Electronic Colloquium on Computational Complexity, Report No. 41 (2013)

On the complexity of parallel prefix circuits *

Igor S. Sergeev†

Abstract

It is shown that complexity of implementation of prefix sums of m variables (i.e. functions $x_1 \circ \ldots \circ x_i$, $1 \leq i \leq m$) by circuits of depth $\lceil \log_2 m \rceil$ in the case $m = 2^n$ is exactly

$$3.5 \cdot 2^n - (8.5 + 3.5(n \bmod 2))2^{\lfloor n/2 \rfloor} + n + 5.$$

As a consequence, for an arbitrary m an upper bound $(3.5 - o(1))m$ holds. In addition, an upper bound $\left(3\frac{3}{11} - o(1)\right) m$ for complexity of the minimal depth prefix circuit with respect to XOR operation is obtained. Some new bounds under different restrictions on the circuit depth are also established.

1 Introduction

Let $\circ$ be a binary associative operation over a set $\mathbf{G}$. A set of functions

$$x_1 \circ \ldots \circ x_i, \qquad 1 \leq i \leq m, \tag{1}$$

is a system of *prefixes* (or *prefix sums*) of an ordered set of variables $x_1, \ldots, x_m$ attaining values in $\mathbf{G}$. Circuits of functional elements which implement (1) over the basis $\{\circ\}$ are often called *prefix circuits*. The notions of circuit depth and complexity one can find in [4, 8].

Prefix circuits are exploited in various theoretic and applied problems of synthesis, e.g. in the problem of constructing of binary adders, sorting networks, in solving linear recurrences. These and other applications of prefix

*Research supported in part by RFBR, grants 11–01–00508, 11–01–00792, and DMS RAS "Algebraic and combinatorial methods of mathematical cybernetics and information systems of new generation" program (project "Problems of optimal synthesis of control systems").

†isserg@gmail.com, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Department of Discrete Mathematics

ISSN 1433-8092

circuits are highlighted in [1]. Some of these problems include synthesis of *parallel* prefix circuits, i.e. circuits of depth $O(\log_2 m)$.

If not stated otherwise, under a prefix circuit we will understand a "universal" prefix circuit. A circuit is *universal* if it computes all prefix sums over an arbitrary set $\mathbf{G}$ with an associative operation $\circ$. That is, such circuits cannot use any specific properties of elements of $\mathbf{G}$ or of the operation $\circ$ itself, besides its associativity. Universality will be important in the lower bound proofs.

Let $L(m)$ denote the complexity of (i.e. the number of gates in) a minimal universal m-input prefix circuit of depth $\lceil \log_2 m \rceil$.

Several simple constructions of prefix circuits of complexity $O(m \log m)$ were proposed in 1950–70's (see e.g. [14, 6]). In 1978 Ladner and Fischer [7] obtained a linear upper bound

$$L(m) \le (4 - o(1))m.$$

In the case $m = 2^n$ they proved a more accurate bound

$$L(2^n) \le 4 \cdot 2^n - \Phi_{n+5} + 1 = 4 \cdot 2^n - O(\varphi^n).$$

Here Φ_k is a k-th Fibonacci number[1], and $\varphi = (1+\sqrt{5})/2$ (the golden ratio).

Somewhat later, Fich [2, 3][2] proved the following lower and upper bounds:

$$\left(3\tfrac{1}{3} - o(1)\right) 2^n \le L(2^n) \le \left(3\tfrac{421}{792} - o(1)\right) 2^n.$$

In the present paper we improve these bounds to:

$$L(2^n) = 3.5 \cdot 2^n - (8.5 + 3.5(n \bmod 2))2^{\lfloor n/2 \rfloor} + n + 5, \qquad L(m) \le (3.5 - o(1))m.$$

A slight weakening of the restriction of minimality of the circuit depth allows to significantly reduce the complexity as well as some other important characteristics, e.g. the fan-out. However, there is a limit for complexity to decrease. The limit is determined by the well-known inequality

$$L + D \ge 2m - 2, \tag{2}$$

valid for any m-input prefix circuit of complexity L and depth D.[3] A circuit achieving a lower bound (2) is called *optimal* (or *zero-deficiency*) circuit.

[1] Fibonacci number Φ_k is a closest integer to $\varphi^k/\sqrt{5}$.

[2] The author didn't have an opportunity to get a look at [2], so further Fich results are cited following [3].

[3] Apparently, the inequality (2) was originally obtained by Fich [3] for a substantial particular case. The general formulation is due to Snir [15], however his proof is somewhat cumbersome.

Synthesis of optimal prefix circuits with various additional properties is a popular direction in circuit design.

It is not difficult to construct an optimal circuit of depth $2\lceil\log_2 m\rceil - 2$ (see e.g. [9]). The minimal possible depth for optimal prefix circuits is $\log_\varphi m - O(1)$. Such circuits were constructed in [16].[4]

Let us denote by $L(m,k)$ the minimal complexity of an m-input prefix circuit of depth $\lceil\log_2 m\rceil + k$. As mentioned above only case $k \le \log_\varphi m - \log_2 m - O(1)$ is nontrivial. In [7, 3] circuits were constructed, which satisfy additional condition of implementation of the longest prefix $x_1 \circ \ldots \circ x_m$ with the minimal possible depth $\lceil\log_2 m\rceil$. We denote by $L'(m,k)$ the minimal complexity of a prefix circuit of this sort. Clearly, $L(m,k) \le L'(m,k)$.

The following bounds are obtained in [7]:

$$L'(m,k) < (2+2^{1-k})m - 2, \qquad L'(2^n,k) \le (2+2^{1-k})2^n - \Phi_{n+5-k} - k + 1,$$

and the next are from [3]:

$$\left(2+\tfrac{1}{3}\cdot 2^{1-k} - o(1)\right)2^n \le L'(2^n,k) \le \left(2+\tfrac{421}{792}\cdot 2^{1-k} - o(1)\right)2^n - k.$$

We improve these bounds to

$$L'(2^n,k) = (2+2^{-k})2^n - (5+2((n-k) \bmod 2))2^{\lfloor (n-k)/2\rfloor} - k + 2,$$

$$L'(m,k) \le (2+2^{-k} - o(1))m.$$

The last inequality is valid when $1 \le k \le \lceil\log_2 m\rceil - 2$ and $m \to \infty$.

Another way to reduce complexity of a prefix circuit is a weakening of the universality condition. As an example, we consider "modulo 2" prefix circuits, that is, prefix circuits over basis $\{\oplus\}$, where $\oplus$ is an associative binary operation satisfying identity $x \oplus y \oplus y = x$ (particularly, XOR is an operation of such kind)[5]. We introduce analogous notation $L^{\oplus}(m)$ and $L'^{\oplus}(m,k)$ for the case of modulo 2 circuits.

It will be shown below that

$$L^{\oplus}(m) \le \left(3\tfrac{3}{11} - o(1)\right)m, \qquad L'^{\oplus}(m,k) \le \left(2+\tfrac{3}{11}\cdot 4^{1-k} - o(1)\right)m,$$

where $1 \le k \le \lceil(\log_2 m)/2\rceil - 1$ and $m \to \infty$.

Results of the article were reported at the seminar "Mathematical Problems of Cybernetics" (Moscow State University, March 27, 2009) and were published in a shortened form (without proofs) in [10, 11].

[4]To be exact, it is shown in [16], that an optimal m-input prefix circuit of depth d exists iff $m \le \Phi_{d+3} - 1$.

[5]A prefix circuit over $(GF(2), \oplus)$ implements a mapping from the Gray encoding to the ordinary binary encoding, see [5] for more details.

The paper is organized as follows. In §2 we introduce notions to describe the structure of a prefix circuit. In §3 and §4 we prove lower and upper bounds for $L(2^n)$ respectively. In §5 some corollaries for the complexity of prefix circuits of various depths are obtained. In §6 we establish an upper bound for $L^{\oplus}(2^n)$ and analogous corollaries. In §7 we collected some remarks on parallel prefix circuits with restriction on the fan-out of circuit gates.

2 Preliminary notions

Here we introduce some notions (generally taken from [3]) useful for analysis of the structure of a prefix circuit.

First notice that in a universal prefix circuit gates connected with outputs of the circuit via oriented paths compute functions of form $x_i \circ x_{i+1} \circ \ldots \circ x_j$.

Indeed, for otherwise it would exist a formula, implementing some prefix sum from (1) and such pair of variables x_j, x_k, where $j < k$, that symbol x_k in the formula precedes symbol x_j. We now show that such formula can not implement any prefix sum over a noncommutative group $(\mathbf{G}, \circ)$ with elements of infinite order (e.g. group of symmetries of circumference). Assign $x_j = a$, $x_k = b$ and $x_i = e$ for all $i \neq j, k$, where $a, b, e \in \mathbf{G}$ and e is the group unit. Prefix sum of these arguments attains value $a \circ b$ whereas the value of the formula is either $b \circ a$ or $a^{l_1} \circ b^{l_2} \circ a^{l_3} \circ \ldots$, where all $l_i \geq 0$ and $\sum_i l_i \geq 3$. In the first case, choose a and b so that $a \circ b \neq b \circ a$. In the second case, one of numbers $l_a = \sum l_{2i-1}$, $l_b = \sum l_{2i}$ is greater than 1. Assuming w.l.o.g. that $l_a > 1$, assign an element of infinite order to a and set $b = e$. As a consequence of $a^{l_a} \neq a$, values of the prefix sum and the formula do not match.

Therefore, we can restrict our attention to circuits with all gates implementing functions of the form $x_i \circ x_{i+1} \circ \ldots \circ x_j$.

If a function $x_i \circ \ldots \circ x_j$ is implemented at the output of a gate v, then we attribute *label* $\lambda(v) = [i; j]$ to v. An input x_i of a circuit is attributed with label $[i; i]$. Notation $l(v) = i$ and $r(v) = j$ stands for the left and right ends of the label respectively. Denote by $w(v) = r(v) - l(v) + 1$ a number of summands in a sum computed by v. It will be referred to as a *width* of v.

Let a gate v take input edges from v' and v''. Then for one of these gates (let us assume that for v') $l(v') = l(v)$ holds, and $r(v'') = r(v)$ holds for another one. Let us call v' the *left parent* and v'' the *right parent* of gate v. Evidently, $w(v) = w(v') + w(v'')$. Denote by $d(v)$ the depth of v in a circuit.

Let us classify gates of a prefix circuit S. We call subcircuit computing the longest prefix sum $x_1 \circ \ldots \circ x_m$ *skeleton* subcircuit. It is a tree containing $m - 1$ gates, among them at most $D + 1$ outputs of S, where D is the depth

of the skeleton subcircuit. We name *skeleton* gates such gates of the skeleton subcircuit which are not outputs of S. A gate of S which is neither skeleton nor output is called an *extra* gate.

It is straightforward that prefix circuits with no extra gates and with the depth of the longest prefix equal to the circuit depth constitute exactly the set of optimal circuits defined in the introduction. (This argument can be easily transformed into the proof of (2). Note that (2) remains valid if one replace D by the longest prefix depth.)

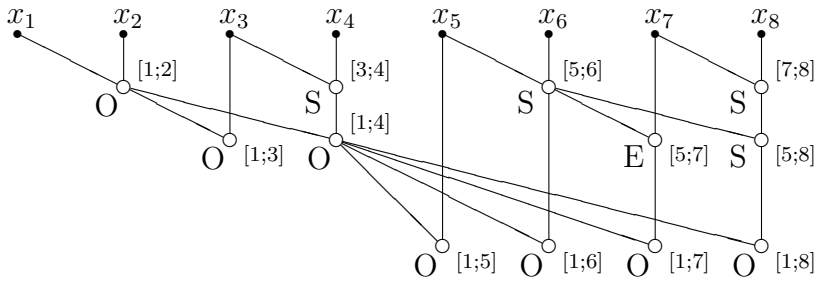


Fig. 1

Fig. 1 represents a 8-input prefix circuit (edges are oriented top-down). Output gates, skeleton gates and an extra gate are marked with symbols "O", "S", "E" respectively.

Skeleton subcircuit of a 2^n-input prefix circuit of depth n is defined uniquely. Gates of a skeleton subcircuit have labels $[i2^k+1;(i+1)2^k]$, where $i=0,\ldots,2^{n-k}-1$ and $k=1,\ldots,n$.

3 Lower bound

Initial idea of the structure of a minimal prefix circuit is given by the following lemma. Denote by $\mathbf{S}_r(m,d)$ a set of m-input prefix circuits of depth at most d whose outputs depending on at least $r+1$ circuit inputs have greater depth than an output implementing $x_1 \circ \ldots \circ x_r$.

Lemma 1 (Fich [3]). *Let S have minimal complexity among circuits from $\mathbf{S}_r(m,d)$. Then an output u^* of S which implements $x_1 \circ \ldots \circ x_r$ is connected via oriented path with any output depending on more than r circuit inputs.*

Proof. If the last condition is violated for some minimal circuit, then the circuit contains gates which are not outputs and depend on each of inputs x_r and x_{r+1}. Transform the circuit in the following way. Remove any such gate v and connect free ends of its outgoing edges to the right parent of v. Replace any edge (u'',u') satisfying $r(u'')<r(u^*)<r(u')$ by an edge (u,u').

One can easily check that the new circuit belongs to $\mathbf{S}_r(m,d)$ and has less complexity. See details in [3]. □

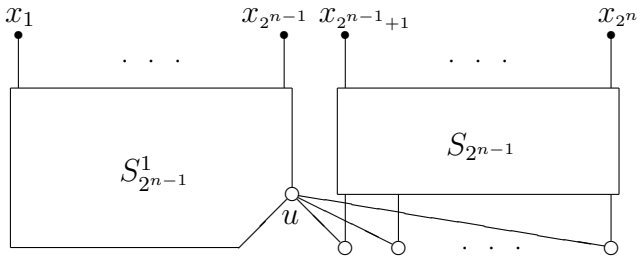


Fig. 2. Structure of S_{2^n}

Evidently, any minimal 2^n-input prefix circuit S_{2^n} of depth n belongs to $\bigcap_{i=0}^{n-1} \mathbf{S}_{2^i}(2^n,n)$. In particular, $S_{2^n} \in \mathbf{S}_{2^{n-1}}(2^n,n)$. Then it contains as a subcircuit a minimal circuit $S_{2^{n-1}}$ implementing prefix sums of 2^{n-1} variables $x_{2^{n-1}+1},\ldots,x_{2^n}$. Furthermore, any output u' of S_{2^n} with $w(u') > 2^{n-1}$ has an output u implementing $x_1 \circ \ldots \circ x_{2^{n-1}}$ as a left parent and a gate labeled by $[2^{n-1}+1; r(u')]$ as a right parent. The latter one is an output of subcircuit $S_{2^{n-1}}$ (see Fig. 2).

Next, like in [3], we bound from below the number of extra gates in S_{2^n}.

The proof of the following lemma is based on the simple observation: if $d(v) = h$, then $w(v) \le 2^h$. Conversely, if $w(v) > 2^{h-1}$, then $d(v) \ge h$.

Lemma 2. *Let a gate v in circuit S have depth h. Suppose that the circuit does not contain skeleton gates whose right ends of labels are $r(v)$ and whose depths are greater than k, where $k < h$. Suppose $w(v) > 2^h - 2^{h-s} + 2^k$. Then the circuit contains s extra gates $v_1,\ldots,v_s$ such that $r(v_i) = r(v)$ and $w(v_i) \ge \big(w(v) \bmod 2^{h-i}\big) > 2^{h-i} - 2^{h-s} + 2^k$. Yet, v_1 is a parent of v, and for any i, gate v_i is a parent of v_{i-1}, and $d(v_s) \le h - s$.*

Proof. The proof is by induction on s. If $s = 0$, then there is nothing to prove.

Take $s \ge 1$ and suppose that the lemma is already proven for all less values of s. Let v' and v_1 be left and right parents of v respectively. It follows from $w(v) = w(v') + w(v_1)$ and $w(v') \le 2^{h-1}$ that

$$w(v_1) \ge w(v) - 2^{h-1} = \big(w(v) \bmod 2^{h-1}\big) > 2^{h-1} - 2^{h-s} + 2^k.$$

Since $w(v_1) > 2^k$, the gate v_1 is not skeleton, so it is extra. Clearly $d(v_1) \le h-1$. Moreover, if $s > 1$, then v_1 satisfies conditions of the lemma (there replace h by $h-1$ and s by $s-1$). Then by the induction hypothesis there exist $s-1$ extra gates $v_2,\ldots,v_s$, and the following condition is satisfied:

$$w(v_i) \ge \big(w(v_1) \bmod 2^{(h-1)-(i-1)}\big) \ge \big(w(v) \bmod 2^{h-i}\big) > 2^{h-i} - 2^{h-s} + 2^k.$$

Any v_i is a parent of v_{i-1}. Further, $d(v_s) \le d(v_1) - (s-1) \le h - s$. □

In particular, the proven lemma justifies an extra gate in the circuit from Fig. 1 under condition that the depth of an output v labeled by $[1;7]$ is 3.

In what follows, S means any 2^n-input prefix circuit of depth n. The following lemma is crucial in the lower bound proof.

Lemma 3 (main). *Suppose $k, N, R \in \mathbb{N}$, $N < 2^k$ and $R < 2^{n-2k-1}$, R is not a power of 2. Then S contains at least N extra gates with right ends of labels from interval*

$$J_{N,R,k} = [N2^{n-k-1} + R2^k,\ N2^{n-k-1} + (R+1)2^k - 1]. \tag{3}$$

In fact, the proof of the lower bound [3] exploits special case $N = 1$ of the above lemma.

To prove Lemma 3 we need some additional notions. But first of all we clarify the meaning of parameters.

