Depth Two \((n - 2)\)-Majority Circuits for \(n\)-Majority

Kazuyuki Amano\(^*\)\(^†\) and Masafumi Yoshida\(^*\)

January 17, 2018

Abstract

We present an explicit construction of a \(\text{MAJ}_{n-2} \circ \text{MAJ}_{n-2}\) circuit computing \(\text{MAJ}_n\) for every odd \(n \geq 7\). This gives a partial solution to an open problem by Kulikov and Podolskii (Proc. of STACS 2017, Article No.49).

1 Introduction

Let \(\text{MAJ}_n : \{0,1\}^n \to \{0,1\}\) denote the Boolean majority function of \(n\) variables, i.e.,

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

where \(1[\cdot]\) denotes 1 if the condition in the bracket is satisfied, and 0 otherwise. The problem of finding efficient circuits (or formulas) for computing (or approximating) the majority function has attracted many researchers for a long time (see e.g., [1, 4, 6, 7]).

Recently, Kulikov and Podolskii [3] initiated the study to determine the minimum value of \(m\) such that \(\text{MAJ}_n\) can be computed by a depth two circuit of \(\text{MAJ}_m\), denoted by \(\text{MAJ}_m \circ \text{MAJ}_m\).

In addition to proving a lower bound \(m \geq n^{13/19+o(1)}\), they presented the construction of such circuits for \((n, m) = (7, 5), (9, 7)\) and \((11, 9)\) with the help of computer search. However, obtaining non-trivial upper bounds on \(m\) for higher values of \(n\) was left as an open problem in [3].

In this letter, we give a solution to this problem by showing:

Theorem 1 For every odd \(n \geq 7\), there is a \(\text{MAJ}_{n-2} \circ \text{MAJ}_{n-2}\) circuit computing \(\text{MAJ}_n\).
2 Proof of Theorem 1

The proof is constructive. Let \([n] := \{1, 2, \ldots, n\}\). Suppose that \(n = 2k + 1\).

For \(i = 1, \ldots, k + 1\), let
\[
S_i = [n] \setminus \{i, i + 1\},
\]
and for \(i = k + 2, \ldots, 2k - 1\), let
\[
S_i = [n] \setminus \{i + 1, i + 2\}.
\]
For \(i = 1, \ldots, 2k - 1\) except for \(i \in \{2, k\}\), the \(i\)-th bottom gate \(G_i\) is defined as
\[
G_i = 1[\sum_{j \in S_i} x_j \geq k].
\]
(1)
The gate \(G_2\) is defined as
\[
G_2 = 1[2x_1 + \sum_{j \in [n] \setminus \{1,2,3, k+2\}} x_j \geq k],
\]
and the gate \(G_k\) is defined as
\[
G_k = 1[2x_{k+2} + \sum_{j \in [n] \setminus \{1,k,k+1,k+2\}} x_j \geq k].
\]
The output of a circuit is just the majority of all the \(G_i\)s, i.e., \(1[\sum_{i=1}^{n-2} G_i \geq k]\).

It is convenient to represent the coefficients of variables by an \((n - 2) \times n\) matrix; its \((i, j)\)-entry represents the weight of \(x_j\) in \(G_i\). We write this matrix as \(M\), which looks like the following (e.g., for \(n = 11\)).

\[
\begin{array}{cccccccccc}
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
2 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
\end{array}
\]

Below we verify that this circuit computes \(\text{MAJ}_n\).

Let \(\mathbf{x} = (x_1, \ldots, x_n)^T\) be a 0/1-column vector representing an input. Let \(|\mathbf{x}|\) denote the number of 1s in \(\mathbf{x}\). What we should verify is that, for every \(\mathbf{x} \in \{0, 1\}^n\) with \(|\mathbf{x}| \geq k + 1\)
(\(|x| \leq k\), respectively), \(Mx\) has at least \(k\) entries whose value is at least \(k\) (at most \(k-1\), respectively).

In fact, it is sufficient to verify this condition only for \(x\) with \(|x| = k\). The correctness for \(x\) with \(|x| = k + 1\) will follow from the fact that \(\text{MAJ}_{n-2}\) is self-dual, i.e.,

\[
\text{MAJ}_{n-2}(x_1, \ldots, x_{n-2}) = \overline{\text{MAJ}_{n-2}(x_1, \ldots, \overline{x}_{n-2})},
\]

and the constructed circuit is \(\text{MAJ}_{n-2} \circ \text{MAJ}_{n-2}\). Then, all other cases will follow from the monotonicity of our circuit.

Let \(M'\) be an \((n-2) \times n\)-matrix \(M'\) whose \((i, j)\)-entry is \(1 - M_{i,j}\). In term of \(M'\), the condition we should verify can be rewritten as: for every \(x\) with \(|x| = k\), \(y := M'x\) has at least \(k\) entries whose value is strictly positive. The matrix \(M'\) looks like the following (again, for \(n = 11\)), where “-” represents \(-1\).

\[
\begin{array}{cccccccccccc}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & - & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
\end{array}
\]

In what follows, we refer to the first \(k + 2\) entries of \(x\) as \(x_A\), and the rest of them as \(x_B\). Similarly, we refer to the first \(k + 1\) entries of \(y\) as \(y_A\), and the rest of them as \(y_B\). Then, we can write \(y = M'x\) as

\[
\begin{pmatrix}
    y_A \\
    y_B
\end{pmatrix}
= \begin{pmatrix}
    M_A & 0 \\
    0 & M_B
\end{pmatrix}
\begin{pmatrix}
    x_A \\
    x_B
\end{pmatrix},
\]

where \(M_A\) is a \((k + 1) \times (k + 2)\) matrix and \(M_B\) is a \((k - 2) \times (k - 1)\) matrix.

