Depth Two Majority Circuits for Majority and List Expanders

Kazuyuki Amano[1]
Department of Computer Science, Gunma University,
1-5-1 Tenjin, Kiryu, Gunma 376-8515, Japan
amano@gunma-u.ac.jp

Abstract

Let MAJ_n denote the Boolean majority function of n input variables. In this paper, we study the construction of depth two circuits computing MAJ_n where each gate in a circuit computes MAJ_m for $m < n$.

We first give an explicit construction of depth two $\mathsf{MAJ}_{\lfloor n/2 \rfloor+2} \circ \mathsf{MAJ}_{\leq n-2}$ circuits computing MAJ_n for every $n \geq 7$ such that $n \equiv 3 \pmod 4$ where MAJ_m and $\mathsf{MAJ}_{\leq m}$ denote the majority gates that take m and at most m *distinct* inputs, respectively. A graph theoretic argument developed by Kulikov and Podolskii (STACS '17, Article No. 49) shows that there is no $\mathsf{MAJ}_{\leq n-2} \circ \mathsf{MAJ}_{n-2}$ circuit computing MAJ_n. Hence, our construction reveals that the use of a smaller fan-in gates at the bottom level is essential for the existence of such a circuit. Some computational results are also provided.

We then show that the construction of depth two $\mathsf{MAJ}_m \circ \mathsf{MAJ}_m$ circuits computing MAJ_n for $m < n$ can be translated into the construction of a newly introduced version of bipartite expander graphs which we call a *list expander*. Intuitively, a list expander is a c-leftregular bipartite graph such that for a given $d < c$, every d-leftregular subgraph of the original graph has a certain expansion property. We formalize this connection and verify that, with high probability, a random bipartite graph is a list expander of certain parameters. However, the parameters obtained are not sufficient to give us a $\mathsf{MAJ}_{n-c} \circ \mathsf{MAJ}_{n-c}$ circuit computing MAJ_n for a large constant c.

2012 ACM Subject Classification Theory of computation → Circuit complexity

Keywords and phrases Boolean function, majority function, constant depth circuit, expander graph

Digital Object Identifier 10.4230/LIPIcs.MFCS.2018.81

Acknowledgements The author would like to thank anonymous reviewers for their careful reading and many constructive suggestions.

1 Introduction

Let MAJ_n denote the Boolean majority function of n variables, i.e.,

$$\mathsf{MAJ}_n(x_1, \ldots, x_n) \quad = \quad \mathbf{1}[\sum_{i=1}^{n} x_i \geq n/2],$$

here $\mathbf{1}[\cdot]$ denotes 1 if the condition in the bracket is satisfied, and 0 otherwise.

The problem of finding an efficient construction of circuits (or formulas) computing the majority function has attracted many researchers for a long time (e.g., [2, 10, 13]). The

[1] A part of this work was supported by JSPS Kakenhi 15K00006, 18K11152 and 18H04090.

43rd International Symposium on Mathematical Foundations of Computer Science (MFCS 2018).
Editors: Igor Potapov, Paul Spirakis, and James Worrell; Article No. 81; pp. 81:1–81:13
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

famous AKS sorting network [1] can be viewed as an $O(\log n)$ depth circuit computing MAJ_n if we pick the middle bit of all the outputs. A probabilistic construction of $\sim 5.3 \log n$-depth Boolean formula by Valiant [13] is another beautiful result on this problem. Here we mention that both of these constructions are monotone, i.e., they do not use negation gates. For more backgrounds and results, see e.g., the introduction of [4] or [7].

Recently, Kulikov and Podolskii [7] initiated the study on the "down scale" version of this problem. Specifically, they studied the construction of a small depth circuit for MAJ_n consisting of gates computing MAJ_m such that $m < n$.

In this paper, we restrict our attention to the case of depth two. Namely, we consider the following type of problems: What is the minimum value of m such that MAJ_n can be computed by a depth two circuits consisting of $\mathsf{MAJ}_{\leq m}$ gates? How to compute MAJ_n by a depth two circuit consisting of $\mathsf{MAJ}_{\leq m}$ gates for $m < n$?

In spite of the simplicity of the problem statement, its solution might be highly non-trivial even for small values of n. For example, constructing a depth two circuit consisting of the 5-bit majority gates that computes the 7-bit majority function is already not trivial.

Formally, we consider depth two circuits of the form $M_2 \circ M_1$ for $M_1, M_2 \in \{\mathsf{MAJ}_m, \mathsf{MAJ}_{\leq m}\}$ where MAJ_m and $\mathsf{MAJ}_{\leq m}$ denote the majority gates that take m and at most m inputs, respectively. Here M_2 denotes the top gate and M_1 denotes the bottom gates. In addition, we impose the restriction that each MAJ_m (or $\mathsf{MAJ}_{\leq m}$) gate on the bottom level takes m (or at most m) *distinct* input variables. Note that this restriction affects the difficulties for computing MAJ_n. Kulikov and Podolskii [7, Lemma 11] showed that there is no $\mathsf{MAJ}_{n-2} \circ \mathsf{MAJ}_{n-2}$ circuit computing MAJ_n for every odd n under this restriction. On the other hand, the author of this paper and Yoshida [3] showed that such circuits do exist for every odd $n \geq 7$ if some of the bottom gates are allowed to read an input variable multiple times. For example, the following circuit (which was presented by Kulikov and Podolskii [7, Introduction]) computes MAJ_7.

$$\begin{aligned}
&\mathsf{MAJ}_7(x_1, \ldots, x_7) \\
&\quad = \mathsf{MAJ}_5(\mathsf{MAJ}_5(x_1, x_2, x_3, x_4, x_5), \mathsf{MAJ}_5(x_1, x_2, x_5, x_6, x_7), \mathsf{MAJ}_5(x_1, x_3, x_4, x_6, x_6), \\
&\qquad \mathsf{MAJ}_5(x_2, x_3, x_3, x_5, x_6), \mathsf{MAJ}_5(x_2, x_4, x_5, x_7, x_7)).
\end{aligned}$$

One of the most interesting problems in this line of research is to find the minimum value of m such that MAJ_n can be computed by a $\mathsf{MAJ}_{\leq m} \circ \mathsf{MAJ}_{\leq m}$ circuit. Kulikov and Podolskii [7] proved a lower bound of $m \geq n^{13/19+o(1)}$. This was then improved to $m = \Omega(n^{0.8})$ by Engels, Garg, Makino and Rao [4]. For the upper bound, the construction of such a circuit for $(n, m) = (7, 5), (9, 7)$ and $(11, 9)$ is provided by Kulikov and Podolskii [7]. This was then generalized to $(n, m) = (n, n - 2)$ for all odd $n \geq 7$ by the author of this paper and Yoshida [3]. However, in all of these constructions some of the gates at the bottom level read an input variable multiple times. In our restricted setting, i.e., every bottom gate can read each variable only once, no non-trivial upper bounds were previously known.