Lemma 4. *Under conditions of Lemma 3 for any skeleton gate e of circuit S with $r(e) \in J_{N,R,k}$, the inequality $w(e) < R2^k$ holds.*

Proof. Note that $w(e) \le 2^\nu$, where 2^ν is the largest power of two dividing $r(e)$ (see §2). It follows from $0 < r(e) - N2^{n-k-1} < 2^{n-k-1}$ that $2^\nu \mid \left(r(e) - N2^{n-k-1}\right)$. If R is not a power of two, then $r(e) - N2^{n-k-1} = R2^k + R_0$, where $0 \le R_0 < 2^k$ is also not a power of two. Hence, $2^\nu \le (R2^k + R_0)/3 < R2^k$. Finally, one has $w(e) \le 2^\nu < R2^k$. □

Write N as a $(k+1)$-digit binary number:

$$N = \underbrace{0\ldots0}_{p_1}\ \underbrace{1\ldots1}_{s_1}\ \underbrace{0\ldots0}_{p_2}\ \ldots\ldots\ \underbrace{1\ldots1}_{s_q}\ \underbrace{0\ldots0}_{p_{q+1}}. \tag{4}$$

Here N is divided into blocks of consecutive zeros and ones: p_1 zeros in the most significant bits, then follows a block of s_1 ones, etc. By definition, $p_{q+1} \ge 0$, other numbers p_i and s_i are positive.

The following lemma sets conditions for an application of Lemma 2. Firstly, define $P_t = \sum_{i=1}^{t-1}(p_i + s_i) + p_t$ and

$$N_t = N - \left(N \bmod 2^{k+1-P_t}\right) = N - \left(2^{k+1-P_t} - 2^{k+1-P_t-s_t}\right),$$

where $t = 1, \ldots, q+1$ (here and further everywhere a sum of no summands is assumed to be zero).

Lemma 5. *Suppose $t \le q$ and a gate v of circuit S satisfies $r(v) \in J_{N,R,k}$, $d(v) = n - P_t$ and $l(v) \le N_t 2^{n-k-1} + 1$. Then the circuit contains s_t extra gates $v_1, \ldots, v_{s_t}$ which are different from v and satisfy $r(v_i) = r(v)$, $d(v) > d(v_1) > \ldots > d(v_{s_t})$ and $l(v_{s_t}) \le N_{t+1}2^{n-k-1} + 1$.*

Proof. Indeed,

$$w(v) \geq r(v) - N_t 2^{n-k-1} \geq (N - N_t)2^{n-k-1} + R2^k = \\ = \left(N \bmod 2^{k+1-P_t}\right) 2^{n-k-1} + R2^k \geq \\ \geq \left(2^{k+1-P_t} - 2^{k+1-P_t-s_t}\right) 2^{n-k-1} + R2^k > 2^{n-P_t} - 2^{n-P_t-s_t} + 2^{k_0},$$

where k_0 is the maximal depth of skeleton gates with right ends of labels in $J_{N,R,k}$. The latter inequality is justified by Lemma 4. Thus, Lemma 2 provides s_t required extra gates together with inequalities $d(v_{s_t}) \leq n - P_t - s_t$ and

$$w(v_{s_t}) \geq \left(w(v) \bmod 2^{n-P_t-s_t}\right) \geq \left((r(v) - N_t 2^{n-k-1}) \bmod 2^{n-P_t-s_t}\right) = \\ = r(v) - N2^{n-k-1} + \left((N - N_t)2^{n-k-1} \bmod 2^{n-P_t-s_t}\right) = \\ = r(v) - N2^{n-k-1} + \left(\left(N \bmod 2^{k+1-P_t}\right) 2^{n-k-1} \bmod 2^{n-P_t-s_t}\right) = \\ = r(v) - N2^{n-k-1} + \left(N \bmod 2^{k+1-P_t-s_t}\right) 2^{n-k-1} = \\ = r(v) - N2^{n-k-1} + \left(N \bmod 2^{k+1-P_{t+1}}\right) 2^{n-k-1} = r(v) - N_{t+1}2^{n-k-1}.$$

Consequently, $l(v_{s_t}) \leq N_{t+1}2^{n-k-1} + 1$. □

3.1 Connection graph

For a prefix circuit S and an interval $J_{N,R,k}$ we introduce a notion of *connection graph* $G_{N,R,k}(S)$. The notion includes three components: a graph itself, nonnegative integer numbers attributed to its vertices (*types* of vertices) and a correspondence between vertices of the graph and a subset of gates in the circuit S.

We construct an oriented graph $G_{N,R,k}(S)$ step by step as follows. Initial graph consists of 2^k isolated vertices z_i, where $i = 0, \ldots, 2^k - 1$. Each vertex z_i corresponds to an output gate $v^{0,i}$ of the circuit S labeled by $[1; N2^{n-k-1} + R2^k + i]$. All vertices in $G_{N,R,k}(S)$ are initially of type 0.

Then a sequence of steps $0, \ldots, q$ is performed, where q is defined by (4). Step t consists in the following.

For any vertex z_i of type t in decreasing order by i, take an appropriate of three choices below and follow instructions.

1) If $i \neq 0$ and the right parent of $v^{t,i}$ is either skeleton gate or input of the circuit, do the following. Denote the left end of its label by $N2^{n-k-1} + R2^k + i' + 1$. Let $v_0^{t,i'}$ be the left parent of $v^{t,i}$. If a gate $v^{t,i'}$ has been defined already, then (re-)denote by $v^{t,i'}$ that of gates $v^{t,i'}$, $v_0^{t,i'}$ which has less depth (in the case of equal depths the assignment is arbitrary). Otherwise, assign

$v^{t,i'} = v_0^{t,i'}$. Set up a correspondence between $z_{i'}$ and $v^{t,i'}$. Remove an edge outgoing from z_i, if such edge exists. Include an edge $(z_i, z_{i'})$ and assign type t to $z_{i'}$.

2) (The following instruction is not performed at the step q.) If $d(v^{t,i}) = n - P_{t+1}$, then assign type $t+1$ to a vertex z_i. Apply Lemma 2 with parameters $v = v^{t,i}$ and $s = s_{t+1}$ to the circuit S and denote by $v^{t+1,i}$ a gate which plays a role of v_s in the lemma. Set up a correspondence between z_i and $v^{t+1,i}$.

3) Otherwise, do nothing.

Note that conditions of the choices 1) and 2) do not hold simultaneously since in the case $d(v^{t,i}) = n - P_{t+1}$ a right parent of $v^{t,i}$ is extra.

By the above procedure, all connected components of a connection graph are rooted trees. A *rooted tree* is defined as an oriented tree containing a vertex with no outgoing edges (a root) and all other vertices connected with the root via oriented paths.

Also note that while moving along edges of a connection graph a type of a vertex does not decrease.

The structure of graph $G_{N,R,k}(S)$ allows us to bound from below the number of extra vertices in S with right ends of labels in $J_{N,R,k}$. Next we state a few preliminary observations.

Lemma 6. *a) All gates $v^{t,i}$ defined after completing the procedure of constructing of a connection graph are distinct.*

b) All gates $v^{t,i}$ with $t > 0$ are extra.

c) $d(v^{t,i}) \le n - P_{t+1} + p_{t+1}$. If $t < q$, then $d(v^{t,i}) \ge n - P_{t+1}$.

d) For any $t < q$, a connection graph does not contain an oriented chain connecting $p_{t+1} + 1$ vertices of type t.

e) If $i > 0$ and a vertex z_i of type t is a root, then the right parent of $v^{t,i}$ is extra gate.

Proof. Claim *a*) holds since gates with distinct first indices have different depths (it follows from the claim *c*) and gates with distinct second indices have different right ends of labels.

Claim *b*) holds since $t > 0$ implies that $v^{t,i}$ is neither output nor skeleton gate. The latter follows from Lemma 4. Indeed, $l(v^{t,i}) \le N2^{n-k-1} + 1$ by Lemma 5; hence, $w(v^{t,i}) \ge R2^k$.

Clearly, claim *c*) holds in the case $t = 0$: gates $v^{0,i}$ are outputs of S. In the case of an arbitrary gate $v^{t,i}$, an upper bound $n - P_t - s_t = n - P_{t+1} + p_{t+1}$ for $d(v^{t,i})$ is provided by that of choices 1) and 2) which defines $v^{t,i}$. The lower bound follows from the bound on width of $v^{t,i}$. By Lemma 5, $l(v^{t,i}) \le N_{t+1}2^{n-k-1} + 1$. As a consequence, for $t < q$,

$$w(v^{t,i}) \ge 2^{n-P_{t+1}} - 2^{n-P_{t+1}-s_{t+1}} + R2^k > 2^{n-P_{t+1}-1}.$$

Claim *d*) follows immediately from the claim *c*) and conditions of the choice 2).

Claim *e*) holds since a vertex z_i does not satisfy conditions of the choice 1) at the step t. □

Now we approach to estimation of the number of extra gates in the considered fragment of a circuit S (that is, gates with right ends of labels in $J_{N,R,k}$). Looking at the structure of a connection graph and types of its vertices, we are able to display some extra vertices with right end of labels $N2^{n-k-1} + R2^k + i$, where $i = 0, \ldots, 2^k - 1$.

Let vertex z_i be of type t. Let it take an edge from a vertex of type $t' > 0$. Then an extra gate $v^{t',i}$ is defined after completing the connection graph constructing. If a vertex z_i is preceded by a chain of $p_{t'}$ vertices of type $t' - 1$, then a gate $v^{t'-1,i}$ is also defined and equality $d(v^{t'-1,i}) = n - P_t$ holds by Lemma 6, claim *c*). Consequently, by conditions of choice 2) there exist extra gates $v^{t'-1,i}$, $v^{t',i}$ and another $s_{t'} - 1$ extra gates settled between former two gates (with respect to depth). Moreover, any of the latter gates does not coincide with any $v^{t'',i}$ by Lemma 6, claim *c*). If a vertex z_i, $i > 0$, is a root, then one can indicate another extra gate, the right parent of $v^{t,i}$.

Since vertex z_0 is always a root, we can write the number of extra gates counted above as

$$I_{N,R,k}(S) = \mu(G_{N,R,k}(S)) - 1 + \sum_{z \in G} \sum_{t=1}^{q} c(z,t), \tag{5}$$

where $\mu(G)$ denotes the number of connected components of G and function $c(z,t)$ is defined for $t \geq 1$ as

$$c(z,t) = \begin{cases} s_t, & \text{vertex } z \text{ is preceded by a chain of } p_t \text{ vertices of type } t-1; \\ 1, & \text{else, if } z \text{ is of type } t \text{ or } z \text{ takes} \\ & \text{an edge from a vertex of type } t; \\ 0, & \text{otherwise.} \end{cases}$$

The lack of measure $I_{N,R,k}(S)$ is its dependence on both topology and types of vertices of the connection graph. Our next step is to replace $I_{N,R,k}(S)$ with a more convenient measure depending on the connection graph topology only.

3.2 Cost of a graph

Denote by Δ a set of graphs will all connected components be rooted trees. Depth $d_G(z)$ of a vertex z in graph $G \in \Delta$ is defined as the maximal length

(number of edges) of an oriented path from a leaf of G to the vertex z. (As usual, under a leaf of a graph we understand a vertex with no input edges. Its depth is zero.) We will use notation $G' \subset G$ to express that G' is a subgraph of graph G.

For a graph $G \in \Delta$ we introduce a notion of $(p_1, s_1, \ldots, p_q, s_q)$-*cost*, where $p_i, s_i \in \mathbb{N}$ for all $i = 1, \ldots, q$. Previously, we define integer intervals:

$$M_t(p_1, \ldots, p_q) = \left[\sum_{i=1}^{t} p_i,\ \sum_{i=1}^{t+1} p_i - 1 \right],\ 0 \le t < q,$$

$$M_q(p_1, \ldots, p_q) = \left[\sum_{i=1}^{q} p_i,\ +\infty \right).$$

Next, we define a $(p_1, s_1, \ldots, p_q, s_q)$-cost of a vertex z of graph G as

$$C^G_{p_1,s_1,\ldots,p_q,s_q}(z) = \sum_{t=1}^{q} c^G_{p_1,s_1,\ldots,p_q,s_q}(z,t),$$

where

$$c^G_{p_1,s_1,\ldots,p_q,s_q}(z,t) = \begin{cases} s_t, & \text{vertex } z \text{ takes an edge from a vertex } z' \\ & \text{such that } d_G(z') = \sum_{i=1}^{t} p_i - 1; \\ 1, & \text{else, if } z \text{ takes an edge from a vertex } z' \\ & \text{such that } d_G(z') \in M_t(p_1, \ldots, p_q); \\ 0, & \text{otherwise.} \end{cases}$$

Finally, we define a $(p_1, s_1, \ldots, p_q, s_q)$-cost of graph G as

$$C_{p_1,s_1,\ldots,p_q,s_q}(G) = \mu(G) - 1 + \sum_{z \in G} C^G_{p_1,s_1,\ldots,p_q,s_q}(z).$$

Speaking formally, cost is also defined for $q = 0$ as $C^G(z) = 0$ and $C(G) = \mu(G) - 1$.

Before clarifying a connection between the cost and introduced above measure $I_{N,R,k}(S)$ we will establish a simple relation between the type and the depth of a vertex of the connection graph.

Lemma 7. *Let $d_{G_{N,R,k}(S)}(z) \ge \sum_{i=1}^{t} p_i$, where parameters N, R, k are given by Lemma 3 and p_i are determined by (4). Then the type of z is at least t.*

Proof. Consider an oriented chain determining the depth of vertex z: by the given condition the chain contains at least $\sum_{i=1}^{t} p_i + 1$ vertices including, by Lemma 6 claim *c*), at most p_{i+1} vertices of any type i. It follows that the type of z is at least t. □

Lemma 8. *Let parameters N, R, k be defined as in Lemma 3 and p_i, s_i be determined by (4). Suppose that all vertices of graph $G_{N,R,k}(S)$ have minimal possible types in the sense of Lemma 7. Then $I_{N,R,k}(S) = C_{p_1,s_1,\ldots,p_q,s_q}(G_{N,R,k}(S))$.*

Proof. The statement of lemma follows from coinciding of values of $c(z,t)$ in (5) with $c^G_{p_1,s_1,\ldots,p_q,s_q}(z,t)$. □

It follows from the proven lemma that the cost of the connection graph $G_{N,R,k}(S)$ is $I_{N,R,k}(S)$ in the case when all its vertices have minimal possible types (in view of Lemma 7). But speaking generally, measure $C_{p_1,s_1,\ldots,p_q,s_q}(G_{N,R,k}(S))$ does not serve as a lower bound for $I_{N,R,k}(S)$. However, a weaker statement holds that allows us to use cost to bound $I_{N,R,k}(S)$ from below.

It is natural to extend the notion and notation of cost to a nonempty set of graphs $\Gamma \subset \Delta$:

$$C_{p_1,s_1,\ldots,p_q,s_q}(\Gamma) = \min_{G\in\Gamma} C_{p_1,s_1,\ldots,p_q,s_q}(G).$$

(We stress that the minimum should be here.)

For an oriented graph T define

$$\delta(T) = \{G \mid G \subset T, G \text{ contains all vertices of } T\} \cap \Delta.$$

Lemma 9. *Let N, R, k be defined by Lemma 3 and p_i, s_i be determined by (4). Then*

$$I_{N,R,k}(S) \geq C_{p_1,s_1,\ldots,p_q,s_q}(\delta(G_{N,R,k}(S))).$$

Proof. We propose a procedure of removing some edges of connection graph $G_{N,R,k}(S)$ resulting in a graph with the cost not exceeding $I_{N,R,k}(S)$.

We denote by G' a graph in the process of transformations. Having in mind an assignment of types to vertices of G' let us define quantities $c'(z,t)$ and $I(G')$ analogously to $c(z,t)$ and $I_{N,R,k}(S)$ defined for a connection graph. Initially, $G' = G_{N,R,k}(S)$ and $I(G') = I_{N,R,k}(S)$.

Next, for any vertex z_i in decreasing order by i, perform the following iteration. If type t of the vertex z_i in G' is not minimal in the sense of Lemma 7 (which is to be applied to graph G' instead of $G_{N,R,k}(S)$), then reduce the type to minimal and remove an outgoing edge, if the latter is present.

Note that a coefficient $c'(z_i,t)$ is positive before the iteration and it turns to zero afterwards. Other coefficients $c'(z,t')$, $z \in G'$, $t' = 1,\ldots,q$, do not increase (only possible changes are decreasing ones: either a coefficient $c'(z',t)$ can decrease, where vertex z' takes an edge from z_i, or a coefficient $c'(z'',t+1)$

can decrease, where z'' is a vertex in a chain beginning in z_i). Hence, the iteration does not increase $I(G')$, since $c'(z_i, t)$ strictly decreases and $\mu(G')$ increases at most by 1.

The order of enumeration of vertices provides that all vertices with indices greater than i have minimal types. Finally, we obtain a graph $G \in \delta(G_{N,R,k}(S))$ satisfying conditions of Lemma 8 (up to notations). Consequently, $I(G) = C_{p_1,s_1,\ldots,p_q,s_q}(G)$. Thus, the statement of lemma follows due to $I(G) \leq I_{N,R,k}(S)$. □

The proven lemma allows to reduce our consideration to the universal cost measure, that is, applicable to any graph in Δ and independent of a circuit S.

Our further strategy is to show that the minimal cost among acceptable graphs is delivered by graphs of a certain kind, namely, by subgraphs of a hyperpair. Calculation of the minimal value of cost of such graphs should lead us to a lower bound on the cost of connection graph $G_{N,R,k}(S)$ and farther to a lower bound on the number of extra gates in the considered fragment of the circuit S given by Lemma 3.

3.3 A set of acceptable graphs. Hyperpairs

Now we determine a set of acceptable graphs, that is, a set containing graphs isomorphic to any possible connection graph. Denote by T_k a graph consisting of vertices $z_0, \ldots, z_{2^k-1}$ which contains an edge $(z_i, z_{i'})$ iff $i - i' = 2^t$ and $2^t \mid i$ for some $t \geq 0$.

Lemma 10. $G_{N,R,k}(S) \in \delta(T_k)$.

