CS 860 Algebraic Complexity Theory May 15, 2024

Lecture 4: Structural Properties of Algebraic Circuits

Instructor: Rafael Oliveira *Scribe: Andrew Luo*

Remark These notes have not been subjected to the scrutiny of a journal publication, and it may contain errors. If you find one, please contact the instructor.

1 Introduction

Our goal in this lecture is to establish a couple important structural results pertaining to the study of algebraic complexity. The first is the notion of homogenization - the idea that we can extract all monomials of a particular degree of any polynomial. Using this machinery, we will derive a method for efficient division elimination, which allows us to rewrite any circuit to compute the same polynomial without using ÷. Finally, we introduce the notion of a Universal Circuit, analogous to the Universal Turing Machine for the algebraic case.

2 Homogenization

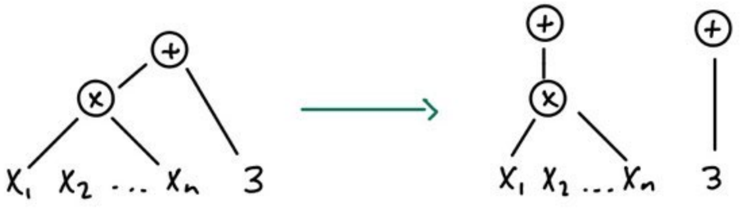
We call a polynomial $f(x_1, ..., x_n) \in \mathbb{F}[x_1, ..., x_n]$ **homogeneous** if all monomials in f have the same degree. An example is $f(x_1, x_2) = x_1^2 + x_1x_2$, which is homogeneous of degree 2.

We can write any polynomial as a sum of its homogeneous components by grouping monomials of the same degree; given $f(\mathbf{x})$ of degree d, we write $f(\mathbf{x}) = \sum_{k=0}^{d} H_k[f]$ where $H_k[f]$ is the k-dimensional homogeneous component of f. We may refer to homogeneous polynomials as **forms**. For example, $f(\mathbf{x}) = x_1^2x_2 + x_3^3$ is a degree 3 form.

The first important result is that we can compute the homogeneous components of f without a large increase in the size of our circuit. More formally,

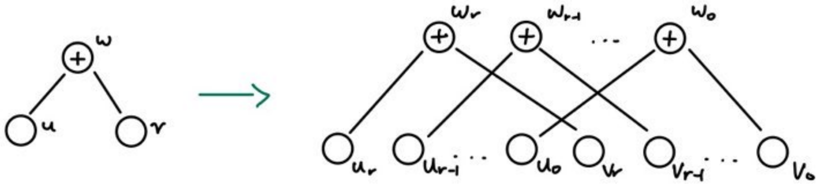
Theorem 1. *If $f(\mathbf{x}) \in \mathbb{F}[x_1, ..., x_n]$ of degree d can be computed by a circuit of size s using $\times$, $+$, and $-$, then $\forall r \leq d$, there exists a homogeneous circuit Φ of size $O(r^2s)$ that computes $H_0[f]$, ..., $H_r[f]$.*

Proof. The proof is by explicitly constructing the new circuit Φ that computes the homogeneous components of f. We will start by modifying each layer of the circuit, inductively starting from the bottom, in such a way that each gate computes a homogeneous polynomial of degree at most d. Note that the bottom layer of our circuit consists just of $x_1, ..., x_n$ and elements of $\mathbb{F}$. Hence, the first layer is already homogeneous.



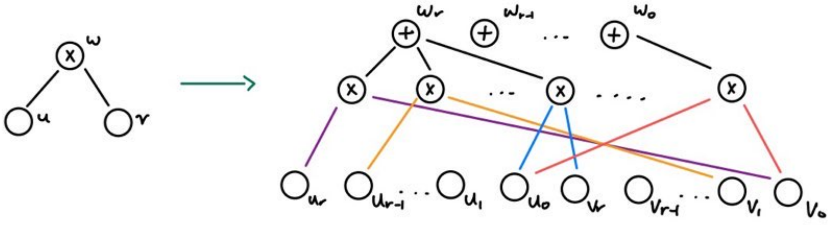
Now, suppose we have an addition or subtraction gate $w = u + v$ as illustrated below, where we assume, via the induction hypothesis, that $u = u_0 + u_1 + ... + u_d$ and $v = v_0 + v_1 + ... + v_d$ where $u_i = H_i[u]$ and

$v_i = H_i[v]$ for $i = 0, 1, ..., d$ were previously computed homogeneous components of u and v from a previous layer.



Then the homogeneous components of w are $w_r = u_r + v_r$, $w_{r-1} = u_{r-1} + v_{r-1}$, ..., $w_0 = u_0 + v_0$.

Instead, suppose we wished to compute $w = u \times v$. Note that given polynomials u_i and v_j of degrees i and j, the degree of $u_i \times v_j$ is $i + j$. Hence, we can compute $w_r = \sum_{i=0}^{r} u_i v_{r-i}$ for any $r \leq d$.