Note that, throughout the paper, we only use the gates computing the *standard* majority, i.e., the majority gates with the threshold value $m/2$ where m denotes its fan-in. In [11], Posobin gave the construction of a depth two circuit for MAJ_n consisting of gates with fan-in $m = (2/3)n + 4$ where the threshold value of the bottom gates is not restricted to $m/2$.

Contributions

The contribution of this paper is twofolds. First, we present an explicit construction of $\mathsf{MAJ}_{\lfloor n/2 \rfloor + 2} \circ \mathsf{MAJ}_{\leq n-2}$ circuits computing MAJ_n for every $n \geq 7$ such that $n \equiv 3 \pmod 4$. The construction is quite simple, but as far as we know, this is the first non-trivial depth two circuits for MAJ_n consisting of the standard majority gates of fan-in strictly less than n and without multiple weights. Since a graph theoretic argument developed by Kulikov and Podolskii [7] can show that there is no $\mathsf{MAJ}_{\leq n-2} \circ \mathsf{MAJ}_{n-2}$ circuit computing MAJ_n, our construction reveals that the use of a smaller fan-in is essential for the existence of such a circuit. Some computational results are also provided in the paper.

During this work, we *feel* that constructing such a circuit for (n, m) with $m \ll n$ or even $m = n - 4$ may be a hard problem. This motivates us to give an explanation or evidence on this hardness, which leads to the second contribution of this paper.

In the second part of the paper, we show that the construction of depth two $\mathsf{MAJ}_m \circ \mathsf{MAJ}_m$ circuits computing MAJ_n for $m < n$ can be translated into the construction of a newly introduced version of bipartite expander graphs which we call a *list expander*. Intuitively, a list expander is a c-leftregular bipartite graph such that for a given $d < c$, every d-leftregular subgraph of the original graph has a certain expansion property. We formalize this connection, and verify that, with high probability, a random bipartite graph is a list expander of certain parameters. However, the parameters obtained are not sufficient to give us a $\mathsf{MAJ}_{n-c} \circ \mathsf{MAJ}_{n-c}$ circuit computing MAJ_n for a large constant c.

Organization of the Paper

The organization of the paper is as follows. In Section 2, we give an explicit construction of $\mathsf{MAJ}_{\lfloor n/2 \rfloor + 2} \circ \mathsf{MAJ}_{\leq n-2}$ circuits computing MAJ_n for $n \equiv 3 \pmod 4$. The results of some computational experiments on the total fan-in of the bottom gates of a $\mathsf{MAJ}_{\leq n-1} \circ \mathsf{MAJ}_{\leq n-1}$ circuit are also provided. In Section 3, we discuss the connection between the construction of depth two $\mathsf{MAJ}_m \circ \mathsf{MAJ}_m$ circuits and the construction of a newly introduced notion of bipartite expander graphs, which we call a *list expander*. Then, in Section 4, we give an analysis on the expansion property of a random bipartite graph. We close the paper by giving the conclusions in Section 5.

2 Depth Two Majority Circuits for Majority

For an integer n, $[n]$ denotes the set $\{1, 2, \ldots, n\}$. For a set S, $|S|$ denotes the cardinality of S. For an n-bit string $\boldsymbol{x} \in \{0,1\}^n$, x_i denotes the i-th bit of $\boldsymbol{x}$ and $|\boldsymbol{x}|$ denotes the number of 1's in $\boldsymbol{x}$, i.e., $|\boldsymbol{x}| = |\{i \in [n] : x_i = 1\}|$.

In this section, we first give a simple construction of depth two majority circuits for MAJ_n.

▶ **Theorem 1.** *For every $n \geq 7$ such that $n \equiv 3 \pmod 4$, there is a $\mathsf{MAJ}_{\lfloor n/2 \rfloor + 2} \circ \mathsf{MAJ}_{\leq n-2}$ circuit computing MAJ_n.*

We should note that in Theorem 1 the use of gates with fan-in less than $n-2$ at the bottom level is necessary since Kulikov and Podolskii [7, Lemma 11] proved that, for every odd n, there is no depth two $\mathsf{MAJ}_{n-2} \circ \mathsf{MAJ}_{n-2}$ circuit computing MAJ_n, and a simple generalization of their proof can be extended to establish the non-existence of $\mathsf{MAJ}_{\leq n-2} \circ \mathsf{MAJ}_{n-2}$ circuits for MAJ_n.

Proof. The proof is by construction.

Let $n = 4k+3$ for some $k \geq 1$. We will construct a $\mathsf{MAJ}_{2k+3} \circ \mathsf{MAJ}_{\leq 4k+1}$ circuit computing MAJ_n. For $1 \leq i \leq 2k+1$, let $S_i := [n] \backslash \{2i-1, 2i\}$. Let $S_{2k+2} := \{1, 3, ..., 4k+1\}$ and $S_{2k+3} := \{2, 4, ..., 4k+2\}$. For $1 \leq i \leq 2k+3$, the i-th bottom gate g_i computes the majority of all the x_j's such that $j \in S_i$. The top gate C computes the majority of all the g_i's, i.e., $C(\boldsymbol{x}) := \mathbf{1}[\sum_i g_i(\boldsymbol{x}) \geq k+2]$. For ease of understanding, we show below a 0/1-matrix representing our circuit (for $n = 11$). The (i,j)-th entry is 1 iff the gate g_i reads the variable x_j.

```
0 0 1 1 1 1 1 1 1 1 1
1 1 0 0 1 1 1 1 1 1 1
1 1 1 1 0 0 1 1 1 1 1
1 1 1 1 1 1 0 0 1 1 1
1 1 1 1 1 1 1 1 0 0 1
1 0 1 0 1 0 1 0 1 0 0
0 1 0 1 0 1 0 1 0 1 0
```

Below we verify that this circuit correctly computes MAJ_n. We first observe that it is sufficient to verify $C(\boldsymbol{x}) = 0$ only for every input $\boldsymbol{x}$ with $|\boldsymbol{x}| = 2k+1$. The correctness for $\boldsymbol{x}$ with $|\boldsymbol{x}| = n - (2k+1) = 2k+2$ will follow from the fact that every majority gate in our circuit has an odd number of inputs and hence computes a self-dual function. This implies that $C(x_1, \ldots, x_n) = 1 - C(\overline{x_1}, \ldots, \overline{x_n})$. Then, all other cases will follow from the monotonicity of our circuit.