Proof. By definition, graph T_k contains an edge $(z_i, z_{i'})$ iff a vertex of S labeled by $[N2^{n-k-1} + R2^k + i' + 1; N2^{n-k-1} + R2^k + i]$ is either skeleton gate or input. Consequently, graph T_k contains any edge which might occur in graph $G_{N,R,k}(S)$ (here, independently of N and R). Hence, $G_{N,R,k}(S) \subset T_k$. □

Lemma shows that $\delta(T_k)$ is appropriate choice for a set of acceptable graphs. The following claim is immediate from the latter lemma and Lemma 9.

Corollary 1. *Let N, R, k be defined by Lemma 3 and p_i, s_i be determined by (4). Then*

$$I_{N,R,k}(S) \geq C_{p_1,s_1,\ldots,p_q,s_q}(\delta(T_k)).$$

For convenience of further arguments we propose another, recursive way of definition of graph T_k. In passing, we define sets of *marked* vertices, *right* and *wrong* edges. Graph T_0 is a single vertex which is marked. Graph T_k

is constructed of two graphs T_{k-1} in the following way. Add edges from the root of the first graph T_{k-1} to all marked vertices of the second graph. (The root of T_k is uniquely defined since the graph is connected.) A set of marked vertices of T_k is constituted by all marked vertices of the first graph and the root of the second graph. The latter vertex also occurs to be a root of T_k. A set of right edges of T_k is formed by right edges of both graphs T_{k-1} and an edge connecting roots of graphs. Other edges are defined to be wrong.

Simplest graphs in the family $\{T_k\}$ are shown on Fig. 3: non-vertical edges are oriented from left to right, vertical edges are oriented upwards, marked vertices and right edges are distinguished.

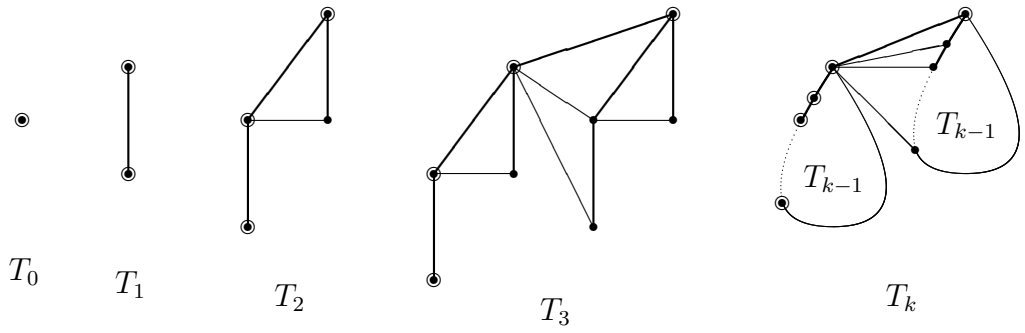


Fig. 3

One can establish a congruence of two definitions via numerating of vertices in the second definition. Let vertex of T_0 be not numbered. Further, while constructing graph T_k of two graphs T_{k-1} we attach digit 1 from the left to numbers of all vertices of the first graph and attach digit 0 to numbers of all vertices of the second graph. Then a vertex z_i from the first definition corresponds to a vertex numbered by i in the second definition.

It can be easily checked that each vertex of graph T_k takes at most one wrong input edge, to be more precise, marked vertices take only right edges and each of other vertices takes besides right edges exactly one wrong edge.

Let us define another important family of graphs, hyperpairs.

Hyperpair H_k is a rooted tree defined recursively as follows. Hyperpair H_0 is a single vertex which is the root. For $k > 0$, hyperpair H_k is composed of two hyperpairs H_{k-1} via connecting of its roots by an edge. Simplest hyperpairs are shown on Fig. 4 (edges are oriented upwards).

Note that hyperpair H_k can be obtained from T_k by removing all wrong edges.

Let a graph $H \in \Delta$ have one of its roots marked as the *main root*. We define a *composition* $T \circ H$ of graphs $T \in \Delta$ and H as a graph obtained by joining of main roots of graphs isomorphic to H into graph T (see Fig. 5, edges are oriented upwards). Note that $T \circ H \in \Delta$.

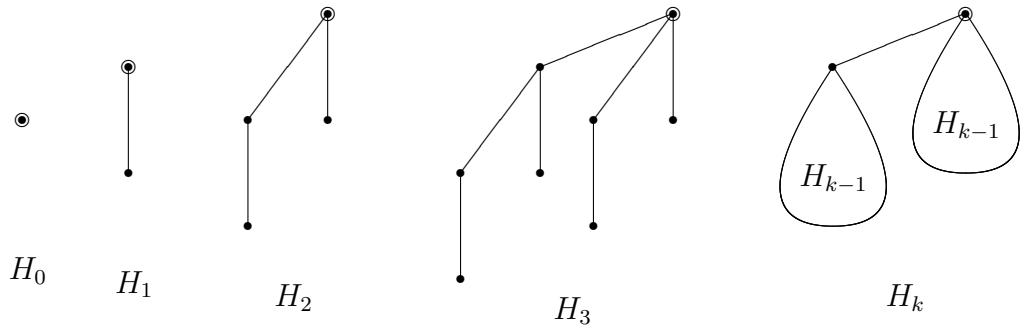


Fig. 4. Hyperpairs

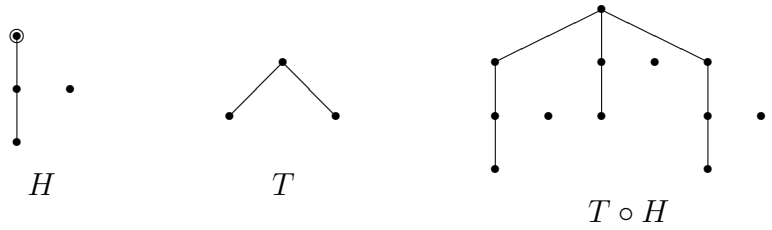


Fig. 5. Composition of graphs

In what follows, if a choice of main root of graph H is clear from context, we omit word "main". In particular, a unique root in a rooted tree is certainly main. If a graph H' is to be chosen from a set $\delta(H)$, $H \in \Delta$, then we assign the main root of H to be the main root of H' as well.

Next, we list some simple properties of hyperpairs.

1) Composition of two hyperpairs is a hyperpair: hyperpair $H_{k_1+k_2}$ is isomorphic to $H_{k_1} \circ H_{k_2}$.

2) For any vertex z of hyperpair H_k, the largest connected subgraph containing given vertex as a root is a hyperpair H_d, where $d = d_{H_k}(z)$.

3) The depth of the root of hyperpair H_k is k. The root takes k input edges.

In graph T_k (as well as in H_k) each vertex is a root of some subgraph T_i (respectively, H_i). Let us define an *order* of vertex z in graph T_k (H_k) as the maximal index i such that T_k (H_k) contains a subgraph isomorphic to T_i (H_i) with root z (in similar cases below we will name "graph isomorphic to T_i" simply "graph T_i"). According to definition of T_k there is an alternative way of definition of order of vertex as the number of right input edges. As mentioned above, an order of vertex z in a hyperpair H_k is $d_{H_k}(z)$.

By the construction, a vertex of order i in graph T_k puts out a right edge to a vertex of greater order and it puts out wrong edges (in the case $i > 0$) to vertices of orders $0, \ldots, i-1$, where latter vertices form a chain of right edges.

In what follows under isomorphism in the set of graphs $\{T_k\}$ and their subgraphs we understand both topological coincidence and coincidence of orders of corresponding vertices except roots. In particular, we want the phrase "subgraph T_i with root v in graph T_k" to point explicitly to a graph from the described above recursive procedure of constructing T_k (it is the only subgraph to have such orders of vertices as in definition of T_i).

Our next goal is to determine values $C_{p_1,s_1,\ldots,p_q,s_q}(\delta(H_k))$. The following paragraph contains technical Lemmas 12, 13, 14 providing a technique for all further arguments.

3.4 Cost of a set of subgraphs of a composition of rooted trees

We say that an edge ρ' of graph $G \in \Delta$ *depends* on an edge ρ if removing of ρ leads to decreasing of the depth of a vertex emitting ρ'.

Lemma 11. *a) A set of edges of $G \in \Delta$ depending on an edge ρ forms an oriented chain (possibly empty) beginning in a vertex which takes ρ.*

Let this chain consist of j edges $\rho_1, \ldots, \rho_j$, connecting subsequently vertices $z_0, \ldots, z_j$. Let z be a vertex emitting edge ρ and G' be a graph obtaining from G by removing ρ.

b) $d_G(z_i) = d_G(z) + i + 1$ for any $j > 0$ and $i < j$.

c) For any $i = 1, \ldots, j$, a set of edges depending on ρ_i is exactly $\rho_{i+1}, \ldots, \rho_j$.

d) If $z' \neq z_i$ for any $i = 0, \ldots, j$, then $C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z') = C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z')$.

Proof. Claim *a*) follows from a simple investigation of vertices whose depths can change after removing ρ.

Claim *b*) holds since the (unique) longest oriented chain from a leaf of G to a vertex z_i passes through z.

To verify claim *c*), denote by G'' a graph obtaining from G via removing an edge ρ_i. For any $i' \geq i$, one has $d_{G''}(z_{i'}) \leq d_{G'}(z_{i'})$ since a set of leaves connected with $z_{i'}$ via oriented chains in G'' is contained in the analogously defined set of graph G'. Therefore, for $i \leq i' < j$ we have $d_{G''}(z_{i'}) < d_G(z_{i'})$.

One observes two possibilities for the vertex z_j: either it is a root or $d_{G'}(z_j) = d_G(z_j)$. In the first case, there is nothing to prove. In the second case, note that G contains an oriented chain of length $d_G(z_j)$ beginning in a leaf and terminating in the vertex z_j, and the chain does not contain ρ_j and, as a consequence, it does not contain any of edges ρ_i. Hence, $d_{G''}(z_j) = d_G(z_j)$.

Claim *d*) holds since depths of vertices putting out edges to z' do not change after removing ρ. □

Lemma 12. *One can remove an arbitrary edge ρ from a graph $G \in \Delta$ and possibly remove some edges depending on ρ so that the cost of the graph increases at most by* 1.

Proof. The proof is by induction on number j of edges depending on ρ.

If $j = 0$, then costs of vertices of the graph do not increase after removing the edge. Only number of connected components increases by 1, so the statement of lemma holds in this case.

For the induction step from $j-1$ to j, we use notation of Lemma 11.

Clearly, $C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_0) \le C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_0)$. Consider two cases.

a) Suppose $C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_0) < C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_0)$. Note that exactly $j-1$ edges in G depend on ρ_1. Thus, by induction hypothesis we can remove ρ_1 from G and also remove some edges in $\{\rho_i\}$ so that the cost of the graph increases at most by 1. Next we remove ρ: the cost will not increase since increasing of the number of connected components is compensated by decreasing of the cost of the vertex z_0.

b) Suppose $C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_0) = C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_0)$. Let $d_G(z) \in M_t(p_1,\ldots,p_q)$. Then $c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_0,t') = c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_0,t')$ for $t' < t$ and $t' > t+1$, since the presence of edge ρ does not matter for the above coefficients.

Assuming $d_G(z) = \sum_{i=1}^{t+1} p_i - 1$ and having in mind $d_{G'}(z_0) < d_G(z_0)$ we conclude $c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_0,t) \le c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_0,t)$ and $c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_0,t+1) = 0 < s_{t+1} = c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_0,t+1)$. But it contradicts the equal costs of vertex z_0 in graphs G and G'. Therefore, $d_G(z) \ne \sum_{i=1}^{t+1} p_i - 1$, consequently, $c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_0,t+1) = c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_0,t+1) = 0$. Then $c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_0,t) = c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_0,t) \ne 0$. So it follows that $d_{G'}(z_0) \in M_t(p_1,\ldots,p_q)$.

By relations

$$d_{G'}(z_0) + i - 1 \le d_{G'}(z_{i-1}) < d_G(z_{i-1}) = d_G(z_0) + i - 1$$

equalities $c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_i,t) = c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_i,t)$ and

$$c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_i,t+1) = c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_i,t+1) = 0,$$

as well as $C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_i) = C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_i)$ remain true for all $i \le j'$, where either $j' = j$ or $d_G(z_{j'}) = \sum_{i=1}^{t+1} p_i - 1$.

b.1) In the case $j' = j$, after removing ρ costs of all vertices in graph remain intact and the cost of the entire graph increases by 1 due to increasing of the number of connected components. Thus, the statement of lemma holds in this case.

b.2) Else if $d_G(z_{j'}) = \sum_{i=1}^{t+1} p_i - 1$, then

$$c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_{j'+1}, t+1) \le c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_{j'+1}, t+1) = s_{t+1},$$

where equality is possible only when $j'+1 = j$. Then $C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_j) = C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_j)$ and we can apply an argument of item b.1).

If $j'+1 < j$, then $c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_{j'+1}, t+1) = 0$, hence, $C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_{j'+1}) < C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z_{j'+1})$. By analogy with item a) and by induction hypothesis we can remove an edge $\rho_{j'+2}$ and some edges in $\{\rho_i\}$ from G to increase the cost of graph at most by 1. Next, we remove the edge ρ: the cost of graph does not increase since the cost of vertex $z_{j'+1}$ decreases. Case b) is completed. □

Lemma 13. *Suppose that a graph $G \in \Delta$ contains a subgraph H with root z and G contains no edges connecting a vertex from $H \setminus \{z\}$ and a vertex from $G \setminus H$. Let $H' \in \Delta$ and graph G' be obtained from G via replacement of H by a graph H' (the root of H' must be superposed with the vertex z). Suppose $d_H(z) \ge d_{H'}(z)$ and $d_G(z)$, $d_{G'}(z) \in M_t(p_1, \ldots, p_q)$ for some t, and*

$$\left(C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z) - C^{H}_{p_1,s_1,\ldots,p_q,s_q}(z)\right) + C_{p_1,s_1,\ldots,p_q,s_q}(H) = \left(C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z) - C^{H'}_{p_1,s_1,\ldots,p_q,s_q}(z)\right) + C_{p_1,s_1,\ldots,p_q,s_q}(H').$$

Then there exists a graph G'' obtained from G' via removing some edges in an oriented chain beginning in z, which satisfies inequality

$$C_{p_1,s_1,\ldots,p_q,s_q}(G'') \le C_{p_1,s_1,\ldots,p_q,s_q}(G).$$

Proof. The condition of disposition of subgraph H inside G (subgraph H is connected with the rest of the graph only via vertex z) implies that a change of cost of G produced by replacement of H by H' is a sum of three summands: difference of costs of these subgraphs, a change of the cost of vertex z (one must keep in mind that the cost of a vertex is included partially in the cost of subgraph) and change of costs of vertices in a chain beginning in z.

It is easy to see that the cost of the subgraph together with the cost of z is $A_2 - A_1$, where

$$A_1 = \left(C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z) - C^{H}_{p_1,s_1,\ldots,p_q,s_q}(z)\right) + C_{p_1,s_1,\ldots,p_q,s_q}(H)$$

(cost of a fragment in the question before replacement) and

$$A_2 = \left(C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z) - C^{H'}_{p_1,s_1,\ldots,p_q,s_q}(z)\right) + C_{p_1,s_1,\ldots,p_q,s_q}(H')$$

(cost after replacement). By conditions of lemma, $A_1 = A_2$. Consequently, the difference in costs of graphs G and G' is determined by the cost of vertices in the chain beginning in z.

If vertex z does not have outgoing edges, then $C_{p_1,s_1,\ldots,p_q,s_q}(G') = C_{p_1,s_1,\ldots,p_q,s_q}(G)$. Therefore, assign $G'' = G'$. Otherwise, consider a sequence of vertices $z = z_0, z_1, z_2, \ldots$ in the oriented chain beginning in z.

If $d_G(z) = d_{G'}(z)$, then costs of vertices in the chain remain intact. So we can also assign $G'' = G'$. In the opposite case note that since $d_H(z) \geq d_{H'}(z)$, the inequality $d_G(z_j) \geq d_{G'}(z_j)$ holds for any j.

If $d_G(z_j) \in M_t(p_1, \ldots, p_q)$ for some $j \geq 1$, then $C^G_{p_1,s_1,\ldots,p_q,s_q}(z_j) = C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_j)$, since $d_G(z_{j-1}), d_{G'}(z_{j-1}) \in M_t(p_1, \ldots, p_q)$ due to the condition $d_G(z), d_{G'}(z) \in M_t(p_1, \ldots, p_q)$. Hence, if $d_G(z_j) \in M_t(p_1, \ldots, p_q)$ for all vertices in the chain, then the replacement of H by H' preserves the cost of the graph. So, assign $G'' = G'$.

Otherwise, let z_k be the first vertex in the chain with $d_G(z_k) \geq \sum_{i=1}^{t+1} p_i$. The only case when quantity $C^G_{p_1,s_1,\ldots,p_q,s_q}(z_k)$ changes after the replacement is $d_G(z_{k-1}) = \sum_{i=1}^{t+1} p_i - 1 > d_{G'}(z_{k-1})$, and the only change can occur is decreasing owing to a change of the coefficient $c^G_{p_1,s_1,\ldots,p_q,s_q}(z_k, t+1)$.

If $d_{G'}(z_k) = d_G(z_k)$, then $C_{p_1,s_1,\ldots,p_q,s_q}(G') \leq C_{p_1,s_1,\ldots,p_q,s_q}(G)$. So, assign $G'' = G'$.

Otherwise, i.e. in the case $d_{G'}(z_k) < d_G(z_k)$, note that $d_G(z_k) = \sum_{i=1}^{t+1} p_i$. Consequently,

$$c^G_{p_1,s_1,\ldots,p_q,s_q}(z_k, t+1) = s_{t+1} > 0 = c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_k, t+1)$$

and further, $C^G_{p_1,s_1,\ldots,p_q,s_q}(z_k) > C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z_k)$. In this case, remove an edge going out of vertex z_k of graph G, if the edge exists, via the method of Lemma 12. Next, replace H by H' and denote obtained graph by G''. Possible increasing by 1 of the graph cost after removing the edge is compensated by the following decreasing of the cost of vertex z_k after replacement. Costs of other vertices in the chain remain intact. Thus, $C_{p_1,s_1,\ldots,p_q,s_q}(G'') \leq C_{p_1,s_1,\ldots,p_q,s_q}(G)$. □

Conditions $d_G(z), d_{G'}(z) \in M_t(p_1, \ldots, p_q)$ and $A_1 = A_2$ (actually, $A_1 \geq A_2$) can be withdrawn in favour of additional assumptions on the graph H'.