Let \(x\) be an input with \(|x| = k\). Suppose that \(x_B\) has \(\ell\) 1s, and hence \(x_A\) has \(k - \ell\) 1s for some \(0 \leq \ell \leq k - 1\). Then, the number of strictly positive entries in \(y_B\) is \(\ell - 1\) if \(\ell = k - 1\), and at least \(\ell\) if \(\ell < k - 1\). This is obvious by noticing that \(M_B\) is the incidence matrix of the path on \(k - 1\) vertices where the rows (or gates) correspond to edges and the columns (or variables) correspond to vertices. Hence, the proof will be finished if we verify that (i) \(y_A\) has at least two 1s if \(x_A\) has exactly one 1, and (ii) for every \(m\) such that \(2 \leq m \leq k\), \(y_A\) has at least \(m\) strictly positive entries whenever \(x_A\) has \(m\) 1s.

The claim (i) is obvious since every column in \(M_A\) contains two 1s. We divide the verification of the claim (ii) into three subcases.

(iii-1) \(x_1 = x_{k+2} = 0\).
Consider a graph $H_1$ whose incidence matrix is $M_A$ with the first and $(k+2)$-nd columns removed. Namely, $H_1$ is a graph on the vertex set $\{x_2,\ldots,x_{k+1}\}$. The edges of $H_1$ are consisting of a path $x_2 - x_3 - \cdots - x_{k+1}$ and two additional self-loops on $x_2$ and $x_{k+1}$. Here a row having a single 1 is considered to be a self-loop.

By the construction, it is clear that the number of strictly positive element in $y_A$ is equal to the number of edges in $H_1$ that covered by the set of vertices of value 1. Since $H_1$ is a path with self-loops on both terminals, for every $2 \leq m \leq k$, every set of $m$ vertices covers at least $m$ (in fact, at least $m+1$) edges. This establishes the claim.

(ii-2) $x_1 = x_{k+2} = 1$.

In this case, $y_1 \geq 1$ and $y_{k+1} \geq 1$ are forced. Notice that, when $x_1 = x_{k+2} = 1$, the values of $y_2, \ldots, y_k$ are unchanged if we discard the first and $(k+2)$-nd columns of $M_A$. Consider a graph $H_2$ whose incidence matrix is $M_A$ with the first and $(k+2)$-nd columns and also the first and $(k+1)$-st rows removed. The graph $H_2$ is just a path $x_2 - x_3 - \cdots - x_{k+1}$ on the vertex set $\{x_2, \ldots, x_{k+1}\}$.

Let $m' = m - 2$. The claim clearly follows since, for every $0 \leq m' \leq k - 2$, every set of $m'$ vertices covers at least $m'$ edges on the path of $k$ vertices.

(ii-3) $x_1 + x_{k+2} = 1$.

Suppose that $x_1 = 1$ and $x_{k+2} = 0$. (The opposite case is analogous.) In this case, $y_1 \geq 1$ and $y_k \geq 1$ are forced. We consider a graph $H_3$ whose incidence matrix is $M_A$ with the first and $(k+2)$-nd columns and also the first, second and $k$-th rows removed. Namely, $H_3$ is a graph on the vertex set $\{x_2, \ldots, x_{k+1}\}$ consisting of a path $x_3 - x_4 - \cdots - x_k$ and a self-loop on $x_{k+1}$. Here $x_2$ is an isolated vertex.

Let $m' = m - 1$. Observe that the number of strictly positive entries in $y_A$ is equal to the number of edges of $H_3$ that covered by the set of vertices of value 1 plus two (accounting for $y_1$ and $y_k$) plus $1[x_2 + x_3 = 2]$ (accounting for $y_2$). It is easy to check that, for every $1 \leq m' \leq k - 1$, this number is at least $m' + 1$ for every set of $m'$ vertices in $H_3$, which establishes the claim.

Here we describe the idea of our construction. In our circuit, some of the bottom gates (namely, $G_2$ and $G_k$) read a variable multiple times. This is necessary as Kulikov and Podolskii [3, Lemma 11] proved that there is no $\text{MAJ}_{n-2} \circ \text{MAJ}_{n-2}$ circuit for $\text{MAJ}_n$ where every bottom gate reads exactly $n - 2$ distinct variables. A careful inspection of their proof reveals that if we consider a circuit such that every bottom gate $G_i$ is given by Eq. (1) then it outputs an incorrect value only when $x = 10^{k+1}1^{k-1}, 0^{k+1}1^k$ and their complement. We can eliminate these errors by slightly modifying the weights of $G_2$ and $G_k$.

A final remark is that, for every even $n \geq 6$, a $\text{MAJ}_{n-1} \circ \text{MAJ}_{n-1}$ circuit computing $\text{MAJ}_n$ is obtained by fixing an arbitrary variable, say $x_1$, to 1 in the above construction. Currently, we do not know how to construct such a circuit with a smaller fan-in.

Note added: Several papers dealing with the same problem were appeared after the initial submission of this letter. In [2], Engels et al. proved an improved lower bound of $m = \Omega(n^{0.8})$ when the gates are not allowed to read inputs multiple times. In [5], Posobin gave a depth
two circuit for $\text{MAJ}_n$ consisting of gates with fan-in $m = (2/3)n + 4$ where the bottom gates use a threshold value not restricted to $m/2$.

**Acknowledgement**

The authors would like to thank an anonymous referee for their helpful comments. This work was supported in part by JSPS KAKENHI No.15K00006.

**References**