It is convenient to consider a hypergraph G over the vertex set $V = \{1, 2, \ldots, n\}$ consisting of edges $E_1, \ldots, E_{2k+3}$ where $E_i = [n] \backslash S_i$ for $1 \leq i \leq 2k+3$. Note that G contains $2k+1$ edges of size two and two edges of size $2k+2$. We call the former small edges, and the latter large edges. For a set of vertices $S \subseteq V$ and an edge E, we say that S *covers* E if $|E \cap S| \geq |E|/2$.

For $\boldsymbol{x} \in \{0,1\}^n$, let $V_{\boldsymbol{x}} := \{i \in [n] \mid x_i = 1\}$. It is easy to observe that $g_i(\boldsymbol{x}) = 0$ iff $V_{\boldsymbol{x}}$ covers E_i for $|\boldsymbol{x}| = 2k+1$. Therefore, it is sufficient to verify that the number of edges that are covered by $V_{\boldsymbol{x}}$ is at least $\lceil \frac{2k+3}{2} \rceil = k+2$ for every $\boldsymbol{x} \in \{0,1\}^n$ with $|\boldsymbol{x}| = 2k+1$.

We divide the proof into two cases.

Case 1 $4k+3 \notin V_{\boldsymbol{x}}$.

Observe that $V_{\boldsymbol{x}}$ covers at least $k+1$ small edges. If $V_{\boldsymbol{x}}$ covers $k+2$ or more small edges, then we are done. Therefore, we can assume that $V_{\boldsymbol{x}}$ covers exactly $k+1$ small edges. However, in this case, $V_{\boldsymbol{x}}$ must cover one of two large edges, and hence $V_{\boldsymbol{x}}$ covers $k+2$ edges in total. This completes the proof.

Case 2 $4k+3 \in V_{\boldsymbol{x}}$.

We view that small edges form a bipartite matching between $2k+1$ left vertices (odd numbers up to $4k+1$) and $2k+1$ right vertices (even numbers up to $4k+2$). If $V_{\boldsymbol{x}}$ covers at least $k+1$ left vertices of small edges or at least $k+1$ right vertices of small edges, then at least $k+2$ edges are covered in total since $V_{\boldsymbol{x}}$ also covers one of two large edges. If $V_{\boldsymbol{x}}$ covers exactly k left vertices and k right vertices of small edges, then it also covers both large edges and hence $V_{\boldsymbol{x}}$ covers at least $k+2$ edges in total. This completes the proof. ◀

Remark that it is quite plausible that there are many other constructions of $\mathsf{MAJ}_{\leq n-2} \circ \mathsf{MAJ}_{\leq n-2}$ circuit for MAJ_n. For example, for every $n \geq 9$ with $n \equiv 3 \pmod 6$, it seems likely that the $\mathsf{MAJ}_{\frac{3}{2}n+1} \circ \mathsf{MAJ}_{\leq n-2}$ circuit given below also computes MAJ_n. Let $n = 3k$ and suppose that k is odd. For $i \in [k]$, $S_{2i-1} = [n] \backslash \{3i-2, 3i\}$ and $S_{2i} = [n] \backslash \{3i-1, 3i\}$. In addition, we let $S_{2k+1} := \{3, 6, \ldots, 3k\}$. For $i \in [2k+1]$, the i-th bottom gate g_i is defined to be

$$g_i(\boldsymbol{x}) = \mathbf{1}\left[\sum_{i \in S_i} x_i \geq \frac{|S_i|}{2}\right],$$

and the top gate computes the majority of all the g_i's. We have computationally verified the correctness of this circuit up to $n = 27$, and it may be a good exercise to give a formal proof.

Sum of Bottom Fan-ins

Let $F(n)$ denote the smallest number of the total fan-ins of all the bottom gates of a depth two $\mathsf{MAJ}_{\leq n-1} \circ \mathsf{MAJ}_{\leq n-1}$ circuit that computes MAJ_n. It would be interesting to find the value of $F(n)$. The circuit constructed in the proof of Theorem 1 gives the upper bound of $F(n) \leq (n-2)\lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{2} \rfloor \cdot 2 = n\lfloor \frac{n}{2} \rfloor \sim n^2/2$.

We show below some computational results on $F(n)$ for small values of n. We obtain these results by using an IP solver [6]. More specifically, if we fix the fan-in of the top gate to m_2, then the optimal value of the following IP problem gives $F(n)$. Intuitively, for each $S \subseteq [n]$, G_S represents the number of wires connecting from the bottom gates $\mathbf{1}[\sum_{i \in S} x_i \geq \frac{\lfloor S \rfloor}{2}]$ to the top gate. The number of variables is $\sim 2^n$, and the number of constraints is $\sim 2\binom{n}{\lfloor n/2 \rfloor}$ as we only need to check for $\boldsymbol{x}$ with $|\boldsymbol{x}| \in \{\lceil n/2 \rceil, \lfloor n/2 \rfloor\}$ by monotonicity.

$$\begin{aligned}
\text{Minimize:} \quad & \sum_{\emptyset \neq S \subsetneq [n]} |S| G_S \\
\text{Subject to:} \quad & \sum_{\emptyset \neq S \subsetneq [n]} G_S = m_2, \\
& \sum_{S : |S \cap V_{\boldsymbol{x}}| \geq \frac{\lfloor S \rfloor}{2}} G_S \geq \frac{m_2}{2}, \quad (\forall \boldsymbol{x} \in \{0,1\}^n \text{ s.t. } \mathsf{MAJ}_n(\boldsymbol{x}) = 1), \\
& \sum_{S : |S \cap V_{\boldsymbol{x}}| \geq \frac{\lfloor S \rfloor}{2}} G_S < \frac{m_2}{2}, \quad (\forall \boldsymbol{x} \in \{0,1\}^n \text{ s.t. } \mathsf{MAJ}_n(\boldsymbol{x}) = 0). \\
& G_S \geq 0 : \text{ integer} \quad (\forall S).
\end{aligned}$$

Here $V_{\boldsymbol{x}}$ denotes $\{i \in [n] : x_i = 1\}$ as in the proof of Theorem 1.

Note that $F(n)$ is undefined for $n \leq 5$ since a simple exhaustive search shows that there is no $\mathsf{MAJ}_{\leq n-1} \circ \mathsf{MAJ}_{\leq n-1}$ circuit computing MAJ_n for $n \leq 5$. The result of our experiments is as follows.

- $F(6) = 18$.
- $F(7) = 21$. This is identical to the value given by the circuit in the proof of Theorem 1.
- $F(8) = 31$.
- $F(9) = 37$.
- $F(10) = 50$.
- $F(11) = 55$. This is identical to the value given by the circuit in the proof of Theorem 1.