Lemma 14. *Suppose that a graph $G \in \Delta$ contains a subgraph H with root z and G contains no edges connecting a vertex from $H \setminus \{z\}$ and a vertex from $G \setminus H$. Let $H' \in \Delta$ and graph G' be obtained from G via replacement of H by the graph H' (the root z' of H' must be superposed with the vertex z). Let $d_H(z) \in M_t(p_1, \ldots, p_q)$, $d_{H'}(z') \in M_{t'}(p_1, \ldots, p_q)$ and $C^{H'}_{p_1,s_1,\ldots,p_q,s_q}(z') = \sum_{i=1}^{t'} s_i$.*

Also suppose that

$$\begin{cases} C_{p_1,s_1,\dots,p_q,s_q}(H') < C_{p_1,s_1,\dots,p_q,s_q}(H), & \text{if } d_{H'}(z') > d_H(z) \\ C_{p_1,s_1,\dots,p_q,s_q}(H') + \sum_{t'+1}^{t} s_i \le C_{p_1,s_1,\dots,p_q,s_q}(H), & \text{if } d_{H'}(z') \le d_H(z) \end{cases}.$$

Then there exists a graph G'' obtained from G' via removing some edges in an oriented chain beginning in z, which satisfies inequality

$$C_{p_1,s_1,\dots,p_q,s_q}(G'') \le C_{p_1,s_1,\dots,p_q,s_q}(G).$$

Additionally, if z is a root of G and $d_G(z) < d_{G''}(z)$, then

$$C_{p_1,s_1,\dots,p_q,s_q}(G'') < C_{p_1,s_1,\dots,p_q,s_q}(G).$$

Proof. a) Consider the case $d_{H'}(z') > d_H(z)$. By the method of Lemma 12 remove from G an edge going out from the vertex z, if the edge exists, and replace subgraph H by H'. Assign obtained graph to be G''. Now we prove the choice to be correct.

Consider a change of the cost of vertex z. By conditions of lemma, $c^{H'}_{p_1,s_1,\dots,p_q,s_q}(z',i) = s_i$ for any $i \le t'$. Hence, for any i, $c^{H'}_{p_1,s_1,\dots,p_q,s_q}(z',i) \ge c^{H}_{p_1,s_1,\dots,p_q,s_q}(z,i)$. As a consequence,

$$C^{G'}_{p_1,s_1,\dots,p_q,s_q}(z) - C^{H'}_{p_1,s_1,\dots,p_q,s_q}(z') \le C^{G}_{p_1,s_1,\dots,p_q,s_q}(z) - C^{H}_{p_1,s_1,\dots,p_q,s_q}(z).$$

So the cost of the graph increases at most by 1 as a result of removing an edge and decreases by $A_1 - A_2$ after replacement of H by H', where

$$A_1 = \left(C^{G}_{p_1,s_1,\dots,p_q,s_q}(z) - C^{H}_{p_1,s_1,\dots,p_q,s_q}(z)\right) + C_{p_1,s_1,\dots,p_q,s_q}(H),$$

$$A_2 = \left(C^{G'}_{p_1,s_1,\dots,p_q,s_q}(z) - C^{H'}_{p_1,s_1,\dots,p_q,s_q}(z')\right) + C_{p_1,s_1,\dots,p_q,s_q}(H').$$

The argument above together with conditions of lemma shows that $A_1 > A_2$. Therefore, the described transformation does not increase the cost of graph.

If z is a root of G, then the cost strictly decreases, since removing an edge going out of z is unnecessary.

b) Let $d_{H'}(z') \le d_H(z)$ (it means that $t' \le t$). We estimate the difference in costs of fragments of graphs G and G' with root z:

$$\begin{aligned} A_1 &= \left(C^{G}_{p_1,s_1,\dots,p_q,s_q}(z) - C^{H}_{p_1,s_1,\dots,p_q,s_q}(z)\right) + C_{p_1,s_1,\dots,p_q,s_q}(H) \ge \\ &\ge \sum_{i=t+1}^{q} c^{G}_{p_1,s_1,\dots,p_q,s_q}(z,i) + C_{p_1,s_1,\dots,p_q,s_q}(H') + \sum_{i=t'+1}^{t} s_i \ge \\ &\ge \sum_{i=t'+1}^{q} c^{G'}_{p_1,s_1,\dots,p_q,s_q}(z,i) + C_{p_1,s_1,\dots,p_q,s_q}(H') = \\ &= \left(C^{G'}_{p_1,s_1,\dots,p_q,s_q}(z) - C^{H'}_{p_1,s_1,\dots,p_q,s_q}(z')\right) + C_{p_1,s_1,\dots,p_q,s_q}(H') = A_2. \end{aligned}$$

If $A_1 > A_2$, then a reasoning is the same as in item a).

Otherwise, by the above computations equality $A_1 = A_2$ is possible only under the following conditions:

$$\begin{aligned} c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z,i) &= c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z,i), && i > t,\\ c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z,i) &= c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z,i) = s_i, && t'+1 \le i \le t. \end{aligned}$$

Therefore, $d_G(z)$, $d_{G'}(z) \in M_{t''}(p_1,\ldots,p_q)$ for some t''. So, conditions of Lemma 13 are satisfied. Thus, we can remove some edges from G' in a chain beginning in vertex z, if necessary, and produce a graph G'' with no larger cost than that of the graph G. □

From now on we denote the number of vertices in a graph G by $|G|$.

Lemma 15. *Let $T, H \in \Delta$. Suppose that the depth of the main root z' of graph H satisfies condition $d_H(z') = d + \sum_{i=1}^{t-1} p_i \in M_{t-1}(p_1,\ldots,p_q)$. Then*

$$C_{p_1,s_1,\ldots,p_q,s_q}(T \circ H) = C_{p_t-d,\, s_t,\ldots,p_q,s_q}(T) + |T| C_{p_1,s_1,\ldots,p_q,s_q}(H).$$

Proof. In compliance with the definition of composition consider graph $T \circ H$ as an outer graph T which is built on the roots of inner graphs isomorphic to H. Denote by Z_T a set of vertices of the outer subgraph and denote by Z_H a set of other vertices of the graph $T \circ H$.

Let $z \in Z_T$. The following relations are easy to check:

$$\mu(T \circ H) = \mu(T) + |T|(\mu(H) - 1),$$

$$C^{T\circ H}_{p_1,s_1,\ldots,p_q,s_q}(z) = C^{T}_{p_t-d,\, s_t,\ldots,p_q,s_q}(z) + C^{H}_{p_1,s_1,\ldots,p_q,s_q}(z').$$

As a consequence, one obtains

$$\begin{aligned} &C_{p_1,s_1,\ldots,p_q,s_q}(T \circ H) = \\ &\quad = \mu(T \circ H) - 1 + \sum_{z \in Z_T} C^{T\circ H}_{p_1,s_1,\ldots,p_q,s_q}(z) + \sum_{z \in Z_H} C^{T\circ H}_{p_1,s_1,\ldots,p_q,s_q}(z) = \\ &\qquad = \mu(T) - 1 + |T|(\mu(H) - 1) + \\ &\quad + \sum_{z \in Z_T} \left(C^{T}_{p_t-d,\, s_t,\ldots,p_q,s_q}(z) + C^{H}_{p_1,s_1,\ldots,p_q,s_q}(z) \right) + \sum_{z \in Z_H} C^{H}_{p_1,s_1,\ldots,p_q,s_q}(z) = \\ &\qquad = C_{p_t-d,\, s_t,\ldots,p_q,s_q}(T) + |T| C_{p_1,s_1,\ldots,p_q,s_q}(H). \end{aligned}$$

□

Next lemma is principal for establishing the cost of a set of subgraphs of a hyperpair. We state it rather generally to involve different situations arising during analysis of the cost of such set. Before the formulation we introduce some notions motivated by Lemma 14.

Let T be a rooted tree with the root z. Define

$$\theta_{p_1,s_1,\ldots,p_q,s_q}(T) = \min\{d_G(z) \mid G \in \delta(T),\, C_{p_1,s_1,\ldots,p_q,s_q}(G) = C_{p_1,s_1,\ldots,p_q,s_q}(\delta(T))\},$$

$$\delta^t_{p_1,\ldots,p_q}(T) = \delta(T) \cap \{G \,|d_G(z) \in M_t(p_1,\ldots,p_q)\}\,,$$

$$\Omega^t_{p_1,s_1,\ldots,p_q,s_q}(T) = \begin{cases} \min\limits_{G\in\delta^t_{p_1,\ldots,p_q}(T)} C_{p_1,s_1,\ldots,p_q,s_q}(G), & \delta^t_{p_1,\ldots,p_q}(T) \neq \emptyset \\ +\infty, & \delta^t_{p_1,\ldots,p_q}(T) = \emptyset \end{cases}.$$

Lemma 16. *Let T, H be rooted trees,*

$$\theta_{p_1,s_1,\ldots,p_q,s_q}(H) = d + \sum_{i=1}^{t'} p_i \in M_{t'}(p_1,\ldots,p_q)$$

and for any $t \geq t'$,

$$C_{p_1,s_1,\ldots,p_q,s_q}(\delta(H)) + \sum_{i=t'+1}^{t} s_i \leq \Omega^t_{p_1,s_1,\ldots,p_q,s_q}(H). \tag{6}$$

Let H^0 be a graph of minimal cost in $\delta(H)$ and z' be its root. Suppose $d_{H^0}(z') = \theta_{p_1,s_1,\ldots,p_q,s_q}(H)$ and $C^{H^0}_{p_1,s_1,\ldots,p_q,s_q}(z') = \sum_{i=1}^{t'} s_i$. Then the minimum of $(p_1, s_1, \ldots, p_q, s_q)$-cost in the set $\delta(T \circ H)$ and the minimum of the depth of the root of a graph of minimal cost are achieved on a graph from $\delta(T) \circ H^0$. In addition,

$$C_{p_1,s_1,\ldots,p_q,s_q}(\delta(T \circ H)) = C_{p_{t'+1}-d,\, s_{t'+1},\ldots,p_q,s_q}(\delta(T)) + |T| C_{p_1,s_1,\ldots,p_q,s_q}(\delta(H)),$$

$$\theta_{p_1,s_1,\ldots,p_q,s_q}(T \circ H) = \theta_{p_{t'+1}-d,\, s_{t'+1},\ldots,p_q,s_q}(T) + \theta_{p_1,s_1,\ldots,p_q,s_q}(H).$$

Proof. As above, consider graph $T \circ H$ as an outer graph T which is built on the roots of inner graphs isomorphic to H. We are going to show the existence of an optimal cost graph from $\delta(T \circ H)$ which contains optimal subgraphs of inner graphs and also delivers the minimum of the root depth. It suffices to prove that one can take an arbitrary graph $G \in \delta(T \circ H)$ and replace its fragment at the intersection with any inner graph H by the graph H^0 and remove some edges in the outer subgraph, if necessary, so that the cost of the entire graph will not increase.

Denote by H_z a fragment of graph G at the intersection with some inner graph with root z. Subgraph H_z of graph G together with a graph G' obtained from G via replacement of H_z by H^0 satisfy conditions of Lemma 14. Actually, if $d_{H_z}(z) < \theta_{p_1,s_1,\ldots,p_q,s_q}(H) = d_{H^0}(z')$, then H_z is not a graph of

minimal cost in $\delta(H)$. Hence, $C_{p_1,s_1,\ldots,p_q,s_q}(H_z) > C_{p_1,s_1,\ldots,p_q,s_q}(H^0)$. Otherwise, i.e. if $d_{H^0}(z') \le d_{H_z}(z) \in M_t(p_1,\ldots,p_q)$, then

$$C_{p_1,s_1,\ldots,p_q,s_q}(H_z) \ge C_{p_1,s_1,\ldots,p_q,s_q}(H^0) + \sum_{i=t'+1}^{t} s_i$$

by (6).

Replace H_z by H^0 via the method of Lemma 14. The method provides that removed edges does not lie in other inner subgraphs of graph G.

Do the same with all inner subgraphs of G. By Lemma 14 increasing of the depth of the root of G occurs only when the cost decreases, so initial graph G is not optimal.

Now we can reduce our attention to graphs $G \in \delta(T) \circ H^0$. The above argument shows that such a graph delivers both minimum of cost and minimum of root depth among minimal cost graphs.

So, the cost of the set $\delta(T \circ H)$ is the same with the cost of the set $\delta(T) \circ H^0$. The latter cost is determined by Lemma 15. The claim of lemma concerning quantity $\theta_{p_1,s_1,\ldots,p_q,s_q}(T \circ H)$ follows immediately. □

3.5 Cost of a set of subgraphs of hyperpair

We now establish some simple relations on the cost of sets $\delta(H_k)$.

Lemma 17. *For all $l \le p_1 - 1$ and $t > 0$,*

$$C_{p_1,s_1,\ldots,p_q,s_q}(\delta(H_l)) = 0, \quad \theta_{p_1,s_1,\ldots,p_q,s_q}(H_l) = l, \quad \Omega^t_{p_1,s_1,\ldots,p_q,s_q}(H_l) = +\infty.$$

Moreover, for any $k \ge l$,

$$C_{p_1,s_1,\ldots,p_q,s_q}(\delta(H_k)) = C_{1,s_1,\ldots,p_q,s_q}(\delta(H_{k-l})),$$

$$\theta_{p_1,s_1,\ldots,p_q,s_q}(H_k) = \theta_{1,s_1,\ldots,p_q,s_q}(H_{k-l}) + l.$$

Proof. The first claim is easy to verify. Indeed, graph H_l is the only minimal cost graph in $\delta(H_l)$. The second claim can be proved via application of Lemma 16 to the graph $H_k = H_{k-l} \circ H_l$. □

Lemma 18. *Consider a connected subgraph of hyperpair H_k, which contains $l > 0$ vertices taking edges from leaves of the subgraph. Then it contains totally at most $l(k-1)+2$ vertices.*

Proof. Let $l = 1$ and t be an order of (the only) vertex connected with a leaf. Then, all that the given subgraph contains are edges (at most t) going into the vertex and an oriented chain beginning in this vertex (the length of the chain is at most $k - t$). Hence, the subgraph contains at most $k + 1$ vertices.

Note that if a connected subgraph of hyperpair H_k does not contain an edge connecting root of the hyperpair with a vertex of order $k - 1$, then it is a subgraph of hyperpair H_{k-1} (see Fig. 4).

Now we prove the induction step from $l - 1$ to l. One can represent a graph containing l vertices connected with leaves as a union of a graph with $l - 1$ such vertices and a graph with the only vertex with this property. For instance, an appropriate choice of the second graph is a vertex of depth 1 with a bunch of input edges together with a chain of edges (possibly empty) beginning in this vertex and containing only vertices not connected with leaves.

Surely, one of graphs is a subgraph of hyperpair H_{k-1}. By induction hypothesis, the first graph contains at most $(l-1)(k-1)+2$ vertices (or at most $(l-1)(k-2)+2$ in the case of subgraph of H_{k-1}). While uniting with the second graph, we add at most $k - 1$ (respectively, at most k) vertices since the resulting graph must be connected. Then the number of vertices in the entire graph is at most

$$\max\{(l-1)(k-1)+2+(k-1),\ (l-1)(k-2)+2+k\} \le l(k-1)+2.$$

□

Lemma 19. *Let $k \le s_1$. Then*

$$C_{1,s_1,\ldots,p_q,s_q}(\delta(H_k)) = 2^k - 1, \quad \theta_{1,s_1,\ldots,p_q,s_q}(H_k) = 0.$$

Moreover,

$$C_{1,s_1,\ldots,p_q,s_q}(\delta(H_{s_1+1})) = 2^{s_1+1} - 2, \quad \theta_{1,s_1,\ldots,p_q,s_q}(H_{s_1+1}) = 1$$

and for any $t \ge 1$,

$$\Omega^t_{1,s_1,\ldots,p_q,s_q}(H_k) \ge 2^k - 1 + (s_1 - k) + \sum_{i=2}^{t} s_i,$$

$$\Omega^t_{1,s_1,\ldots,p_q,s_q}(H_{s_1+1}) \ge 2^{s_1+1} - 2 + \sum_{i=2}^{t} s_i.$$

Proof. Let graph $G \in \delta(H_k)$ contain connected components $G_1, \ldots, G_j$ being not isolated vertices. The case $j = 0$ is trivial, so we proceed with the case $j \geq 1$. W.l.o.g. assume that $G_i \in \delta(H_{k-1})$ for $i > 1$. Let graph G_i contain l_i vertices connected with leaves. Thus, by Lemma 18 it contains at most $l_i(k-2)+2$ vertices in the case $i > 1$, and at most $l_1(k-1)+2$ vertices in the case $i = 1$.

Exploiting relations

$$\mu(G) = |G| - \sum_{i=1}^{j}(|G_i| - 1), \qquad C_{1,s_1,\ldots,p_q,s_q}(G_i) \geq l_i s_1,$$

we can bound the cost of G as

$$\begin{aligned} C_{1,s_1,\ldots,p_q,s_q}(G) &= \mu(G) - 1 + \sum_{i=1}^{j} C_{1,s_1,\ldots,p_q,s_q}(G_i) \geq \\ &\geq |G| - 1 + \sum_{i=1}^{j}(l_i s_1 - |G_i| + 1) \geq \\ &\geq 2^k - 1 + l_1(s_1 - k + 1) - 1 + \sum_{i=2}^{j}(l_i(s_1 - k + 2) - 1). \quad (7) \end{aligned}$$

When $k \leq s_1$, one has $C_{1,s_1,\ldots,p_q,s_q}(G) \geq 2^k - 1$. The bound $2^k - 1$ is achieved on the graph formed by all isolated vertices. So, the first claim of lemma follows. If the depth of the root of G is at least 1, then by setting $l_1 \geq 1$ in (7) we obtain $\Omega^1_{1,s_1,\ldots,p_q,s_q}(H_k) \geq 2^k - 1 + (s_1 - k)$.

