CIRCUITS CONSTRUCTED WITH MOD\textsubscript{q} GATES CANNOT COMPUTE "AND" IN SUBLINEAR SIZE

DENIS THÉRIEN

Abstract. Algebraic techniques are used to prove that any circuit constructed with MOD\textsubscript{q} gates that computes the AND function must use \( \Omega(n) \) gates at the first level. The best bound previously known to be valid for arbitrary \( q \) was \( \Omega(\log n) \).

Subject classifications. 68Q05, 68Q25, 68Q40.

Introduction

Bounded-depth circuits provide a natural computational framework for boolean functions. In spite of the simplicity of the model, analyzing the exact complexity of explicitly given functions remains a challenge. A landmark result, proved independently by Furst, Saxe and Sipser \cite{5} and Ajtai \cite{1}, asserts that the MOD\textsubscript{q} function cannot be computed in polynomial size and constant depth using AND and OR gates of unbounded fan-in. Yao \cite{12} and Håstad \cite{6} later established that exponentially many gates are in fact required. Razborov \cite{8} and Smolensky \cite{10} improved the result by showing that, when \( p \) is a prime not dividing \( q \), a constant-depth circuit constructed with AND, OR and MOD\textsubscript{p} gates of arbitrary fan-in requires exponentially many AND and OR to compute MOD\textsubscript{q}.

Since MOD\textsubscript{q} is difficult to compute using AND and OR gates, it seems reasonable to conjecture the dual result that the AND function (and hence also the OR function) is difficult to compute using modular counting gates, i.e., that constant-depth circuits of MOD\textsubscript{q} gates require superpolynomial size to compute AND. This is indeed the case if \( q = p^\alpha \) is a prime power: the function computed by an \( n \)-input constant-depth circuit of arbitrary size can be represented by a polynomial in \( \mathbb{Z}_p[x_1, \ldots, x_n] \) of constant degree, whereas such a representation for the AND of \( n \) variables has degree \( n \).

The situation is much less clear when \( q \) is divisible by two distinct primes. It is known that AND (and in fact any boolean function) can be computed
in depth two, but the construction uses exponential size and it is conjectured that it cannot be significantly improved. Smolensky [11] and Barrington [2] observed that $\Omega(\log n)$ MOD$^q$ gates are required to compute AND; in [11] a linear lower bound is obtained for a slightly more complicated function. Our contribution is to prove that any arrangement of MOD$^q$ gates will require $\Omega(n)$ gates at the first level to realize the AND of $n$ variables. The proof is based on algebraic arguments that were introduced in [3].

1. Definitions

For $q > 1$, the boolean function $\text{MOD}_q : \{0, 1\}^n \rightarrow \{0, 1\}$ is defined by

$$\text{MOD}_q(x_1, \ldots, x_n) = \begin{cases} 0 & \text{if } \sum_{i=1}^n x_i \equiv 0 \mod q \\ 1 & \text{otherwise.} \end{cases}$$

We will consider the class $CC(q)$ of boolean circuits constructed with gates computing the MOD$^q$ function.

An $n$-input circuit $C_n$ is defined by a directed acyclic graph: vertices of fan-in 0 (the input gates) are labeled by elements of $\{1, X_1, \ldots, X_n\}$, all other vertices are labeled MOD$^q$, and we assume a unique node of fan-out 0 (the output gate). Such a graph naturally determines a function $C_n : \{0, 1\}^n \rightarrow \{0, 1\}$: given $x \in \{0, 1\}^n$, an input gate labeled $1$ ($X_i$) returns $1$ (the $i$th bit of $x$), an inner vertex returns 0 or 1 according to the MOD$^q$ sum of its entries, and the value of $C_n(x)$ is the value returned by the output gate.

The class $CC(q)$ consists of sequences $C = (C_n)_{n \geq 0}$ where each $C_n$ is an $n$-input circuit as defined above. $C$ naturally defines a function from $\{0, 1\}^*$ into $\{0, 1\}$. We will also call $C^{-1}(1)$ the language recognized by the circuit.

The parameters associated with $C$ are the depth ($d_n$) where $d_n$ is the length of the longest path in $C_n$, and the size ($s_n$) where $s_n$ is the number of inner nodes in $C_n$.

2. An algebraic result

Fix a prime $\alpha + 1 > 2$ and let $F$ denote the field with $\alpha + 1$ elements. Under the group multiplication, $F^* = F - \{0\}$ then forms a cyclic group of order $\alpha$. Choose a generator $g$ for $F^*$; the map $\psi : \mathbb{Z}_\alpha \rightarrow F^*$ given by $c \mapsto g^c$ for any $c$ in $\mathbb{Z}_\alpha$ is thus a bijection and we can identify $(F^*)^n$ with $\{\hat{C} : C \in \mathbb{Z}_\alpha^n\}$ where, for any $C = (c_1, \ldots, c_n)$ in $\mathbb{Z}_\alpha^n$, $\hat{C} = (c_1, \ldots, c_n)$.

For each $n$ we consider the vector space $V_n = \{f : (F^*)^n \rightarrow F\}$. For any $C \in \mathbb{Z}_\alpha^n$, let $\chi_C \in V_n$ be the characteristic function of $\hat{C}$; thus, any $f$ in $V_n$