We show an example of circuits that attain $F(n)$ for $n = 6, 8, 9$ and 10 in Table 1. Given these data, we conjecture that $F(n)$ is of the order of n^2.

▶ **Conjecture 2.** $F(n) = \Theta(n^2)$. *More ambitiously,* $F(n) \sim \frac{n^2}{2}$.

Table 1 The matrix representation of an example of a $\mathsf{MAJ}_{\leq n-1} \circ \mathsf{MAJ}_{\leq n-1}$ circuit for MAJ_n of a smallest total fan-ins for $n = 6, 8, 9$ and 10. Here the (i, j)-entry of each matrix represents whether the i-th bottom gate reads the variable x_j.

0	0	1	1	1	1
1	1	0	0	1	1
1	1	1	1	0	0
0	1	0	1	0	1
1	0	1	0	1	0

0	0	1	1	1	1	0	0
0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1
1	1	0	0	1	1	0	0
1	1	1	1	0	0	0	0
1	1	0	0	0	0	1	1
1	1	1	1	1	1	1	0

0	0	0	1	1	0	0	0	1
0	1	1	1	0	1	1	1	1
0	1	1	1	1	0	0	0	1
1	0	0	0	0	1	1	0	0
1	1	0	0	0	1	1	1	0
1	1	1	0	1	0	1	1	1
1	1	1	1	1	1	0	1	0

0	0	1	1	0	1	1	0	1	0
0	0	1	1	1	1	0	1	0	0
1	1	0	0	0	0	0	1	1	1
1	1	0	0	1	0	1	0	0	1
1	1	1	1	0	1	0	0	0	1
1	1	1	1	1	0	1	1	1	0
0	1	0	1	1	1	1	1	1	1
1	0	1	0	1	1	1	1	1	1

3 Connection between Circuits and List Expanders

For a $\mathsf{MAJ}_{m_2} \circ \mathsf{MAJ}_{m_1}$ circuit on n input variables, we naturally associate a bipartite graph over m_2 left vertices and n right vertices as follows.

▶ **Definition 3.** Let C be a $\mathsf{MAJ}_{m_2} \circ \mathsf{MAJ}_{m_1}$ circuit on n input variables where the bottom gates are labeled by $g_1, \dots, g_{m_2}$. We define a bipartite graph $G_C = (L \cup R, E)$ *associated to* C as follows: Let $L = \{g_1, \dots, g_{m_2}\}$ and $R = \{x_1, \dots, x_n\}$, i.e., each left vertex is corresponding to a bottom gate and each right vertex is corresponding to an input variable. For $g_i \in L$ and $x_j \in R$, $(g_i, x_j) \in E$ iff the gate g_i *does not* read x_j as an input in C.

Let $G = (V, E)$ be a graph. For a vertex $v \in V$, $N_G(v)$ denotes the neighbors of v, and for a set of vertices $S \subseteq V$, $N_G(S)$ denotes the neighbors of S, i.e., $N_G(S) := \{u : \exists v \in S \text{ s.t. } (v, u) \in E\}$.

By Definition 3, a bipartite graph G_C associated to a $\mathsf{MAJ}_{m_2} \circ \mathsf{MAJ}_{n-\ell_1}$ circuit C is ℓ_1-*leftregular*, which means that every left vertex has exactly ℓ_1 neighbors, i.e., $|N_{G_C}(v)| = \ell_1$ for every $v \in L$.

The following is the main theorem in this section, which translates the construction of depth two circuits computing MAJ_n into the construction a bipartite graph with a certain expansion property.

▶ **Theorem 4.** *Suppose that n is an odd integer. For every even numbers $\ell_1, \ell_2 > 0$, the following are equivalent.*

(i) *A depth two $\mathsf{MAJ}_{n-\ell_2} \circ \mathsf{MAJ}_{n-\ell_1}$ circuit C computes MAJ_n.*

(ii) *Let $G_C = (L \cup R, E)$ be a ℓ_1-leftregular bipartite graph associated to C. Then, for every $(\ell_1/2 + 1)$-leftregular subgraph $G' \subseteq G_C$ over the same set of vertices of G_C,*

$$|N_{G'}(S)| \geq \left\lceil \frac{|R|}{2} \right\rceil + 1 \text{ for every } S \subseteq L \text{ with } |S| = \left\lceil \frac{|L|}{2} \right\rceil.$$

Proof. By using an argument similar to the one used in the proof of Theorem 1, we see that the statement (i) is equivalent to the statement that for every $\boldsymbol{x} \in \{0, 1\}^n$ with $|\boldsymbol{x}| = \lceil n/2 \rceil$, $C(\boldsymbol{x}) = 1$, which we refer to as (i'). Here we use the assumption that n is odd as well as the fan-in of each gate is also odd.

(i') → (ii) Assume for contradiction that there exists an $(\ell_1/2 + 1)$-leftregular subgraph G' of G_C such that $|N_{G'}(S)| \leq \lceil |R|/2 \rceil$ for some $S \subseteq L$ with $|S| = \lceil |L|/2 \rceil$. Fix an arbitrary such S. Let $X_1 \subseteq R$ be an arbitrary superset of $N_{G'}(S)$ with $|X_1| = \lceil |R|/2 \rceil = \lceil n/2 \rceil$. Define

$\boldsymbol{x} = (x_1, \dots, x_n) \in \{0,1\}^n$ so that $x_j = 1$ iff $x_j \in X_1$ for $j \in [n]$. For every $g_i \in S$, we have $g_i(\boldsymbol{x}) = 0$ and hence $C(\boldsymbol{x}) = 0$ since $|S| = \lceil |L|/2 \rceil$. This contradicts the statement (i'), completing the proof.

(ii) → (i') Assume for contradiction that there exists an input $\boldsymbol{x} = (x_1, \dots, x_n) \in \{0,1\}^n$ such that $|\boldsymbol{x}| = \lceil n/2 \rceil$ and $C(\boldsymbol{x}) = 0$. Fix an arbitrary such $\boldsymbol{x}$. Define $X_1 \subseteq R$ as $X_1 := \{x_j : x_j = 1\}$, and for $1 \le i \le |L|$, let $V_i \subseteq R$ be the set of variables x_j such that g_i reads x_j. By the construction of the graph G_C, we have

$$\left|\left\{g_i \in L : |V_i \cap X_1| \le \left\lfloor \frac{n-\ell_1}{2} \right\rfloor\right\}\right| \ge \left\lceil \frac{|L|}{2} \right\rceil.$$

Since $|X_1| = \lceil n/2 \rceil$, this is equivalent to

$$\left|\left\{g_i \in L : |\overline{V_i} \cap X_1| \ge \frac{\ell_1}{2} + 1\right\}\right| \ge \left\lceil \frac{|L|}{2} \right\rceil,$$

where $\overline{V_i}$ denotes the set $R \backslash V_i$.