For $k = s_1 + 1$, we derive a bound $C_{1,s_1,\ldots,p_q,s_q}(G) \geq 2^k - 2$, where equality is possible only when $|G_1| = l_1(k-1)+2$; hence, the root of hyperpair H_k is not an isolated vertex in graph G. The above bound is achieved on the graph formed by a bunch of edges going into the root of hyperpair and a set of isolated vertices. Consequently, $C_{1,s_1,\ldots,p_q,s_q}(\delta(H_{s_1+1})) = 2^{s_1+1} - 2$ and $\theta_{1,s_1,\ldots,p_q,s_q}(H_{s_1+1}) = 1$.

We are left to prove final relations of lemma for $t \geq 2$. Graph $G \in \delta^t_{1,p_2,\ldots,p_q}(H_k)$ contains vertices $z_2, \ldots, z_t$ such that $d_G(z_j) = 1 + \sum_{i=2}^{j} p_i$. The required relations follow: just take into account summands $c^G_{1,s_1,\ldots,p_q,s_q}(z_j, j) = s_j$ in the cost of the graph. □

Lemma 20. *Let $p_1 \leq k < p_1 + s_1$. Then*

$$C_{p_1,s_1,\ldots,p_q,s_q}(\delta(H_k)) = 2^{k-p_1+1} - 1, \qquad \theta_{p_1,s_1,\ldots,p_q,s_q}(H_k) = p_1 - 1.$$

Let $k \geq p_1 + s_1$. Then

$$C_{p_1,s_1,\ldots,p_q,s_q}(\delta(H_k)) = 2^{k-p_1-s_1+1}(2^{s_1} - 1) + C_{p_2,s_2,\ldots,p_q,s_q}(\delta(H_{k-p_1-s_1})),$$

$$\theta_{p_1,s_1,\ldots,p_q,s_q}(H_k) = p_1 + \theta_{p_2,s_2,\ldots,p_q,s_q}(H_{k-p_1-s_1}).$$

Proof. In the first case, consider hyperpair H_k as a composition $H_{k-p_1+1} \circ H_{p_1-1}$. In the second case, consider it as a composition $H_{k-p_1-s_1} \circ H_{s_1+1} \circ H_{p_1-1}$. Next, apply Lemma 16 exploiting relations of Lemmas 17 and 19. □

Let us summarize the above series of lemmas.

Lemma 21. *Let $k = \sum_{i=1}^{t}(p_i+s_i)+k'$ and either $k' < (p_{t+1}+s_{t+1})$ or $t = q$. Then*

$$C_{p_1,s_1,\ldots,p_q,s_q}(\delta(H_k)) = \sum_{t'=1}^{t} 2^{k'+1+\sum_{i=t'+1}^{t}(p_i+s_i)}(2^{s_{t'}}-1)+ \\ + \begin{cases} 0, & k' < p_{t+1} \\ 2^{k'-p_{t+1}+1}-1, & k' \geq p_{t+1} \end{cases},$$

$$\theta_{p_1,s_1,\ldots,p_q,s_q}(H_k) = \sum_{i=1}^{t} p_i + \begin{cases} k', & k' < p_{t+1} \\ p_{t+1}-1, & k' \geq p_{t+1} \end{cases}.$$

In addition, there exists a graph H_k^0 of minimal cost in $\delta(H_k)$ with root z satisfying condition

$$C^{H_k^0}_{p_1,s_1,\ldots,p_q,s_q}(z) = \sum_{i=1}^{t} s_i, \qquad d_{H_k^0}(z) = \theta_{p_1,s_1,\ldots,p_q,s_q}(H_k).$$

Proof. Apply Lemma 20 while possible. Graph H_k^0 has a form of (a multiple) composition of graphs of minimal costs produced in Lemmas 17 and 19. □

One can easily deduce that the proven relation for the cost can be rewritten in a more compact form.

Corollary 2. *Define $(k+1)$-bit number N as*

$$N = \underbrace{0\ldots0}_{p_1}\,\underbrace{1\ldots1}_{s_1}\,\underbrace{0\ldots0}_{p_2}\ldots$$

Then

$$C_{p_1,s_1,\ldots,p_q,s_q}(\delta(H_k)) = N.$$

3.6 Optimality of hyperpairs

To proceed, we need the following extension of Lemma 14.

Lemma 22. *Suppose that a graph $G \in \Delta$ contains a subgraph $W = H \circ F$ with root z and G contains no edges connecting a vertex from $W \setminus \{z\}$ and a vertex from $G \setminus W$. Let $H' \in \Delta$, $|H'| = |H|$, $W' = H' \circ F$ and graph G' be obtained from G via replacement of subgraph W by the graph W' (the root z' of W' must be superposed with the vertex z). Denote by z_F the main root of F. Suppose $d_F(z_F) = d + \sum_{i=1}^{t-1} p_i \in M_{t-1}(p_1, \ldots, p_q)$ and $C^F_{p_1,s_1,\ldots,p_q,s_q}(z_F) = \sum_{i=1}^{t-1} s_i$.*

Set $(p'_1, s'_1, \ldots, p'_{q'}, s'_{q'}) = (p_t - d, s_t, \ldots, p_q, s_q)$. Denote by z_H and z'_H main roots of graphs H and H' respectively. Suppose that $d_H(z_H) \in M_\tau(p'_1, \ldots, p'_{q'})$, $d_{H'}(z'_H) \in M_{\tau'}(p'_1, \ldots, p'_{q'})$ and $C^{H'}_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z'_H) = \sum_{i=1}^{\tau'} s'_i$.

Suppose also that

$$\begin{cases} C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H') < C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H), & d_{H'}(z'_H) > d_H(z_H) \\ C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H') + \sum_{\tau'+1}^{\tau} s'_i \le C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H), & d_{H'}(z'_H) \le d_H(z_H) \end{cases}.$$

Then one can remove some edges from G' in an oriented chain beginning in vertex z so that the cost of the resulting graph G'' satisfies inequality

$$C_{p_1,s_1,\ldots,p_q,s_q}(G'') \le C_{p_1,s_1,\ldots,p_q,s_q}(G).$$

Proof. Our goal is to reduce the present lemma to Lemma 14. Consider a change $A_2 - A_1$ of the cost of vertex z together with the cost of subgraph W inside graph G after replacement of W by W':

$$A_1 = \left(C^G_{p_1,s_1,\ldots,p_q,s_q}(z) - C^W_{p_1,s_1,\ldots,p_q,s_q}(z)\right) + C_{p_1,s_1,\ldots,p_q,s_q}(W),$$

$$A_2 = \left(C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z) - C^{W'}_{p_1,s_1,\ldots,p_q,s_q}(z')\right) + C_{p_1,s_1,\ldots,p_q,s_q}(W').$$

By conditions of lemma for all $i < t$,

$$c^G_{p_1,s_1,\ldots,p_q,s_q}(z,i) = c^W_{p_1,s_1,\ldots,p_q,s_q}(z,i) = c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z,i) = c^{W'}_{p_1,s_1,\ldots,p_q,s_q}(z',i) = s_i.$$

Moreover, it follows from Lemma 15 that

$$C_{p_1,s_1,\ldots,p_q,s_q}(W) - C_{p_1,s_1,\ldots,p_q,s_q}(W') = C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H) - C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H').$$

Thus, $A_1 - A_2 = A'_1 - A'_2$, where

$$A'_1 = \left(\sum_{i \ge t} c^G_{p_1,s_1,\ldots,p_q,s_q}(z,i) - C^H_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z_H)\right) + C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H),$$

$$A'_2 = \left(\sum_{i \geq t} c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z,i) - C^{H'}_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z'_H) \right) + C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H').$$

Basing on the latter relation the proof can be proceeded with the repeating of argument of the proof of Lemma 14 (this argument in the considered case is suitable up to some re-notation). □

Lemma 23. $C_{p_1,s_1,\ldots,p_q,s_q}(\delta(T_k)) = C_{p_1,s_1,\ldots,p_q,s_q}(\delta(H_k))$.

Proof. We will show that an arbitrary graph $G \in \delta(T_k)$ can be transformed to a graph $G' \in \delta(H_k)$ with no larger cost. Recall that condition $G \in \delta(T_k) \setminus \delta(H_k)$ implies that G contains wrong edges, i.e. edges from vertices with greater order to vertices with smaller order.

To characterize the "wrong" of a graph $G \subset T_k$, i.e. the property $G \not\subset H_k$, we introduce a numeric quantity $e(G)$ defined as follows. Let $\rho = (v, v')$ be an edge of graph G. Assign $e(\rho) = 0$ if ρ is right, and assign $e(\rho)$ as the difference of orders of vertices v and v' in graph T_k if ρ is wrong. Next, define $e(G) = \sum_{\rho \in G} e(\rho)$. Particularly, $e(G) = 0$ if $G \subset H_k$ and $e(G) > 0$ otherwise.

Thus, to prove the lemma it suffices to obtain a transformation of a graph $G \in \delta(T_k) \setminus \delta(H_k)$ that decreases $e(G)$ and does not increase the graph cost.

The proof strategy is to choose an appropriate wrong edge ρ in an arbitrary graph $G \in \delta(T_k) \setminus \delta(H_k)$ and perform a transformation which either removes ρ or redirects it to a vertex with greater order and which does not increase the cost and does not insert new wrong edges.

Let vertex z' have minimal order j' among vertices of graph G emitting wrong edges. Denote by $\rho = (z', z)$ a (wrong) edge in the question. Let j be the order of vertex z. Denote by z^* the vertex taking right edge from z in graph T_k (denote that edge by ρ_1). Note that $\rho^* = (z', z^*) \in T_k$ by definition of T_k.

Denote by H_z and H_{z^*} intersections of graph G with subgraphs T_j of graph T_k with roots z and z^* respectively. All these subgraphs are uniquely defined, see above in subsection 3.3. The introduced notation and a suitable fragment of graph G are illustrated by Fig. 6.

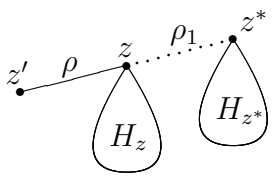


Fig. 6

Note that $H_z, H_{z^*} \in \delta(H_j)$ since all inner vertices of H_z and H_{z^*} have orders smaller than j'. Therefore, the fragment of graph G on Fig. 6 can be connected with the rest of graph G only via vertices z' and z^*.

Let $j = \sum_{i=1}^{r-1}(p_i + s_i) + a$, where $0 \le a < p_r + s_r$. Represent graph H_j as a composition $H_l \circ H_{j_{2r-1}} \circ \ldots \circ H_{j_2} \circ H_{j_1}$, where for $i < r$ we set $j_{2i-1} = p_i - 1$ and $j_{2i} = s_i + 1$; $j_{2r-1} = \min\{p_r - 1, a\}$, $l = a - j_{2r-1}$. By the construction, $0 \le l \le s_r$.

With the use of Lemma 22 we are going to show that subgraphs H_z and H_{z^*} can be replaced by graphs from $\delta(H_l) \circ H^0_{j-l}$, where H^0_k is optimal cost and minimal root depth graph from Lemma 21 so that the cost of G will not increase. We restrict our attention to subgraph H_z (the case of subgraph H_{z^*} is analogous).

Initially, set $F = H^0_0$ and $(p'_1, s'_1, \ldots, p'_{q'}, s'_{q'}) = (p_1, s_1, \ldots, p_q, s_q)$.

Represent graph H_j as a composition $T \circ U$ of an outer graph $T = H_l \circ H_{j_{2r-1}} \circ \ldots \circ H_{j_2}$ and an inner graph $U = H_{j_1}$. Note that $H_z = H_z \circ F$. In graph H_z consider any subgraph $H \circ F$ with root z^0 (the root belongs to an outer graph) formed as an intersection of H_z with a corresponding inner subgraph of graph H_j. By Lemma 22 one can replace subgraph H by graph $H' = H^0_{j_1}$ and remove some edges depending on z^0, if necessary, so that the cost of G will not increase. Necessary conditions for Lemma 22 are provided by Lemma 17 (actually, at this first step one can use Lemma 14 instead of Lemma 22). Applying the above transformation to all inner subgraphs of H_z one finally transform H_z to a graph of form $T' \circ H' \circ F$, $T' \in \delta(T)$.

Update notation:

$$H_z := T' \circ H' \circ F, \quad F := H' \circ F, \quad p'_1 := p'_1 - j_1.$$

If $r > 1$, then proceed further. In this case, $p'_1 = 1$, $j_2 = s'_1 + 1$.

Now rewrite $H_j = T \circ U$, where $T = H_l \circ H_{j_{2r-1}} \circ \ldots \circ H_{j_3}$ and $U = H_{j_2} \circ H_{j_1}$. In graph H_z consider any subgraph $H \circ F \in \delta(U)$ with root z^0 formed as an intersection of H_z with a corresponding inner subgraph of graph H_j. Via the method of Lemma 22 replace subgraph $H \circ F$ by graph $H' \circ F$, where $H' = H^0_{j_2}$. Lemma 19 provides conditions for an application of Lemma 22. Do the same with all inner subgraphs of graph H_z. Finally, one obtains a graph of form $T' \circ H' \circ F$, $T' \in \delta(T)$, instead of H_z.

Update notation:

$$H_z := T' \circ H' \circ F, \quad F := H' \circ F, \quad (p'_1, s'_1, \ldots, p'_{q'}, s'_{q'}) := (p'_2, s'_2, \ldots, p'_{q'}, s'_{q'}).$$

Proceed in the same manner, while H_z is not from $\delta(H_l) \circ H^0_{j-l}$.

The above argument restricts us to the case $H_z = H \circ H^0_{j-l}$, $H^*_z = H^* \circ H^0_{j-l}$, where $H, H^* \in \delta(H_l)$. Set

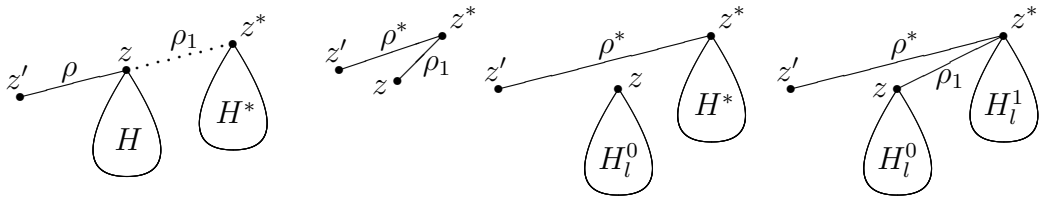
$$(p'_1, s'_1, \ldots, p'_{q'}, s'_{q'}) = (p_r - j_{2r-1}, s_r, \ldots, p_q, s_q).$$

Recall that $l \le s'_1$. Note that either $p'_1 > 0$ and $l = 0$ or $p'_1 = 1$.

Further, consider several cases.

a) Suppose $d_G(z') < d_{H^0_{j-l}}(z^0) = \theta_{p_1,s_1,\ldots,p_q,s_q}(H_{j-l}) = \sum_{i=1}^{r-1} p_i + j_{2r-1}$, where z^0 is the root of H^0_{j-l}. Since $C^{H^0_{j-l}}_{p_1,s_1,\ldots,p_q,s_q}(z^0) = \sum_{i=1}^{r-1} s_i$, one can replace edge ρ by edge ρ^* preserving the cost of graph G. The latter is due to the fact that replacement preserves the number of connected components, depths of all vertices and, consequently, costs of all vertices except z and z^*. It remains to note that costs of z and z^* are independent of presence of edges ρ and ρ^*.

From now on assume $d_G(z') \ge \theta_{p_1,s_1,\ldots,p_q,s_q}(H_{j-l})$. Next, we consider some transformations of the fragment of graph G shown on Fig. 6. Transformations involve edges ρ, ρ_1, ρ^* and outer subgraphs H and H^* of graphs H_z and H^*_z. Additionally, we may remove some edges in a chain beginning in z^* via methods of Lemmas 12 and 13. A change in the cost of graph which occurs outside the considered fragment, may be estimated by Lemmas 12 and 13. A change inside the fragment is actually determined by a change of $(p'_1, s'_1, \ldots, p'_{q'}, s'_{q'})$-cost of a graph W represented on Fig. 7a, where we define formally the depth of vertex z' as $d = d_G(z') - \theta_{p_1,s_1,\ldots,p_q,s_q}(H_{j-l})$ (more formal explanation see below).



a) W b) W^+ $[l = 0]$ c) W^- d) $W^\times$

Fig. 7

Define

$$A = C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H) + \left(C^W_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z) - C^H_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z)\right). \qquad (8)$$

b) Let $\rho_1 \notin G$ and $A \ge C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(\delta(H_l)) + 1$. Then remove edge ρ and replace subgraph H by graph H^0_l. Increasing of the number of connected components as a result of removing an edge is compensated by the subsequent decreasing of the cost of subgraph.

c) Else, if $\rho_1 \in G$ and $A \ge C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(\delta(H_l)) + 2$, then remove edge ρ_1 via the method of Lemma 12, next remove ρ and replace subgraph H by graph H^0_l.

From now on we assume that either $\rho_1 \notin G$ and $A = C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(\delta(H_l))$ or $\rho_1 \in G$ and $A \le C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(\delta(H_l)) + 1$.

Next, we discuss several ways of transformation of graph G into graph G' derived via replacement of W by one of graphs shown on Fig. 7b–d. Any replacement causes a change of the cost of graph G which is a sum of four summands:

$$C_{p_1,s_1,\ldots,p_q,s_q}(G') - C_{p_1,s_1,\ldots,p_q,s_q}(G) = \sigma_1 + \sigma_2 + \sigma_3 + \sigma_4,$$

where σ_1 is a change of cost of vertex z together with subgraph H, σ_2 is a change of cost of vertex z^* together with subgraph H^*, σ_3 is a change of the number of connected components via possible insertion or removing of edge ρ_1, σ_4 is a change of cost of vertices in a chain beginning in z^*.

