1}^{i} \lambda(h,k) < (7/5)\lambda(i,k)$ by Lemma 13, if $\lambda(i,k) \leq 5/7$ then the compressors, C1(i) and C0(i), are removed from the layer joined at the j-th execution of step 4 for each $j = k, k+1, \ldots, k_{\max}$. Since $\lambda(1,0) < n$, by Lemma 13 and the definition of k_0, we have $\lambda(1,k_0) \leq 1$. Therefore, we have the following inequality by estimating the total size of the compressors not removed.

$$\begin{aligned}
&\sum_{k=k_0+1}^{k_{\max}} \\
&\quad \leq 2\sum_{i=1}^{j_{\max}} 8(1+\varepsilon)|X(i)| \log_{\frac{49}{24}} \left(\frac{7}{5}\left(\frac{7}{2}\right)^{i-1} \right) \\
&\quad \leq 16(1+\varepsilon)\sum_{i=1}^{j_{\max}} (\log_2 4^i)|X(i)| \\
&\quad \leq 32(1+\varepsilon)\sum_{i=1}^{j_{\max}} i\left(\frac{n}{2}(1-\eta)\eta^{i-1}+1\right) .
\end{aligned}$$

Since $j_{\max} = O(\log n)$, we conclude that

$$\sum_{k=k_0+1}^{k_{\max}} s_1(k) = O(n) .$$

□

From Lemma 16, Lemma 17 and Lemma 18, the following main theorem is immediately obtained.

Theorem 1 *For every positive even integer n, $N(n)$ is an $(n, n/2)$-selector. There exists a positive integer n_3 such that, for every even integer $n \geq n_3$, $\mathrm{size}(N(n)) \leq 8n\log_2 n$. Moreover, $\mathrm{depth}(N(n)) = O(\log n)$.*

References

[AKS83a] M. Ajtai, J. Komlós, and E. Szemerédi. An $O(n\log n)$ sorting network. In *Proceedings of the 15th Annual ACM Symposium on Theory of Computing*, pages 1–9, 1983.

[AKS83b] M. Ajtai, J. Komlós, and E. Szemerédi. Sorting in $c\log n$ parallel steps. *Combinatorica*, 3 (1):1–19, 1983.

[Bas81] L. A. Bassalygo. Asymptotically optimal switching circuits. *Problemy Peredachi Informatsii*, 17:206–211, 1981. English translation in *Problems of Information Transmission.*

[Mar73] G. A. Margulis. Explicit constructions of concentrators. *Problemy Peredachi Informatsii*, 9 (4):71–80, 1973. English translation in *Problems of Information Transmission.*

[Pat] M. S. Paterson. Improved sorting networks with $O(\log n)$ depth. *Algorithmica*, to appear.

[Pin73] N. Pinsker. On the complexity of a concentrator. In *7th International Teletraffic Conference*, pages 318/1–318/4, Stockholm, June 1973.

[Pip90] N. Pippenger. Selection networks. In *SIGAL of IPSJ '90 Algorithms*, pages 2–11, Springer-Verlag, August 1990. (*Lecture Notes in Computer Science 450*).