Let S be an arbitrary $\lceil |L|/2 \rceil$-element subset of $\left\{g_i \in L : |\overline{V_i} \cap X_1| \ge \frac{\ell_1}{2} + 1\right\}$. Then we can pick an $(\ell_1/2 + 1)$-leftregular subgraph G' of G_C such that $N_{G'}(g_i) \subseteq X_1$ for every $g_i \subseteq S$. For this graph G', $N_{G'}(S) \subseteq X_1$, and hence $|N_{G'}(S)| \le |X_1| = \lceil n/2 \rceil$, contradicting the statement (ii). ◀

We see that the statement (ii) in Theorem 4 has a similar spirit to bipartite expander graphs. This leads us to the following definition.

▶ **Definition 5.** Let $d_1 \ge d_2 > 0$ be two integers. A d_1-leftregular bipartite graph $G = (L \cup R, E)$ with $|L| = m$ and $|R| = n$ is said to be an $((m,n),(d_1,d_2),K,A)$ *list expander* if for every d_2-leftregular subgraph G' of G over the same set of vertices of G, it holds that

$|N_{G'}(S)| \ge A$ for every $S \subseteq L$ with $|S| = K$.

When $d_1 = d_2$ we simply call it an expander. Formally, a d_1-leftregular bipartite graph $G = (L \cup R, E)$ with $|L| = m$ and $|R| = n$ is said to be an $((m,n),d_1,K,A)$ *expander* if

$|N_G(S)| \ge A$ for every $S \subseteq L$ with $|S| = K$.

Note that our definition of an expander is different from the usual definition in a sense that the expansion property is only required for the sets of size equal to K.

The existence of a $\mathsf{MAJ}_{n-4} \circ \mathsf{MAJ}_{n-4}$ circuit computing MAJ_n is equivalent to the existence of an $((n-4,n),(4,3),\lceil \frac{n-4}{2} \rceil, \lceil \frac{n}{2} \rceil + 1)$ list expander. Moreover, an explicit construction of such a circuit implies an explicit construction of such an expander, and vice versa. Currently, we do not know whether such an expander can be built from known constructions of expanders in the usual sense.

A similar argument to the proof of Theorem 4 can show that a list expander of the form "d_1 choose d_2" for $d_2 > d_1/2 + 1$ captures a promise version of the problem for constructing majority circuits. The proof of Theorem 6 is very similar to the proof of Theorem 4 and omitted in this version.

▶ **Theorem 6.** *Let n be an odd integer, and $c \ge 2$ be an even integer. Let C be a $\mathsf{MAJ}_{n-c} \circ \mathsf{MAJ}_{n-c}$ circuit over $\{x_1, \dots, x_n\}$ and let G_C be a c-leftregular bipartite graph associated to C. Suppose that d is an integer such that $d \ge \frac{c}{2} + 1$. Then, the following are equivalent.*

(i) *$C(\boldsymbol{x}) = 1$ for every $|\boldsymbol{x}| = \lfloor \frac{n}{2} \rfloor - \frac{c}{2} + d$ and $C(\boldsymbol{x}) = 0$ for every $|\boldsymbol{x}| = \lceil \frac{n}{2} \rceil + \frac{c}{2} - d$.*

(ii) *G_C is an $((n-c,n),(c,d),\lceil \frac{n-c}{2} \rceil, \lfloor \frac{n}{2} \rfloor - \frac{c}{2} + d)$ list expander.*

Algorithm 1 Construct an witness for refuting an expansion property.

```
 1: procedure CONVERT($G$)
 2:     $\tilde{S} := S$ and $\tilde{T} := N_G(S)$
 3:     $d := d_1$
 4:     while $d > d_2$ do
 5:         $S' := \tilde{S}$ and $T' := \tilde{T}$
 6:         repeat
 7:             Let $v^*$ be a vertex $v \in T'$ minimizing $|N_G(v) \cap S'|$. Ties are broken arbitrary.
 8:             Put $S_{v^*} := N_G(v^*) \cap S'$
 9:             Remove all edges connecting $v^*$ and a vertex in $S'$ from $G$
10:             $\tilde{T} := \tilde{T} \backslash \{v^*\}$
11:             $S' := S' \backslash S_{v^*}$
12:             $T' := T' \backslash (N_G(S_{v^*}) \cap T')$
13:         until $|\tilde{T}| < \left(1 + \frac{d - d_2}{5d_1^2}\right) A$
14:         $d := d - 1$
15:     end while
16: end procedure
```

3.1 List Expanders imply Expanders

In this subsection, we give a result roughly stating that a list expander implies an expander of a certain expansion factor, and observe that converse of it is not true.

▶ **Theorem 7.** *Let $d_1 > d_2 > 0$ be two integers. Suppose that a bipartite graph $G = (L \cup R, E)$ is an $((m, n), (d_1, d_2), K, A)$ list expander for $A \geq K$. Then, G is an $((m, n), d_1, K, (1 + \epsilon)A)$ expander for $\epsilon = (d_1 - d_2)/(5d_1^2)$.*

Note that we did not optimize the constant ϵ in Theorem 7.

Proof. The proof is by contrapositive. Put $\epsilon = (d_1 - d_2)/(5d_1^2)$. Assume that a d_1-leftregular bipartite graph $G = (L \cup R, E)$ is not an $((m, n), d_1, K, (1 + \epsilon)A)$ expander for $A \geq K$. This means that there exists a set of vertices $S \subseteq L$ with $|S| = K$ such that $|N_G(S)| < (1 + \epsilon)A$. We will see that for this case, G is not an $((m, n), (d_1, d_2), K, A)$ list expander. In order to show this, it is sufficient to show that there exists a d_2-leftregular subgraph G' of G such that for some $\tilde{S} \subseteq L$ with $|\tilde{S}| = K$ and for some $\tilde{T} \subseteq R$ with $|\tilde{T}| < A$, $|N_{G'}(\tilde{S})| \subseteq \tilde{T}$ holds.

We set $\tilde{S} := S$. We will find a subgraph G' and a set $\tilde{T} \subseteq T$ by using Algorithm 1 shown above.