Denote by H'_z and H'_{z^*} graphs derived from subgraphs H_z and H_{z^*} of graph G after a replacement. Quantities σ_1 and σ_2 satisfy the following formulae:

$$\begin{aligned}\sigma_1 = \left(C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z) - C^{H'_z}_{p_1,s_1,\ldots,p_q,s_q}(z)\right) + C_{p_1,s_1,\ldots,p_q,s_q}(H'_z) - \\ - \left(C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z) - C^{H_z}_{p_1,s_1,\ldots,p_q,s_q}(z)\right) - C_{p_1,s_1,\ldots,p_q,s_q}(H_z) = \\ = C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H^0_l) - A,\end{aligned}$$

$$\begin{aligned}\sigma_2 = \left(C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z^*) - C^{H'_{z^*}}_{p_1,s_1,\ldots,p_q,s_q}(z^*)\right) + C_{p_1,s_1,\ldots,p_q,s_q}(H'_{z^*}) - \\ - \left(C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z^*) - C^{H_{z^*}}_{p_1,s_1,\ldots,p_q,s_q}(z^*)\right) - C_{p_1,s_1,\ldots,p_q,s_q}(H_{z^*}).\end{aligned}$$

By the condition on A we also have $\sigma_1 \in \{0, -1\}$. Evidently, $\sigma_3 \in \{0, \pm 1\}$. Note also that if vertex z^* in graph G does not have outgoing edges, then $\sigma_4 = 0$.

d) Suppose $p'_1 > 1$ and $l = 0$. In this case, graphs H and H^* are single vertices.

Consider graph G' derived from G via replacement of W by W^+, see Fig. 7b.

d.1) Let $\rho_1 \notin G$. Note that in this case $C^W_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z) = 0$. Remove an edge going out of vertex z^*, if the edge is present, via the method of Lemma 12, and replace subgraph W by W^+. It does not increase the cost since possible increasing caused by removing the edge is compensated while the replacement of W by W^+: $\sigma_1 = \sigma_2 = 0$ (as costs of vertices z and z^* remain unchanged) and $\sigma_3 = -1$.

d.2) Let $\rho_1 \in G$. In this case, $C^W_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z) \le 1$ and $\sigma_3 = 0$. It occurs that $\sigma_1 + \sigma_2 \le 0$ since

$$C^{W^+}_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z) = 0, \quad C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z^*) \le C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z^*) + C^{W}_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z).$$

d.2.1) If $\sigma_1 + \sigma_2 < 0$, then do the same as in item d.1).

d.2.2) Else, that is, if $\sigma_1 + \sigma_2 = 0$,

$$C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z^*) = C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z^*) + C^{W}_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z). \tag{9}$$

One can check that it implies $d_G(z^*), d_{G'}(z^*) \in M_t(p_1, s_1, \ldots, p_q, s_q)$ for some t. Indeed, assume the converse. By the construction, $d_G(z^*) - 1 \le d_{G'}(z^*) \le d_G(z^*)$, hence, $d_G(z^*) = d_{G'}(z^*) + 1 = \sum_{i=1}^{t} p_i$ for some t. But it follows that

$$C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z^*) \le C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z^*) - s_t + C^{W}_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z),$$

which leads us to contradiction.

Consider an arbitrary subgraph U of graph G with root z^* containing the fragment shown on Fig. 6 and which is connected with the rest of graph G only via vertex z^*. Lemma 13 allows us to replace it by graph U', derived from U via replacement of W by W^+, not increasing the cost of graph G. The lemma condition $d_U(z^*) \ge d_{U'}(z^*)$ holds since $\rho_1 \in G$. The last condition of Lemma 13 holds since costs of graphs U and U' differ only in costs of vertices z and z', or speaking formally,

$$\begin{aligned} &C_{p_1,s_1,\ldots,p_q,s_q}(U) - C_{p_1,s_1,\ldots,p_q,s_q}(U') = \\ &\quad = C^{U}_{p_1,s_1,\ldots,p_q,s_q}(z) - C^{U'}_{p_1,s_1,\ldots,p_q,s_q}(z) + C^{U}_{p_1,s_1,\ldots,p_q,s_q}(z^*) - C^{U'}_{p_1,s_1,\ldots,p_q,s_q}(z^*), \end{aligned}$$

and due to the relation

$$C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z^*) + C^{U}_{p_1,s_1,\ldots,p_q,s_q}(z) = C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z^*) + C^{U'}_{p_1,s_1,\ldots,p_q,s_q}(z)$$

provided by (9).

e) Otherwise, suppose $p'_1 = 1$.

By Lemma 19 inequality $A \le C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(\delta(H_l)) + 1$ implies either $l \ge s'_1 - 1$ or $A = C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(\delta(H_l)) + 1$ and $d_H(z) = 0$. The second possibility means $d, d_W(z) \in M_\tau(p'_1, \ldots, p'_{q'})$ for some τ.

Indeed, if $l \le s'_1 - 2$, then $d_H(z) = 0$. Otherwise, $C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H) \ge C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(\delta(H_l)) + 2$. Therefore, $C^W_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z) - C^H_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(z) \ge 1$,

where equality possible only in the case $d, d_W(z) \in M_\tau(p'_1, \ldots, p'_{q'})$ for some τ. At the same time it implies $A = C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(\delta(H_l)) + 1$.

e.1) Let $A = C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(\delta(H_l)) + 1$ and $d_H(z) = 0$. Recall that $\rho_1 \in G$.

Consider graph G' derived from G via replacement of W by W^-, see Fig. 7c. One has $\sigma_1 = -1$, $\sigma_3 = 1$. It follows from what mentioned above that $d_G(z'), d_G(z) \in M_t(p_1, \ldots, p_q)$ for some t. Then σ_2 satisfies the formula

$$\sigma_2 = C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z^*) - C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z^*) = -c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z^*, t+1) \le 0.$$

e.1.1) In the case $\sigma_2 < 0$, remove an edge going out of vertex z^*, if the edge is present, via the method of Lemma 12 and replace W by W^-.

e.1.2) If $\sigma_2 = 0$, then $d_G(z^*), d_{G'}(z^*) \in M_{t'}(p_1, \ldots, p_q)$ for some t'. With the use of Lemma 13 replace W by W^- in graph G in the same manner as in item d.2.2).

e.2) Suppose $l \ge s'_1 - 1$.

Consider graph G' derived from G via replacement of W by $W^\times$ (see Fig. 7d: graph H^1_l contains a bunch of edges going into the root and all other vertices being isolated).

In this case, $\sigma_3 \in \{0, -1\}$. To estimate σ_2, we list few relations. By the construction,

$$C_{p_1,s_1,\ldots,p_q,s_q}(H'_{z^*}) - C_{p_1,s_1,\ldots,p_q,s_q}(H_{z^*}) = C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H^1_l) - C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H^*)$$

and, as one can easily check,

$$C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H^1_l) = C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H^0_l) + (s'_1 - l).$$

Let $d_{H^*}(z^*) \in M_t(p'_1, \ldots, p'_{q'})$. By Lemma 19 for $t \ge 1$, one has

$$C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H^*) \ge C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H^1_l) + \sum_{i=2}^{t} s'_i, \tag{10}$$

and for $t = 0$ (i.e. $d_{H^*}(z^*) = 0$),

$$C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H^*) \ge C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(H^1_l) - (s'_1 - l). \tag{11}$$

Lemma 19 permits us to conclude the following. If $\sigma_1 = 0$, i.e. $A = C_{p'_1,s'_1,\ldots,p'_{q'},s'_{q'}}(\delta(H_l))$, then $l = s'_1$ and $d_W(z) \in M_1(p'_1, \ldots, p'_q)$. In the case $\sigma_1 = -1$, according to item e.1) we may assume $d_H(z) > 0$. Three situations are possible: either $d_W(z) \in M_1(p'_1, \ldots, p'_q)$, or $l = s'_1$ and $d, d_W(z) \in M_\tau(p'_1, \ldots, p'_{q'})$ for some τ, or $s'_2 = 1$, $l = s'_1$ and $d_W(z) \in M_2(p'_1, \ldots, p'_q)$.

Comparing summands of the cost of vertex z^* in graphs G and G', we obtain the following bound valid in all four cases:

$$C^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z^*) \le \sum_{i=1}^{r-1} s_i + s'_1 + \sum_{i=2}^{t} s'_i + \sum_{i\ge r+t} c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z^*,i) \le$$

$$\le \sum_{i=1}^{r-1} s_i + C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z^*) - C^{H_{z^*}}_{p_1,s_1,\ldots,p_q,s_q}(z^*) + s'_1 + \sum_{i=2}^{t} s'_i =$$

$$= C^{G}_{p_1,s_1,\ldots,p_q,s_q}(z^*) - C^{H_{z^*}}_{p_1,s_1,\ldots,p_q,s_q}(z^*) + C^{H'_{z^*}}_{p_1,s_1,\ldots,p_q,s_q}(z^*) + \sum_{i=2}^{t} s'_i. \quad (12)$$

Taking into account (10), (11) we deduce from (12) that $\sigma_2 \le s'_1 - l$ in the former three cases and $\sigma_2 \le 0$ in the latter case (when $\sigma_1 = -1$, $s'_2 = 1$, $l = s'_1$ and $d_W(z) \in M_2(p'_1,\ldots,p'_q)$).

Consequently, $\sigma_1+\sigma_2+\sigma_3 \le 0$, with equality possible only if $\sigma_2 = s'_1 - l = -\sigma_1$ and $\sigma_3 = 0$. Latter equalities imply $\rho_1 \in G$ and either $\sigma_1 = 0$ or $\sigma_1 = -1$ and $\tau = 1$.

e.2.1) Let $\sigma_1+\sigma_2+\sigma_3 < 0$. Remove an edge going out of vertex z^*, if the edge is present, via the method of Lemma 12 and replace W by $W^{\times}$.

e.2.2) Let $\sigma_1+\sigma_2+\sigma_3 = 0$, that is, $\sigma_2 = s'_1 - l = -\sigma_1$ and $\sigma_3 = 0$.

Equality $\sigma_2 = s'_1 - l$ implies that inequality (12) turns into equality and further that $d_{G'}(z^*) \ge \sum_{i=1}^{r+t-1} p_i$ and $c^{G}_{p_1,s_1,\ldots,p_q,s_q}(z^*,i) = c^{G'}_{p_1,s_1,\ldots,p_q,s_q}(z^*,i)$ for any $i \ge r+t$. Thus, $d_G(z^*), d_{G'}(z^*) \in M_{t'}(p_1,\ldots,p_q)$ for some t'.

In this case, replace W by $W^{\times}$ in graph G via the method of Lemma 13. Lemma 13 is applied in the same manner as in item d.2.2). □

The proven lemma together with corollaries 1 and 2 immediately implies the main Lemma 3.

3.7 Final of the proof

Theorem 1. $L(2^n) \ge 3.5 \cdot 2^n - (8.5 + 3.5(n \bmod 2))2^{\lfloor n/2 \rfloor} + n + 5$.

Proof. It follows from Lemma 1 that a minimal circuit S_{2^n} has a form shown on Fig. 2. It contains a similar subcircuit $S_{2^{n-1}}$ which implements a set of prefix sums of variables $x_{2^{n-1}+1},\ldots,x_{2^n}$ with minimal depth $n-1$, and it also contains a subcircuit $S^1_{2^{n-1}}$ which implements a set of prefix sums of variables $x_1,\ldots,x_{2^{n-1}}$ with depth n, and, in addition, it contains 2^{n-1} output gates. So,

$$L(2^n) \ge L(2^{n-1}) + L\left(S^1_{2^{n-1}}\right) + 2^{n-1}.$$

Subcircuit $S^1_{2^{n-1}}$ contains $2^{n-1}-1$ output gates and $2^{n-1}-n$ skeleton gates. It remains to bound the number of extra gates in the subcircuit. Exploiting Lemma 3 we will show that the number is at least the cardinality of the set

$$\{(N,R,k) \mid N < 2^k,\ N \text{ is odd},\ R < 2^{n-2k-1},\ R \text{ is not a power of } 2\} \cap \mathbb{N}^3. \tag{13}$$

We apply Lemma 3 subsequently increasing parameter k. Let $k=1$. Then for an appropriate choice of parameters $N=1$ (other values are impossible in this case) and R the lemma provides an extra gate with the right end of label in a suitable interval of two values.

Further, each triple $(N = 2N' + n_0, R, k > 1)$, where $n_0 \in \{0, 1\}$, satisfying conditions of Lemma 3, informs us about presence of $2N'$ extra gates with right ends of labels from interval $J_{N,R,k}$ (see (3)) being accounted earlier via triples with less values of the first parameter, and in the case $n_0 = 1$, it reveals one more extra gate with the right end of label from the considered interval. Indeed, each of triples $(N', R' = n_0 2^{n-2k-2} + 2R, k-1)$ and $(N', R'+1, k-1)$ counts N' extra gates in the corresponding intervals $J_{N',R',k-1}$ and $J_{N',R'+1,k-1}$. The union of these intervals is $J_{N,R,k}$.

Hence, we established a bijection between triples (N,R,k) with odd N's and a subset of extra gates of circuit $S^1_{2^{n-1}}$. Thus, the problem is reduced to computation of the cardinality of the set (13).

Clearly, a given k allows 2^{k-1} choices of an odd N and independently $2^{n-2k-1} - n + 2k$ choices of the parameter R, where we assume $k < \lfloor n/2 \rfloor$. As a consequence, the number of extra gates in subcircuit $S^1_{2^{n-1}}$ is bounded from below by

$$\begin{aligned}
&\sum_{k=1}^{\lfloor n/2 \rfloor - 1} 2^{k-1}\left(2^{n-2k-1} - n + 2k\right) = \\
&\qquad = \sum_{k=1}^{\lfloor n/2 \rfloor - 1} 2^{n-k-2} - n \sum_{k=1}^{\lfloor n/2 \rfloor - 1} 2^{k-1} + \sum_{k=1}^{\lfloor n/2 \rfloor - 1} k2^k = \\
&= \left(2^{n-2} - 2^{n-\lfloor n/2 \rfloor - 1}\right) - n\left(2^{\lfloor n/2 \rfloor - 1} - 1\right) + (\lfloor n/2 \rfloor - 2)2^{\lfloor n/2 \rfloor} + 2 = \\
&\qquad = 2^{n-2} - (2.5 + (n \bmod 2))2^{\lfloor n/2 \rfloor} + n + 2.
\end{aligned}$$

Therefore, we are given the following recurrence for $L(2^n)$:

$$L(2^n) \geq L(2^{n-1}) + 3.5 \cdot 2^{n-1} - (2.5 + (n \bmod 2))2^{\lfloor n/2 \rfloor} + 1. \tag{14}$$

Evidently, $L(1) = 0$, so the statement of the theorem holds for $n = 0$.

Let us proceed with induction step.

$$L(2^n) \geq 3.5 \cdot 2^{n-1} - (12 - 3.5(n \bmod 2))2^{\lceil n/2 \rceil - 1} + n + 4 + \\ + 3.5 \cdot 2^{n-1} - (2.5 + (n \bmod 2))2^{\lfloor n/2 \rfloor} + 1 = \\ = 3.5 \cdot 2^n - (12 - 3.5(n \bmod 2))2^{\lceil n/2 \rceil - 1} - (2.5 + (n \bmod 2))2^{\lfloor n/2 \rfloor} + n + 5.$$

The identity

$$(12 - 3.5(n \bmod 2))2^{\lceil n/2 \rceil - 1} = (6 + 2.5(n \bmod 2))2^{\lfloor n/2 \rfloor}$$

is easy to verify and it completes the proof of the induction step and of the entire theorem. □

4 Upper bound

Now we show that the bound of Theorem 1 is tight. For this, we propose an optimal way of constructing of circuits $S^1_{2^k}$, which is, in fact, a modification of method [3].

Denote by Q_{2^k} a minimal (in fact, free of extra gates) 2^k-input prefix circuit of complexity $2^{k+1} - k - 2$ and depth $2k - 2$, which implements the longest prefix $x_1 \circ \ldots \circ x_{2^k}$ with depth k. Such circuit is easy to construct, see [7, 3].

For $i = 1, \ldots, \lceil n/2 \rceil$ set $l_i = 2^n - 2^{n+1-i}$ and $l_{\lceil n/2 \rceil + 1} = 2^n$. Additionally, for $i = 1, \ldots, \lceil n/2 \rceil - 1$, set $m_i = n - 2i$ and $m_{\lceil n/2 \rceil} = 1 - (n \bmod 2)$. Define a family of circuits $S^1_{2^n}$ according to Fig. 8–9.

Some comments are required. Circuit $S^1_{2^n}$ (Fig. 8) contains $\lceil n/2 \rceil$ subcircuits denoted by $P_{i,n}$. Subcircuit $P_{i,n}$ contains outputs of circuit $S^1_{2^n}$ with right ends of labels from $l_i + 1$ to l_{i+1}. Each subcircuit also implements a function $\beta_i = x_{l_i+1} \circ \ldots \circ x_{l_{i+1}}$ utilized by subcircuits $P_{j,n}$, where $j > i$.

If $i > 1$, then the subcircuit $P_{i,n}$ takes as inputs functions $\beta_1, \ldots, \beta_{i-1}$ and $\gamma_{i-1} = x_1 \circ \ldots \circ x_{l_i}$, not counting variable inputs.

Variable inputs of subcircuit $P_{i,n}$ are divided into groups: each of first two groups includes 2^{i-1} inputs each, any other group includes 2^i inputs (see Fig. 9). Circuits $Q_{2^{i-1}}$ and Q_{2^i} are involved to compute prefix sums in every group. These sums are denoted by $\alpha_{i,j,k}$, where

$$\alpha_{i,j,k} = \begin{cases} x_{l_i+2^{i-1}+1} \circ \ldots \circ x_{l_i+k}, & j = 1,\ k > 2^{i-1} \\ x_{l_i+(j-1)2^i+1} \circ \ldots \circ x_{l_i+(j-1)2^i+k}, & \text{otherwise} \end{cases}.$$

Each function $\alpha_{i,j,k}$ is implemented with the depth at most $2i - 2 \leq n$.