Altogether, we need $r+1$ new gates for each gate in the original circuit to store $w_0, ..., w_r$. For multiplication, we also need up to $3(r+1)^2$ new gates to store intermediate calculations. Hence, our final circuit has size $O(r^2 s)$. □

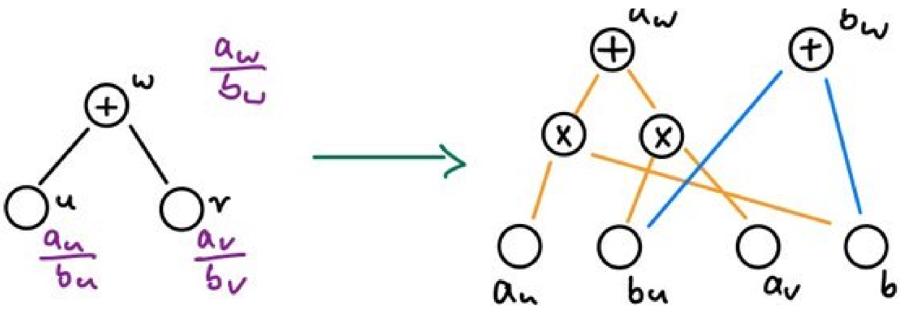
3 Division Elimination

Another major result and our first non-trivial usage of homogenization comes from division elimination, which is the process of re-writing an equivalent circuit that uses no ÷ gate.

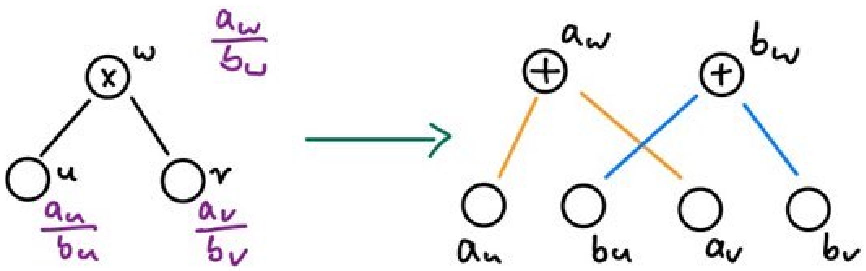
Theorem 2. *If $f(\mathbf{x}) \in F[x_1, ..., x_n]$ is a polynomial of degree d that can be computed by a circuit Ψ of size s using $\times$, $\div$, $+$, and $-$, then there exists a circuit Φ of size poly(s, d) using $\times$, $+$, and $-$ that computes f.*

Proof. Each gate of our circuit computes a rational function; therefore, we can easily modify our circuit to compute the numerator and denominator of the value at each gate separately.

Suppose $w = u + v$, where the rational function computed at w, u, and v are $\frac{a_w}{b_w}$, $\frac{a_u}{b_u}$, and $\frac{a_v}{b_v}$, respectively. Then $a_w = a_u b_v + a_v b_u$ and $b_w = b_u b_v$. Hence, computing a_w and b_w requires an additional 4 gates, as illustrated below. Note that subtraction is similar.



Next, suppose $w = u \times v$. Then $a_w = a_u b_u$ and $b_w = a_v b_v$. Similarly, if $w = u \div w$, $a_w = a_u b_v$ and $b_w = b_u a_v$.



Hence, we assume our circuit can be broken into $\Psi_1 \div \Psi_2$ where Ψ_1 and Ψ_2 are circuits of size at most $5s$ that use no division gates. Say Ψ_1 and Ψ_2 compute a_s and b_s, respectively, so that $f = \frac{a_s}{b_s}$ and b_s is not identically 0. We may also assume that $b_s(\mathbf{0}) = 1$; if $b_s(\mathbf{0}) \neq 0$, then we may construct $\left(\Psi_1 \times b_s(0)^{-1}\right) \div \left(\Psi_2 \times b_s(0)^{-1}\right)$ to achieve the same result. If $b_s(\mathbf{0}) = 0$, we may find $\bar{\mathbf{x}}$ such that $b_s(\bar{\mathbf{x}}) \neq 0$. Via variable substitution, we can construct the circuit for $f(x_1 - \bar{x}_1, ..., x_n - \bar{x}_n)$ and shift the variables at the beginning to compute $f(x_1, ..., x_n)$.

Write $b_s = 1 - \tilde{b}$ where $\tilde{b}$ has min degree ≥ 1 and max degree $d = \deg b_s$. Then, $f = \frac{a_s}{b_s} = \frac{a_s}{1 - \tilde{b}} \implies f(x) = a_s(1 + \tilde{b} + ... + \tilde{b}^d) + H(x)$ where $H(x)$ has min degree $\geq d + 1$. By Theorem 1, we can compute the degree $\leq d$ components of $a_s(1 + \tilde{b} + ... + \tilde{b}^d)$ with a circuit of size $O(d^2(5s + d))$, which is exactly $f(x)$. □

Remark This formulation only works with circuits, *not formulas*, since it is crucial in the proof that we are reusing gates when performing addition. It is currently an open problem whether or not division elimination can be done efficiently for formulas in general.

4 Universal Circuits

We end off this lecture by introducing the notion of a Universal Circuit, analogous to the universal Turing Machine for the algebraic case.

Definition 3 (Universal Circuits)**.** *A circuit Φ is said to be (n, s, d)-**universal** for circuits of input size n, output size n, and size s if for any n forms $f_1(x_1, ..., x_n), ..., f_n(x_1, ..., x_n)$ of degree at most d that can be simultaneously computed by a circuit of size s, then there is a circuit Ψ computing $f_1, ..., f_n$ such that the computation graph of Ψ is exactly that of Φ.*

*In other words, we say Ψ is a **projection** of Φ.*

In the next lecture, we will show that such a circuit exists, and is not too large.

References