First we observe that whenever $|T'| \geq A$, there are at least $A/2$ v's in T' such that $|N_G(v) \cap \tilde{S}| \leq 2d_1$ since if otherwise, we have $\sum_{v \in T'} |N_G(v) \cap \tilde{S}| > Ad_1 \geq Kd_1$, which contradicts the assumption that G is d_1-leftregular. Suppose that a vertex v^* chosen in Line 7 satisfies $|S_{v^*}| \leq 2d_1$. We refer to this condition as (*). Then, in Line 12, $|T'|$ decreases at most $2d_1^2$. For every fixed d, the number of iterations of Lines 6 to 13 is at least $\frac{1}{5d_1^2}A$. Since $2d_1^2 \frac{1}{5d_1^2} A < \frac{1}{2} A$, the condition (*) is always satisfied.

A crucial observation is that after each execution of the **While** loop in the algorithm, G satisfies that $|N_G(v)| \geq d$ for every $v \in \tilde{S}$ and $N_G(\tilde{S}) \subseteq \tilde{T}$. Hence, after the execution of the entire algorithm, we have a graph G such that $|N_G(v)| \geq d_2$ for every $v \in \tilde{S}$ and $N_G(\tilde{S}) \subseteq \tilde{T}$ with $|\tilde{T}| < A$. Then, an arbitrary d_2-leftregular subgraph of G is not an expander for the parameter given in the statement of the theorem. ◀

We remark that an argument below suggests that the converse of Theorem 7 is not true. Let $G = (L \cup R, E)$ be a bipartite graph with $L = R = \mathbb{Z}_p$ and edge set $\{(x, x+1), (x, x-1), (x, x^{-1})\}_{x \in \mathbb{Z}_p}$ where all arithmetic is modulo p and define 0^{-1} to be 0. It was shown that this 3-leftregular bipartite graph has an expansion property with some constant expansion factor. (This was stated implicitly in [8]. See e.g., [12, Construction 4.26] for the statement in this form.) If we add the edges $\{(x, x)\}_{x \in \mathbb{Z}_p}$ to G (and make a slight rearrangement for $x = 0$ to avoid parallel edges $(0, 0)$), then it becomes a 4-leftregular expander. However, a 3-leftregular subgraph consisting of the edges $\{(x, x+1), (x, x), (x, x-1)\}_{x \in \mathbb{Z}_p}$ is not an expander anymore.

4 Probabilistic Constructions

In this section, we show a statement roughly saying that a random c-leftregular bipartite graph is a list expander of the form "c choose d" for $d \sim \frac{2}{3}c$ with a non-negligible probability. Note that this is not sufficient for obtaining a non-trivial depth two circuit computing the majority function, for which we need $d \sim \frac{1}{2}c$.

We first show a fact that will be used in our analysis.

▶ **Fact 8.** *Suppose that a, b, p are positive integers satisfying $a - p > b - p > 0$. Then,*

$$\frac{a^{a-p}}{b^{b-p}} \geq \frac{(a-p)^{a-p}}{(b-p)^{b-p}}.$$

Proof. The fact can be verified by the following series of inequalities.

$$\begin{aligned}
&a^{a-p}(b-p)^{b-p} - (a-p)^{a-p}b^{b-p} \\
&\quad = \quad (a-p+a)^{a-p}(b-p)^{b-p} - (a-p)^{a-p}(b-p+b)^{b-p} \\
&\quad = \quad \sum_{i=0}^{a-p}\binom{a-p}{i}(a-p)^{a-p-i}a^i(b-p)^{b-p} - \sum_{i=0}^{b-p}\binom{b-p}{i}(b-p)^{b-p-i}b^i(a-p)^{a-p} \\
&\quad \geq \quad \sum_{i=0}^{b-p}(a-p)^{a-p-i}(b-p)^{b-p-i}\left\{\binom{a-p}{i}(b-p)^i - \binom{b-p}{i}(a-p)^i\right\} \qquad (1) \\
&\quad \geq \quad 0.
\end{aligned}$$

Here the last inequality follows from the fact that the value inside the bracket in Eq. (1) is non-negative for every fixed i. ◀

The following is the main theorem in this section.

▶ **Theorem 9.** *Let $\epsilon > 0$ be an arbitrary small positive constant. Suppose that c is a constant such that $\epsilon c \geq 3$, and let $m = n - c$. Then for every sufficiently large n, there is an $((m, n), (c, d), \lceil \frac{m}{2} \rceil, \lfloor \frac{n}{2} \rfloor - \frac{c}{2} + d)$ list expander, where $d = \lceil (\frac{2}{3} + \epsilon)c \rceil$.*

By Theorem 6 and Theorem 9, we can see that for every sufficiently large n, there exists a $\mathsf{MAJ}_{n-c} \circ \mathsf{MAJ}_{n-c}$ circuit C such that $C(\boldsymbol{x}) = \mathsf{MAJ}_n(\boldsymbol{x})$ for every $\boldsymbol{x} \in \{0,1\}^n$ such that $|\boldsymbol{x}| \lesssim \frac{n}{2} - \frac{c}{6}$ or $|\boldsymbol{x}| \gtrsim \frac{n}{2} + \frac{c}{6}$.

The rest of this section is devoted to prove Theorem 9. The proof relies on relatively basic but a bit lengthy calculations.

Proof. Consider a bipartite graph over the vertex set $L \cup R$ with $|L| = m (= n - c)$ and $|R| = n$. We view a c-leftregular bipartite graph as a union of c bipartite matchings. For $i \in [c]$, let M_i be a bipartite matching over $L \cup R$ in which the left vertices are saturated. A c-leftregular bipartite graph $G = (L \cup R, E)$ is specified by a sequence of c such matchings

$E = (M_1, \ldots, M_c)$, which we denoted by G_E. Let $\mathcal{E}$ denote the set of all possible E's and thus $|\mathcal{E}| = (\frac{n!}{c!})^c$. Notice that at this moment, a graph obtained in this way may have a multiedge. We will take into account this issue later.

Roughly speaking, a c-leftregular bipartite graph is a list expander if every d-leftregular subgraph of it is an expander. For $d \leq c$, a d-leftregular subgraph of G is specified by a sequence of m sets $D_i \subseteq [c]$ $(1 \leq i \leq m)$ of size d. Given a sequence of c matchings $E = (M_1, \ldots, M_c)$ and a sequence of m sets $\mathbf{D} = (D_1, \ldots, D_m)$, let $G_{E,\mathbf{D}}$ denote a d-leftregular bipartite graph such that for every $i \in [m]$, the set of edges connecting to the i-th left vertex consists of an edge in M_j for $j \in D_i$. Let $\mathcal{D}$ denote the set of all possible $\mathbf{D}$'s and thus $|\mathcal{D}| = \binom{c}{d}^m$.