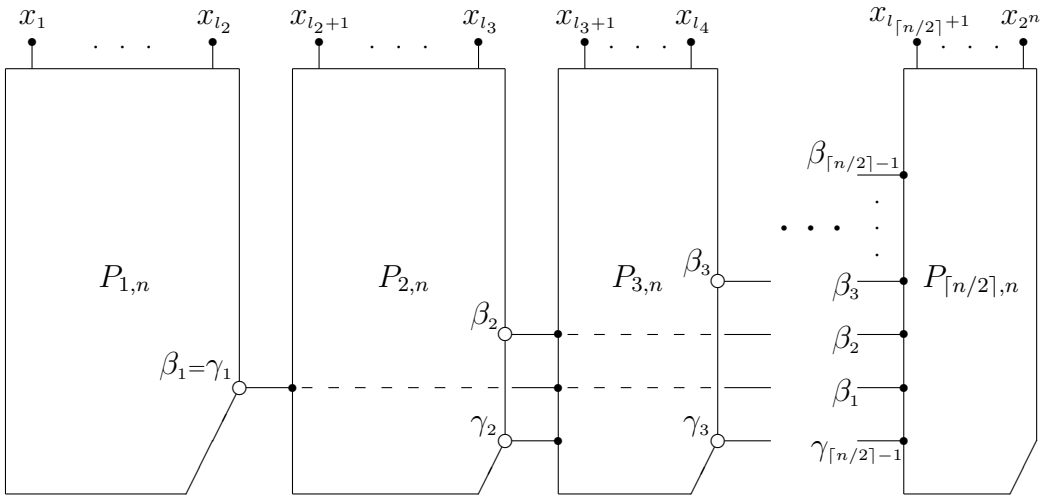


Fig. 8. Structure of circuit $S^1_{2^n}$

Outputs of gates implementing functions $\alpha_{i,1,2^{i-1}} \circ \alpha_{i,1,2^i}$ and $\alpha_{i,j,2^i}$, where $j > 1$ (all gates have depth i), are connected with inputs of the subcircuit $S^1_{2^{m_i}}$. The longest prefix output of the subcircuit implements function β_i. Thus, for any $i < \lceil n/2 \rceil$, function β_i is computed with the depth at most $i + m_i = n - i$, and function $\beta_{\lceil n/2 \rceil}$ is computed with the depth $\lceil n/2 \rceil + m_{\lceil n/2 \rceil} = n - (\lceil n/2 \rceil - 1)$.

Output of the gate implementing function $\alpha_{i,0} = \alpha_{i,1,2^{i-1}}$ and outputs $\alpha_{i,1}, \ldots, \alpha_{i,2^{m_i}}$ of the subcircuit $S^1_{2^{m_i}}$ are connected with inputs of subcircuit W_i. Subcircuit W_i computes sums $\alpha_{i,k} \circ \beta_1 \circ \ldots \circ \beta_{i-1}$ including γ_i (when $k = 2^{m_i}$) with the depth at most n. Clearly, outputs of subcircuit W_i implement sums $x_1 \circ \ldots \circ x_k$, where $k \in \{l_i + 2^{i-1}\} \cup \{l_i + j2^i \mid j = 1, \ldots, 2^{m_i}\}$.

Consequently, depth of any subcircuit $P_{i,n}$ is at most $n + 1$.

Lemma 24. *The complexity of circuit $S^1_{2^n}$ is*

$$L(S^1_{2^n}) = 5 \cdot 2^{n-1} - (3.5 - (n \bmod 2))2^{\lceil n/2 \rceil} + 1.$$

Proof. Calculate the complexity of $P_{i,n}$:

$$\begin{aligned} L(P_{i,n}) &= L(S^1_{2^{m_i}}) + 2L(Q_{2^{i-1}}) + (2^{m_i} - 1)L(Q_{2^i}) + 1 + \\ &\quad + (2^{m_i} + 1)(i - 1) + 2(2^{i-1} - 1) + (2^{m_i} - 1)(2^i - 1) = \\ &= L(S^1_{2^{m_i}}) + 2(2^i - i - 1) + (2^{m_i} - 1)(2^{i+1} - i - 2) + \\ &\quad + (2^{m_i} + 1)(i - 1) + 2^{m_i}(2^i - 1) = \\ &= L(S^1_{2^{m_i}}) + 2^{m_i}(3 \cdot 2^i - 4) - 1. \end{aligned}$$

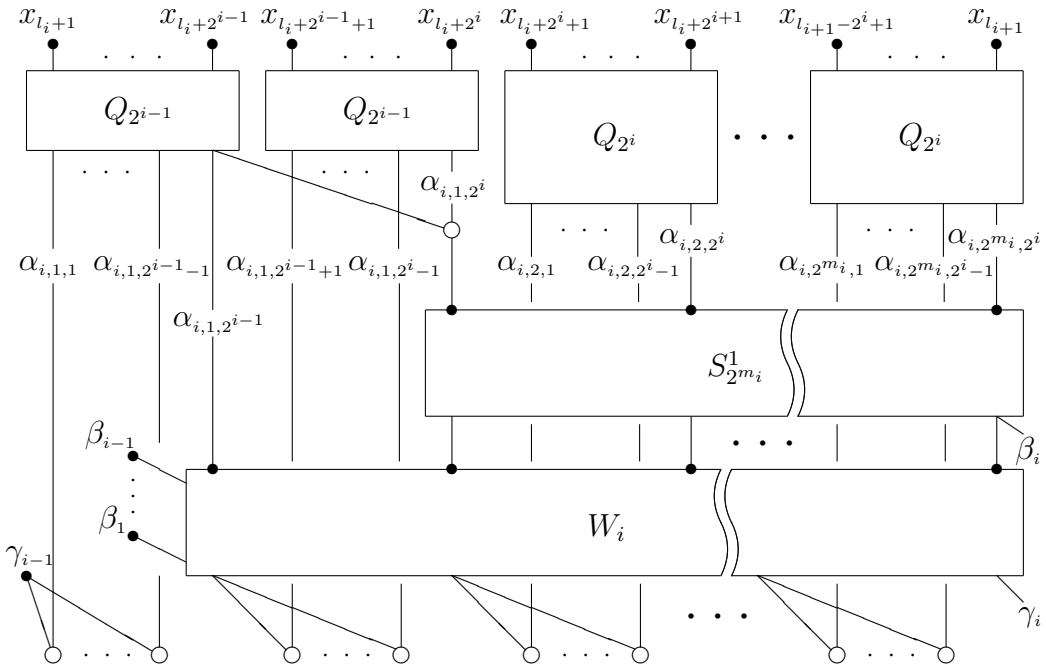


Fig. 9. Structure of circuit $P_{i,n}$

Regarding values $L(S^1_1) = 0$ and $L(S^1_2) = 1$ as a base of induction, let us prove the induction step.

$$L(S^1_{2^n}) = \sum_{i=1}^{\lceil n/2 \rceil} L(P_{i,n}) = \sum_{i=1}^{\lceil n/2 \rceil} \left(L(S^1_{2^{m_i}}) + 2^{m_i}(3 \cdot 2^i - 4) - 1 \right) =$$

$$= \sum_{i=1}^{\lceil n/2 \rceil} \left(5 \cdot 2^{m_i - 1} - (3.5 - (m_i \bmod 2)) 2^{\lceil m_i/2 \rceil} + 2^{m_i}(3 \cdot 2^i - 4) \right) =$$

$$= \sum_{i=1}^{\lceil n/2 \rceil} \left(3(2^{m_i+i} - 2^{m_i-1}) - (3.5 - (m_i \bmod 2)) 2^{\lceil m_i/2 \rceil} \right).$$

Set $m_i = n - 2i$ and calculate the sum of first $\lceil n/2 \rceil - 1$ summands:

$$\Sigma_1 = \sum_{i=1}^{\lceil n/2 \rceil - 1} \left(3(2^{m_i+i} - 2^{m_i-1}) - (3.5 - (m_i \bmod 2))2^{\lceil m_i/2 \rceil}\right) =$$
$$= \sum_{i=1}^{\lceil n/2 \rceil - 1} 3(2^{n-i} - 2^{n-2i-1}) - \sum_{i=1}^{\lceil n/2 \rceil - 1} (3.5 - (n \bmod 2))2^{\lceil n/2 \rceil - i} =$$
$$= 3(2^n - 2^{\lfloor n/2 \rfloor + 1}) - \left(2^{n-1} - 2^{1-(n \bmod 2)}\right) - (3.5 - (n \bmod 2))(2^{\lceil n/2 \rceil} - 2) =$$
$$= 5 \cdot 2^{n-1} - (3.5 - (n \bmod 2))2^{\lceil n/2 \rceil} - 3 \cdot 2^{\lfloor n/2 \rfloor + 1} + 9 - 3(n \bmod 2).$$

Given $m_{\lceil n/2 \rceil} = 1 - (n \bmod 2)$, the latter summand of the initial sum can be computed as

$$\Sigma_2 = 3\left(2^{\lceil n/2 \rceil + 1 - (n \bmod 2)} - 2^{-(n \bmod 2)}\right) - (2.5 + (n \bmod 2))2^{1-(n \bmod 2)} =$$
$$= 3 \cdot 2^{\lfloor n/2 \rfloor + 1} - (4 + (n \bmod 2))2^{1-(n \bmod 2)} = 3 \cdot 2^{\lfloor n/2 \rfloor + 1} - 8 + 3(n \bmod 2).$$

Summing up Σ_1 and Σ_2 one obtains the required complexity value. □

Theorem 2. $L(2^n) \leq 3.5 \cdot 2^n - (8.5 + 3.5(n \bmod 2))2^{\lfloor n/2 \rfloor} + n + 5$.

Proof. Make use of the corollary of Lemma 1 (see Fig. 2):

$$L(2^n) \leq L(2^{n-1}) + L(S^1_{2^{n-1}}) + 2^{n-1}.$$

With the above circuits $S^1_{2^k}$ satisfying Lemma 24, one has a recurrence

$$L(2^n) \leq L(2^{n-1}) + 3.5 \cdot 2^{n-1} - (2.5 + (n \bmod 2))2^{\lfloor n/2 \rfloor} + 1.$$

It is solved as (14) up to the inequality sign. □

Theorems 1 and 2 together establish tight complexity of a minimal 2^n-input prefix circuit of depth n. Ladner—Fischer circuits [7] appear to be non-minimal for $n \geq 6$. Recently, a sequence of 2^n-input prefix circuits of depth n and complexity $L(2^n)$ (at least for $n \leq 25$) was discovered by Sheeran [12, 13] via computer programming.

Extracting from the constructed circuit a subcircuit depending on first m variables, where $2^{n-1} < m \leq 2^n$, one obtains

Corollary 3. *For any m, $L(m) \leq (3.5 - o(1))m$.*

5 Almost minimal depth circuits

Theorem 3. *For* $1 \le k \le n-2$,

$$L'(2^n, k) = \left(2 + 2^{-k}\right) 2^n - (5 + 2((n-k) \bmod 2))2^{\lfloor (n-k)/2 \rfloor} - k + 2.$$

Proof. As follows from Lemma 1, to prove a lower bound it suffices to consider a subcircuit of circuit $S_{2^{n+k}}$, depending on first 2^n variables.

In the case $k = 1$, upper bound is achieved on the circuit $S^1_{2^n}$ described in §4. Exploiting this circuit and method [7] we obtain minimal circuits $S^k_{2^n}$ for other values of k (see Fig. 10). □

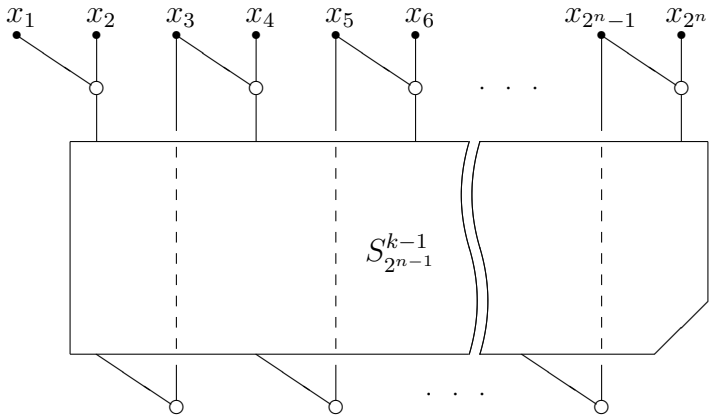


Fig. 10. Structure of circuit $S^k_{2^n}$

For an arbitrary m an upper bound can be obtained in a similar way as in Corollary 3.

Corollary 4. *For any* m, k, *where* $1 \le k \le \lceil \log_2 m \rceil - 2$, *with* $m \to \infty$,

$$L'(m, k) \le (2 + 2^{-k} - o(1))m.$$

6 Modulo 2 prefix circuits

We will show in the present paragraph that under some additional assumptions on the operation "$\circ$" one can decrease the complexity of a parallel prefix circuit as compared with the general case. As an example, we consider an associative operation $\oplus$ with the axiom $x \oplus y \oplus y = x$. If $\oplus$ is a group operation, then it can be interpreted as addition modulo 2.

The advantage of operation $\oplus$ is a possibility to compute a sum $x_i \oplus \ldots \oplus x_j$ by the formula

$$x_i \oplus \ldots \oplus x_j = (x_i \oplus \ldots \oplus x_{j+k}) \oplus (x_{j+1} \oplus \ldots \oplus x_{j+k}).$$

We construct a 2^n-input prefix circuit Λ_{2^n} of depth n over basis $\{\oplus\}$ according to Fig. 2, replacing circuit $S^1_{2^n}$ by a circuit $\Lambda^1_{2^n}$. The structure of circuit $\Lambda^1_{2^n}$ is generally analogous to the structure of circuit $S^1_{2^n}$ described in §4. Distinction is in the following.

Circuits Q_{2^k} are replaced by circuits Ψ_{2^k}. Circuit Ψ_{2^k} has complexity $2^{k+1}-2k-1$ and depth $k+\lceil k/2\rceil-1$. It implements sums $x_1\oplus\ldots\oplus x_i$ and $x_{2^{k-1}+i}\oplus\ldots\oplus x_{2^k}$, where $i=1,\ldots,2^{k-1}$, and also the sum $x_1\oplus\ldots\oplus x_{2^k}$ with the depth k. A way to construct such a circuit is shown on Fig. 11.

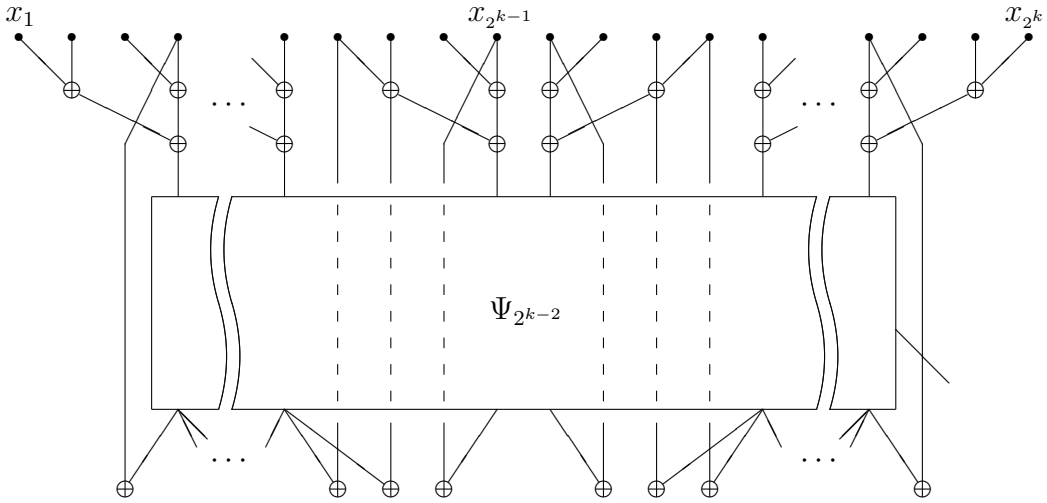


Fig. 11. Structure of circuit Ψ_{2^k}

For $i=1,\ldots,n-\lceil n/3\rceil$, set $\lambda_i=2^n-2^{n+1-i}$, and also set $\lambda_{n-\lceil n/3\rceil+1}=2^n$. Circuit $\Lambda^1_{2^n}$ consists of subcircuits $\Pi_{i,n}$, where $i=1,\ldots,n-\lceil n/3\rceil$, which are similar to circuits $P_{i,n}$ (see Fig. 8), and which are connected similarly.

Subcircuit $\Pi_{i,n}$ contains output gates of circuit $\Lambda^1_{2^n}$ with right ends of labels in the interval from λ_i+1 to λ_{i+1}. Subcircuit $\Pi_{i,n}$ also computes a sum $\beta_i=x_{\lambda_i+1}\oplus\ldots\oplus x_{\lambda_{i+1}}$. If $i>1$, then subcircuit $\Pi_{i,n}$ takes as inputs functions $\beta_1,\ldots,\beta_{i-1}$ and $\gamma_{i-1}=x_1\oplus\ldots\oplus x_{\lambda_i}$, not counting variable inputs.

A structure of subcircuit $\Pi_{i,n}$ resembles the structure of subcircuit $P_{i,n}$ (see Fig. 9) with minor differences. Variable inputs are divided into groups: each of first two groups contains $2^{\lceil i/2\rceil}$ inputs, any other group contains $2^{\lceil i/2\rceil+1}$ inputs. Every group is supplied with a suitable circuit from the family $\{\Psi_{2^k}\}$. Outputs of these circuits, which implement longest prefixes, are connected to inputs of subcircuit $\Lambda^1_{2^{\mu_i}}$, where $\mu_i=n-i-\lceil i/2\rceil-1$ for $i<n-\lceil n/3\rceil$, and $\mu_{n-\lceil n/3\rceil}=2\lceil n/3\rceil+\lfloor n/3\rfloor-n$.

