

Discrete Mathematics Problems. June 25, 2001

Instructor: Laszlo Babai

Definition 0.1 A *Boolean function in n variables* is a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$. The $(0,1)$ -valued input variables are called *Boolean variables*.

Definition 0.2 A *Boolean circuit* is a DAG (directed acyclic graph) with variables and their negations at the input nodes and AND and OR gates at all other nodes. Such a gate computes the AND/OR of the values of the nodes from which an edge points to it. One or several nodes are designated as *output node(s)*. At every node, the circuit computes a Boolean function. The *depth* of the circuit is the longest path from input to output. The *size* of the circuit is the number of *wires* (directed edges).

Exercise 1 Prove that every Boolean function can be computed by a depth-2 Boolean circuit of size $O(n2^n)$.

Exercise 2 Prove that addition of n -bit integers can be done by a depth-3 Boolean circuit of size $O(n^3)$.

Exercise 3 (*)** Multiplication is hard. Show that multiplication of n -bit integers cannot be done by bounded-depth, polynomial-size Boolean circuits. (Polynomial size means size $O(n^C)$ for some constant $C > 0$.)

Definition 0.3 *Parity functions:* $P(x_1, x_2, \dots, x_n) = \sum_{i=1}^n x_i \bmod 2$;
 $\neg P(x_1, x_2, \dots, x_n) = 1 + \sum_{i=1}^n x_i \bmod 2$.

Theorem 0.4 (Ajtai, Furst-Saxe-Sipser, 1980) *Parity cannot be computed in bounded depth and polynomial size.*

Exercise 4 Show that Exercise 3 follows from Theorem 0.4.

Exercise 5 Prove: if a depth-2 circuit computes parity then its size is $\Omega(n2^n)$.

Exercise 6 Compute parity in (a) depth 3, size $O(n2^{\sqrt{n}})$; (b) depth 4, size $O(n2^{n^{\frac{1}{3}}})$; (c) depth d , size $O(n2^{n^{\frac{1}{d-1}}})$; (d) depth $O(\log n)$, size $O(n)$.

Theorem 0.5 (Yao, Hastad, 1985) *To compute parity in depth d requires size $> 2^{cn^{\frac{1}{d-1}}}$, $c = \frac{1}{10}$.*

Definition 0.6 (Pudlák–Rödl, 1992) Let $G = (V, E)$ be a graph. Let X be a vector space over a field \mathbb{F} . A *projective representation of G in X* is a function ρ which assigns to each vertex $i \in V$ a subspace of X , which we will call $W_i = \rho(i)$. To be a representation, ρ must have the property

$$i \sim j \iff W_i \cap W_j \neq \{0\}$$

Definition 0.7 *Projective dimension of G* : $\text{pdim}_{\mathbb{F}}(G) =$ minimum dimension such that there is a projective representation of G over \mathbb{F} of that dimension.

Exercise 7 Let \mathbb{F} be a field and $G = (V, E)$ a graph. Show: (a) $\text{pdim}_{\mathbb{F}}(G) \leq |E|$. (b) If $|\mathbb{F}| \geq |E|$ then $\text{pdim}_{\mathbb{F}}(G) \leq 2\Delta$, where $\Delta = \max_{i \in V} \deg(i)$.

Theorem 0.8 Let f_i be polynomials, and let $Z_{\mathbb{F}}(f_1, \dots, f_m)$ denote the number of zero-patterns of (f_1, \dots, f_m) .

$$Z_{\mathbb{F}}(f_1, \dots, f_m) \leq \binom{md + n}{n}$$

where $d = \max_{1 \leq i \leq n} \deg(f_i)$.

A combination of the following two exercises yields a proof of this theorem.

Exercise 8 Let S_1, \dots, S_M be the supports of the zero-patterns of (f_1, \dots, f_m) and let a_1, \dots, a_M be the corresponding witnesses, i. e., $f_i(a_j) \neq 0 \iff i \in S_j$. Let

$$g_j = \prod_{\ell \in S_j} f_{\ell}.$$

Prove that the polynomials g_1, \dots, g_M are linearly independent.

Exercise 9 The number of monomials (products of powers of variables) of degree $\leq t$ in n variables is $\binom{t+n}{n}$. The number of monomials of degree exactly t in n variables is $\binom{t+n-1}{n-1}$.

Exercise 10 Let $G = (V, E)$ be a graph. If $\text{pdim}_{\mathbb{F}}(G) = d$ then there exists a projective representation of G over \mathbb{F} of dimension $2d$ such that for all $i \in V$, $\dim W_i = d$.

Exercise 11 (*) For any field \mathbb{F} , almost all graphs have projective dimension

$$\text{pdim}_{\mathbb{F}}(G) > c\sqrt{n/\log n}.$$

OPEN PROBLEM. Construct explicit graphs with $\text{pdim}_{\mathbb{F}}(G) > 10 \log n$.

Recommended reading:

Pudlák–Rödl: A combinatorial approach to complexity. *Combinatorica* **12** (1992), 221–226.

Rónyai–Babai–Ganapathy: On the number of zero-patterns of a sequence of polynomials. *Journal of the Amer. Math. Soc.* **14** (2001), 717–735.

[Note: Murali Ganapathy is a CS grad student.]