We define $\mathcal{E}' \subseteq \mathcal{E}$ as the set of all E's in $\mathcal{E}$ such that G_E is a c-leftregular bipartite graph where G_E does not contain a multiedge. The following lemma says that the cardinality of $\mathcal{E}'$ is not too small compared to the cardinality of $\mathcal{E}$. Here e denotes the base of the natural logarithm. The proof of the lemma is postponed to the end of this section.

▶ **Lemma 10.** *For all sufficiently large n, the cardinality of $\mathcal{E}' \subseteq \mathcal{E}$ satisfies*

$$|\mathcal{E}'| \quad \geq \quad \frac{(n!)^c}{e^{\binom{c}{2}} n^{c^2}}.$$

Given a set $S \subseteq L$ and a set $T \subseteq R$ and a sequence $\mathbf{D} \in \mathcal{D}$, we count the number of $E \in \mathcal{E}$ such that $G_{E,\mathbf{D}}$ satisfies $N_{G_{E,\mathbf{D}}}(S) \subseteq T$, which we refer to as the property $P_{S,T}$.

For $j \in [c]$, let $a_j := |\{i \in S : j \notin D_i\}|$. Define an auxiliary function f as

$$f((m, n), (\ell, r), a) \quad = \quad \frac{r!(n - (\ell - a))!}{(r - (\ell - a))!(n - m)!}.$$

This represents the number of left saturated bipartite matchings in the $(m + n)$-vertex complete bipartite graph such that the neighbors of some specified $l - a$ left vertices are contained in some specified r right vertices. Then, the number of $E \in \mathcal{E}$ such that $G_{E,\mathbf{D}}$ satisfies $P_{S,T}$ is given by

$$\prod_{j \in [c]} f((m, n), (|S|, |T|), a_j). \tag{2}$$

We say that the a_j's are equally distributed if, for every $i, j \in [c]$, $|a_i - a_j| \leq 1$. The following lemma is useful for our calculation.

▶ **Lemma 11.** *Eq. (2) is maximized when the a_j's are equally distributed.*

Proof. Let $b_j = \ell - a_j$, i.e. b_j is the number of edges in M_j connecting to a vertex in S in the graph $G_{E,\mathbf{D}}$. Suppose that $a_i = a_j + \alpha$ for some $i, j \in [n]$ and for some $\alpha \geq 2$. In order to prove the lemma, it is sufficient to show that

$$g(a_i)g(a_j) \leq g(a_i - 1)g(a_j + 1),$$

where $g(a)$ stands for $f((m,n),(\ell,r),a)$. This is verified by the following.

$$\begin{aligned}
&g(a_i-1)g(a_j+1)-g(a_i)g(a_j)\\
&= \left(\frac{r!}{(n-m)!}\right)^2\left(\frac{(n-(b_i+1))!}{(r-(b_i+1))!}\frac{(n-(b_i+\alpha-1))!}{(r-(b_i+\alpha-1))!}-\frac{(n-b_i)!}{(r-b_i)!}\frac{(n-(b_i+\alpha))!}{(r-(b_i+\alpha))!}\right)\\
&= \left(\frac{r!}{(n-m)!}\right)^2\left(\frac{(n-(b_i+1))!}{(r-(b_i+1))!}\frac{(n-(b_i+\alpha))!}{(r-(b_i+\alpha))!}\right)\left(\frac{n-(b_i+\alpha-1)}{r-(b_i+\alpha-1)}-\frac{n-b_i}{r-b_i}\right)\\
&= \left(\frac{r!}{(n-m)!}\right)^2\left(\frac{(n-(b_i+1))!}{(r-(b_i+1))!}\frac{(n-(b_i+\alpha))!}{(r-(b_i+\alpha))!}\right)\left(\frac{(n-r)(\alpha-1)}{(r-(b_i+\alpha-1))(r-b_i)}\right)\\
&\geq 0.
\end{aligned}$$

◀

We go back to the proof of Theorem 9.

Put $d=(\frac{2}{3}+\epsilon)c$, and put $|S|=\lceil\frac{n-c}{2}\rceil$ and $|T|=\lfloor\frac{n}{2}\rfloor-\frac{c}{2}+d$. Then, Eq. (2) is equal to

$$\prod_{i\in[c]}\frac{(\lfloor\frac{n}{2}\rfloor+\frac{c}{6}+c\epsilon)!\cdot(n-(\lceil\frac{n}{2}\rceil-\frac{c}{2}-a_j))!}{(\lfloor\frac{n}{2}\rfloor+\frac{c}{6}+c\epsilon-(\lceil\frac{n}{2}\rceil-\frac{c}{2}-a_j))!\cdot c!}=\prod_{i\in[c]}\frac{(\lfloor\frac{n}{2}\rfloor+\frac{c}{6}+c\epsilon)!\cdot(\lfloor\frac{n}{2}\rfloor+\frac{c}{2}+a_j)!}{(\frac{2}{3}c+c\epsilon-1+a_j)!\cdot c!}.$$

By Lemma 11, this is upper bounded by

$$\left(\frac{(\lfloor\frac{n}{2}\rfloor+\frac{c}{6}+c\epsilon)!\cdot(\lfloor\frac{n}{2}\rfloor+\frac{c}{2}+a)!}{(\frac{2}{3}c+c\epsilon-1+a)!\cdot c!}\right)^c,$$

where $a=(\frac{1}{3}-\epsilon)(\lceil\frac{n}{2}\rceil-\frac{c}{2})$. By substituting the RHS for a, the inside of the outer bracket of the above formula is upper bounded by

$$\frac{(\lceil\frac{n}{2}\rceil+\frac{c}{6}+c\epsilon)!\cdot(\frac{2}{3}n-\frac{\epsilon n}{2}+\frac{c}{3}+\frac{c\epsilon}{2})!\cdot n^{C_0}}{(\frac{n}{6}-\frac{\epsilon n}{2}+\frac{c}{2}+\frac{3c\epsilon}{2})!\cdot c!} \tag{3}$$

for some small positive constant C_0. Since c and ϵ are constants, there are large enough constants C_1 and C_2, Eq. (3) is upper bounded by

$$\begin{aligned}
\frac{(\frac{n}{2})!\cdot(\frac{2}{3}n-\frac{\epsilon n}{2})!\cdot n^{C_1}}{(\frac{n}{6}-\frac{\epsilon n}{2})!} &\leq \frac{(\frac{n}{2})^{\frac{n}{2}}\cdot(\frac{2}{3}n-\frac{\epsilon n}{2})^{\left(\frac{2}{3}n-\frac{\epsilon n}{2}\right)}n^{C_2}}{(\frac{n}{6}-\frac{\epsilon n}{2})^{\left(\frac{n}{6}-\frac{\epsilon n}{2}\right)}e^n}\\
&\leq \frac{(\frac{n}{2})^{\frac{n}{2}}\cdot(\frac{2}{3}n)^{\left(\frac{2}{3}n-\frac{\epsilon n}{2}\right)}n^{C_2}}{(\frac{n}{6})^{\left(\frac{n}{6}-\frac{\epsilon n}{2}\right)}e^n}\\
&= n^{C_2}\cdot\frac{n^n}{e^n}\cdot\left(\frac{2^{1/3}}{3^{1/2}}\right)^n\cdot\left(\frac{1}{2}\right)^{\epsilon n}. \qquad (4)
\end{aligned}$$

Here the first inequality is by the Stirling formula, and the second inequality is by Lemma 8.