The last difference between circuits $\Pi_{i,n}$ and $P_{i,n}$ concerns a final level where output sums $x_1\oplus\ldots\oplus x_j$ are computed (it corresponds to bunches of

gates at the bottom of Fig. 9). If variable x_j is an input of subcircuit Ψ_{2^k}, then a sum $x_1 \oplus \ldots \oplus x_j$ is computed as (denote $r = (j \bmod 2^k)$)

$$\begin{cases} (x_1 \oplus \ldots \oplus x_{j-r}) \oplus (x_{j-r+1} \oplus \ldots \oplus x_j), & r \le 2^{k-1} \\ (x_1 \oplus \ldots \oplus x_{j+2^k-r}) \oplus (x_{j+1} \oplus \ldots \oplus x_{j+2^k-r}), & r > 2^{k-1} \end{cases},$$

where the second "summand" is computed by a subcircuit Ψ_{2^k}.

Lemma 25. *The complexity of circuit $\Lambda^1_{2^n}$ is*

$$L(\Lambda^1_{2^n}) = 2\tfrac{3}{11} \cdot 2^n - \sigma_n,$$

where σ_n is determined by a recurrence

$$\sigma_n = 2\sigma_{n-3} + \sigma_{n-4} + 1$$

with initial conditions

$$\sigma_0 = \tfrac{25}{11}, \quad \sigma_1 = \tfrac{39}{11}, \quad \sigma_2 = \tfrac{56}{11}, \quad \sigma_3 = \tfrac{79}{11}.$$

Remark Clearly, it is possible to write down an explicit analytic formula for σ_n, though it should be cumbersome. To do this, one can assign $\sigma_n = \chi_n - 0.5$ and determine χ_n from the recurrence $\chi_n = 2\chi_{n-3} + \chi_{n-4}$ with appropriate initial conditions. The solution of the recurrence can be derived as a linear combination of powers of roots of the polynomial $x^4 - 2x - 1$. In particular, $\sigma_n \sim c\chi^n$, where $\chi = 1,3953\ldots$ is the maximal root with respect to absolute value, and $c = 2,86\ldots$

Proof. Let us calculate the complexity of circuit $\Pi_{i,n}$ for $i > 1$:

$$\begin{aligned} L(\Pi_{i,n}) &= L(\Lambda^1_{2^{\mu_i}}) + 2L(\Psi_{2^{\lceil i/2 \rceil}}) + (2^{\mu_i} - 1)L(\Psi_{\lceil i/2 \rceil + 1}) + 1 + \\ &\quad + (2^{\mu_i} + 1)(i-1) + 2\left(2^{\lceil i/2 \rceil} - 1\right) + (2^{\mu_i} - 1)\left(2^{\lceil i/2 \rceil + 1} - 1\right) = \\ &= L(\Lambda^1_{2^{\mu_i}}) + 2\left(2^{\lceil i/2 \rceil + 1} - 2\lceil i/2 \rceil - 1\right) + (2^{\mu_i} - 1)\left(2^{\lceil i/2 \rceil + 2} - 2\lceil i/2 \rceil - 3\right) + \\ &\quad + (2^{\mu_i} + 1)(i-1) + 2^{\mu_i}\left(2^{\lceil i/2 \rceil + 1} - 1\right) = \\ &= L(\Lambda^1_{2^{\mu_i}}) + 2^{\mu_i}\left(3 \cdot 2^{\lceil i/2 \rceil + 1} - (i \bmod 2) - 5\right) - (i \bmod 2). \end{aligned}$$

Complexity of circuit $\Pi_{1,n}$ is the same but less by 1 due to the absence of gate $\gamma_0 \oplus x_1$ (bottom-left on Fig. 9).

It is easy to check that $L(\Lambda^1_{2^0}) = 0$, $L(\Lambda^1_{2^1}) = 1$, $L(\Lambda^1_{2^2}) = 4$, $L(\Lambda^1_{2^3}) = 11$. Regarding these relations as a base of induction, let us prove the induction step.

For convenience of writing, we introduce notation $\omega_3(n)$ for an undetermined function depending only on $(n \bmod 3)$. By definition, for any integer k, one has $\omega_3(n) = \omega_3(n + 3k)$.

$$L(\Lambda^1_{2^n}) = \sum_{i=1}^{n-\lceil \frac{n}{3} \rceil} L(\Pi_{i,n}) =$$

$$= \sum_{i=1}^{n-\lceil \frac{n}{3} \rceil} \left(L(\Lambda^1_{2^{\mu_i}}) + 2^{\mu_i} \left(3 \cdot 2^{\lceil i/2 \rceil + 1} - (i \bmod 2) - 5 \right) - (i \bmod 2) \right) - 1 =$$

$$= \sum_{i=1}^{n-\lceil \frac{n}{3} \rceil} \left(2^{\mu_i} \left(3 \cdot 2^{\lceil i/2 \rceil + 1} - (i \bmod 2) - 2\tfrac{8}{11} \right) - \sigma_{\mu_i} - (i \bmod 2) \right) - 1.$$

Set $\mu_i = n - i - \lceil i/2 \rceil - 1$ and compute the sum of all summands except the latter:

$$\Sigma_1 = \Sigma_1^1 - \Sigma_1^2 - \Sigma_1^3 - \Sigma_1^4 - \Sigma_1^5 - 1,$$

where

$$\Sigma_1^1 = \sum_{i=1}^{n-\lceil \frac{n}{3} \rceil - 1} 3 \cdot 2^{\mu_i + \lceil i/2 \rceil + 1} = 3 \sum_{i=1}^{n-\lceil \frac{n}{3} \rceil - 1} 2^{n-i} = 3(2^n - 2^{\lceil n/3 \rceil + 1}),$$

$$\Sigma_1^2 = \sum_{i=1}^{n-\lceil \frac{n}{3} \rceil - 1} (i \bmod 2) 2^{\mu_i} = \sum_{i=1}^{n-\lceil \frac{n}{3} \rceil - 1} (i \bmod 2) 2^{n-i-\lceil i/2 \rceil - 1} =$$

$$= \sum_{j=1}^{\lfloor n/3 \rfloor} 2^{n-3j} = \tfrac{1}{7} \cdot 2^n + \omega_3(n),$$

$$\Sigma_1^3 = \sum_{i=1}^{n-\lceil \frac{n}{3} \rceil - 1} 2\tfrac{8}{11} \cdot 2^{\mu_i} = 2\tfrac{8}{11} \sum_{i=1}^{n-\lceil \frac{n}{3} \rceil - 1} 2^{n-i-\lceil i/2 \rceil - 1} =$$

$$= 2\tfrac{8}{11} \left(\sum_{j=1}^{\lfloor n/3 \rfloor} 2^{n-3j} + \sum_{j=1}^{n-\lceil \frac{n}{3} \rceil - \lfloor \frac{n}{3} \rfloor - 1} 2^{n-3j-1} \right) =$$

$$= 2\tfrac{8}{11} \left(\tfrac{1}{7} \cdot 2^n + \tfrac{1}{7} \cdot 2^{n-1} + \omega_3(n) \right) = \tfrac{45}{77} \cdot 2^n + \omega_3(n),$$

$$\Sigma_1^4 = \sum_{i=1}^{n-\lceil \frac{n}{3} \rceil - 1} \sigma_{\mu_i} = \sum_{i=1}^{n-\lceil \frac{n}{3} \rceil - 1} \sigma_{n-i-\lceil i/2 \rceil - 1}, \quad \Sigma_1^5 = \sum_{i=1}^{n-\lceil \frac{n}{3} \rceil - 1} (i \bmod 2) = \lfloor n/3 \rfloor.$$

Since $\mu_{n-\lceil n/3\rceil} = 2\lceil n/3\rceil + \lfloor n/3\rfloor - n$, the latter summand of the initial sum is

$$\Sigma_2 = 3 \cdot 2^{\mu_{n-\lceil n/3\rceil}+\lceil (n-\lceil n/3\rceil)/2\rceil+1} + \omega_3(n) = 3 \cdot 2^{\lceil n/3\rceil+1} + \omega_3(n).$$

We finally obtain

$$L(\Lambda^1_{2^n}) = \Sigma_1 + \Sigma_2 = 2\tfrac{3}{11} \cdot 2^n - n/3 - \sum_{i=1}^{n-\left\lceil \frac{n}{3}\right\rceil -1} \sigma_{n-i-\lceil i/2\rceil-1} + \psi(n \bmod 3),$$

and consequently,

$$\sigma_n = \sum_{i=1}^{n-\left\lceil \frac{n}{3}\right\rceil -1} \sigma_{n-i-\lceil i/2\rceil-1} + n/3 - \psi(n \bmod 3) =$$

$$= \sigma_{n-3}+\sigma_{n-4}+1+ \sum_{i=1}^{(n-3)-\left\lceil \frac{n-3}{3}\right\rceil -1} \sigma_{(n-3)-i-\lceil i/2\rceil-1}+\frac{n-3}{3}-\psi((n-3) \bmod 3) =$$

$$= \sigma_{n-3} + \sigma_{n-4} + 1 - L(\Lambda^1_{2^{n-3}}) + 2\tfrac{3}{11} \cdot 2^{n-3} = 2\sigma_{n-3} + \sigma_{n-4} + 1.$$

□

The proven lemma leads to the following

Theorem 4. *$L^{\oplus}(2^n) \le 3\frac{3}{11} \cdot 2^n - \tau_n$, where*

$$\tau_n = \frac{\sigma_{n+3} + \sigma_{n+2} + \sigma_{n+1} - \sigma_n - n - 7}{2}.$$

Remark Taking into account Remark after Lemma 25 we conclude that $\tau_n \sim c'\chi^n$, where $c' = 7,235\ldots$

The proof of the following corollary is analogous to that of Corollary 3.

Corollary 5. *For any m, $L^{\oplus}(m) \le \left(3\frac{3}{11} - o(1)\right) m$.*

In the case $k \ge \lceil (\log_2 m)/2\rceil - 1$, it can be easily shown that $L'^{\oplus}(m,k) = 2m - \lceil \log_2 m\rceil - 2$. The lower bound follows from the relation between the complexity and the longest prefix depth in a prefix circuit [3, 15] considered in §2. To prove an upper bound one divides all inputs in groups of 4, computes sums in each group and delivers these sums to inputs of analogous $\lceil m/4\rceil$-input circuit. Remaining prefixes can be implemented with additional depth 1 with respect to depths of outputs of the inner subcircuit.

To prove the following corollary, one can exploit Lemma 25 and the method of [7] with only difference that inputs must be divided into groups of 4.

Corollary 6. *For any m, k, where $1 \le k \le \lceil (\log_2 m)/2 \rceil - 1$, with $m \to \infty$,*

$$L'^{\oplus}(m,k) \le \left(2 + \tfrac{3}{11} \cdot 4^{1-k} - o(1)\right) m.$$

It is of interest, whether the upper bound of Theorem 2 can be improved under different assumptions on operation $\circ$. Specific operations to attract more attention are commutative operations, idempotent operations ($x \circ x = x$) and, particularly, Boolean disjunction and conjunction.

7 Notes on bounded fan-out prefix circuits

The problem of synthesis of prefix circuits with bounded fan-out is stimulated by electronics. (A restriction q on the fan-out of inputs and inner gates of a circuit is given and fan-out of output gates must not exceed $q-1$.) To design such circuits one use functional gates $\circ$ together with branching gates $\triangledown$. In the case $q = 2$, the latter type of gates is generally unavoidable in the synthesis of parallel prefix circuits.

To denote a complexity of prefix circuits with fan-out bounded by q we use notation introduced above but supplemented with subscript q.

Fich [3] investigated the complexity of parallel prefix circuits under various restrictions q. In the case $q \ge 3$, she proposed prefix circuits of minimal depth and linear complexity $O(m)$. She also proved that in the case $q = 2$ complexity is superlinear, $L_2(m) = \Theta(m \log m)$. Specifically, for $m = 2^n$ the following bounds were obtained:

$$(n + 1 - o(1))2^{n-1} \le L_2(2^n) \le (3n - 3.5 - o(1))2^{n-1}.$$

Note however, that a better upper bound is known since 1973 and is due to Kogge and Stone [6]. The complexity of the Kogge—Stone circuit is $(n - 0.5)2^n$ (including $(n-1)2^n + 1$ functional gates $\circ$). The 8-input circuit is shown on Fig. 12.

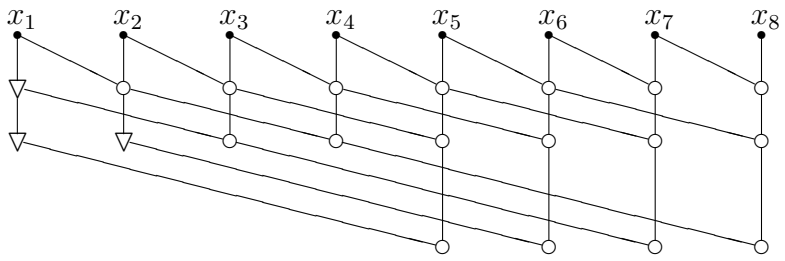


Fig. 12

Basing on the Kogge—Stone circuit one can design a 2^n-input prefix circuit of depth $n+k$ and complexity $(n-k-3)2^{n-k}+5\cdot 2^{n-1}-k$ via the method of [7] (as on Fig. 10). Therefore,

$$L_2(2^n)\le (n-0.5)2^n, \qquad L_2'(2^n,k)\le (n-k-3)2^{n-k}+5\cdot 2^{n-1}-k.$$

The second bound can be slightly improved with the use of modification of the Kogge—Stone circuit shown on Fig. 13 (its complexity is $(n-0.5)2^n$ as well, though it can be completed to a circuit with zero fan-out of outputs, which has lower complexity $(n-0.25)2^n$). Thus,

$$L_2'(2^n,k)\le (n-k-3.25)2^{n-k}+5\cdot 2^{n-1}-k. \tag{15}$$

(Details of the proof are easy to reproduce.)

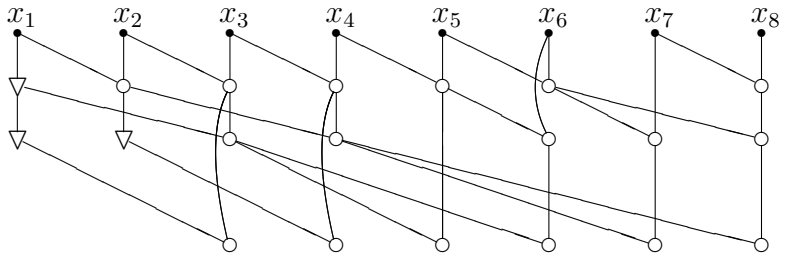


Fig. 13

For a small k the bound (15) is approximately 2 times greater than a lower bound $(n-2)2^{n-k-1}+2^n-O(n(n+k)2^{-k})$ from [3]. When $k\asymp n$ it is asymptotically 1.25 times greater than a standard lower bound 2^{n+1}. At the same time, a slightly modified construction from [15] allows to reach a bound $L_2'(2^n,n-1)\lesssim 2.3\cdot 2^n$. With the use of it one can design a circuit of complexity $(2+o(1))2^n$ and depth $(2+o(1))n$. On the whole, asymptotic behavior of functions $L_2(2^n)$ and $L_2'(2^n,k)$ still remains unclear.

The author is grateful to S. B. Gashkov and Stasys Jukna for helpful comments.

References

[1] Blelloch G. E. Prefix sums and their applications. Synthesis of parallel algorithms. San Francisco: Morgan Kaufmann, 1993, 35–60.

[2] Fich F. E. Two problems in concrete complexity: cycle detection and parallel prefix computation. IBM research report RJ 3651, 1982. (Ph.D. thesis, Univ. of California, Berkeley, 1982.)

[3] Fich F. E. New bounds for parallel prefix circuits. Proc. ACM Symp. Theory of Comput. 1983. 100–109.

[4] Jukna S. Boolean function complexity. Berlin, Heidelberg: Springer-Verlag, 2012.

[5] Knuth D. E. The art of computer programming. Vol. 4, fasc. 2. Generating all tuples and permutations. Addison–Wesley, 2005.

[6] Kogge P. M., Stone H. S. A parallel algorithm for the efficient solution of a general class of recurrence equations. IEEE Trans. on Comp. 1973. Vol. 22(8), 786–793.

[7] Ladner R. E., Fischer M. J. Parallel prefix computation. J. ACM. 1980. Vol. 27(4), 831–838.

[8] Lupanov O. B. Asymptotic bounds for the complexity of control systems. Moscow: MSU, 1984. (in Russian)

[9] Ofman Y. P. On the algorithmic complexity of discrete functions. Soviet Physics Doklady. 1963. V. 7(7), 589–591.

[10] Sergeev I. S. Some bounds on the complexity of parallel prefix circuits. Proc. X Intern. Seminar "Discrete Math. and its Appl." (Moscow, MSU, Febr. 2010). Moscow: Mech. Math. Faculty Publishing, 2010. 136–139. (in Russian)

[11] Sergeev I. S. Minimal parallel prefix circuits. Moscow University Math. Bulletin. 2011. V. 66(5), 215–218.

[12] Sheeran M. Functional and dynamic programming in the design of parallel prefix networks. Tech. report N. 2009:12. Chalmers/Göteborg Univ., 2009.

[13] Sheeran M. Functional and dynamic programming in the design of parallel prefix networks. J. Funct. Programming. 2010. Vol. 21(1), 59–114.

[14] Sklansky J. Conditional-sum addition logic. IRE Trans. Electr. Comput. 1960. EC-9, 226–231.

[15] Snir M. Depth-size trade-offs for parallel prefix computation. J. Algorithms. 1986. Vol. 4, 185–201.

[16] Zhu H., Cheng C.-K., Graham R. On the construction of zero-deficiency parallel prefix circuits with minimum depth. ACM Trans. on Design Autom. of Electr. Syst. 2006. Vol. 11(2), 387–409.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de