The number of $E\in\mathcal{E}$ such that

$$^{\exists}S\subseteq L\ ^{\exists}T\subseteq R\ ^{\exists}\mathbf{D}\in\mathcal{D}\quad G_{E,\mathbf{D}} \text{ has the property } P_{S,T} \tag{5}$$

is at most

$$\frac{2^{n-c}\cdot 2^n\cdot(\text{Eq.}(4))^c\cdot|\mathcal{D}|}{\binom{c}{d}^{\lfloor\frac{m}{2}\rfloor}}=2^{n-c}\cdot 2^n\cdot(\text{Eq.}(4))^c\cdot\binom{c}{d}^{\lceil\frac{m}{2}\rceil}. \tag{6}$$

By using the upper bound on the binomial coefficients (see e.g., [9, Lemma 9.2])

$$\binom{c}{\alpha c}\leq 2^{cH(\alpha)},$$

where $H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary entropy function, we have

$$\binom{c}{d}^{\lceil \frac{m}{2} \rceil} \le 2^{H(\frac{1}{3}-\epsilon)\lceil \frac{m}{2} \rceil} < 2^{H(\frac{1}{3})\frac{n}{2}} = \left(\frac{3^{1/2}}{2^{1/3}}\right)^n .$$

Therefore, we have

$$\text{(Eq. (6))} \quad < \quad 2^{2n} n^{C_2 c} \cdot \frac{n^{cn}}{e^{cn}} \cdot \left(\frac{1}{2}\right)^{\epsilon c n} . \tag{7}$$

Recall that $\mathcal{E}' \subseteq \mathcal{E}$ is the set of all E's in $\mathcal{E}$ such that G_E is a c-leftregular bipartite graph where G_E does not contain a multiedge. The proof of Theorem 9 will be completed if we verify that Eq. (7) is smaller than the cardinality of $\mathcal{E}'$ since it implies the existence of a c-leftregular bipartite graph G_E not satisfying the condition Eq. (5), i.e., G_E is a list expander of the desired parameter.

By Lemma 10, we have

$$|\mathcal{E}'| \quad \ge \quad \frac{(n!)^c}{e^{\binom{c}{2}} n^{c^2}} \ge \frac{n^{cn}}{e^{cn}} \frac{1}{n^{C_3}},$$

for a sufficiently large constant C_3. We can see that when n goes to infinity the last term in the above is larger than Eq. (7) by recalling that $\epsilon c \ge 3$. ◀

Proof of Lemma 10. We use the result on counting the number of *Latin rectangles*. A $c \times n$ Latin rectangle is a $c \times n$ matrix L with symbols from $[n]$ such that each row and each column contains only distinct symbols. Let $L_{c,n}$ denote the number of $c \times n$ Latin rectangles. It was shown by Erdős and Kaplansky [5] that, for $c = O((\log^n)^{3/2-\epsilon})$,

$$L_{c,n} \sim \frac{(n!)^c}{e^{\binom{c}{2}}}.$$

It is easy to observe that a c-leftregular bipartite graph with $n-c$ left vertices and n right vertices can be naturally represented by a $c \times (n-c)$ matrix obtained from a $c \times n$ Latin rectangle by discarding the last c columns. Since we shall discard c^2 entries with symbols from $[n]$, the number of variations of such $c \times (n-c)$ matrices is at least $L_{c,n}/(n^{c^2})$, completing the proof of the lemma. ◀

5 Conclusions

In this paper, we introduce a new notion of expander graphs and give the translation result from the construction of depth two circuits computing the majority function. Currently, the existence of a $\mathsf{MAJ}_{n-c} \circ \mathsf{MAJ}_{n-c}$ circuit computing MAJ_n is open even for $c = 4$. We hope that our translation result leads us to a better understanding on this problem with the help of a rich theory on expander graphs. In addition, it would be interesting to find other applications of list expanders.

References

1 Miklós Ajtai, János Komlós, and Endre Szemerédi. Sorting in $c \log n$ parallel steps. *Combinatorica*, 3(1):1–19, 1983.

2 Kazuyuki Amano. Bounds on the size of small depth circuits for approximating majority. In *Automata, Languages and Programming, 36th International Colloquium, ICALP 2009, Rhodes, Greece, July 5-12, 2009, Proceedings, Part I*, pages 59–70, 2009.

3 Kazuyuki Amano and Masafumi Yoshida. Depth two $(n-2)$-majority circuit for n-majority. *to appear in IEICE Trans. Fundamentals*, E101-A(9), 2018.

4 Christian Engels, Mohit Garg, Kazuhisa Makino, and Anup Rao. On expressing majority as a majority of majorities. *Electronic Colloquium on Computational Complexity (ECCC)*, 24:174, 2017.

5 Paul Erdős and Irving Kaplansky. The asymptotic number of latin rectangles. *Amer. J. Math*, 68:230–236, 1946.

6 LLC Gurobi Optimization. Gurobi optimizer reference manual, 2018. URL: `http://www.gurobi.com`.

7 Alexander S. Kulikov and Vladimir V. Podolskii. Computing majority by constant depth majority circuits with low fan-in gates. In *34th Symposium on Theoretical Aspects of Computer Science, STACS 2017, March 8-11, 2017, Hannover, Germany*, pages 49:1–49:14, 2017.

8 Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

9 Michael Mitzenmacher and Eli Upfal. *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, 2005.

10 Ryan O'Donnell and Karl Wimmer. Approximation by DNF: examples and counterexamples. In *Automata, Languages and Programming, 34th International Colloquium, ICALP 2007, Wroclaw, Poland, July 9-13, 2007, Proceedings*, pages 195–206, 2007.

11 Gleb Posobin. Computing majority with low-fan-in majority queries. *CoRR*, abs/1711.10176, 2017. `arXiv:1711.10176`.

12 Salil P. Vadhan. Pseudorandomness. *Foundations and Trends in Theoretical Computer Science*, 7(1-3):1–336, 2012.

13 Leslie G. Valiant. Short monotone formulae for the majority function. *J. Algorithms*, 5(3):363–366, 1984.