Electronic Colloquium on Computational Complexity, Report No. 124 (2007)

Diagonal Circuit Identity Testing and Lower Bounds

Nitin Saxena
Centrum voor Wiskunde en Informatica
Amsterdam, The Netherlands
ns@cwi.nl

November 23, 2007

Abstract

In this paper we give the first deterministic polynomial time algorithm for testing whether a *diagonal* depth-3 circuit $C(x_1,\ldots,x_n)$ (i.e. C is a sum of powers of linear functions) is zero. We also prove an exponential lower bound showing that such a circuit will compute determinant or permanent only if there are exponentially many linear functions. Our techniques generalize to the following new results:

1. Suppose we are given a depth-3 circuit (over any field $\mathbb{F}$) of the form:

$$C(x_1,\ldots,x_n) := \sum_{i=1}^{k} \ell_{i,1}^{e_{i,1}} \cdots \ell_{i,s}^{e_{i,s}}$$

where, the $\ell_{i,j}$'s are linear functions living in $\mathbb{F}[x_1,\ldots,x_n]$. We can test whether C is zero deterministically in $poly\,(nk, max\{(1+e_{i,1})\cdots(1+e_{i,s}) \mid 1 \leqslant i \leqslant k\})$ field operations. This immediately gives a deterministic $poly(nk2^d)$ time identity test for general depth-3 circuits of degree d.

2. We prove that if the above circuit $C(x_1,\ldots,x_n)$ computes the determinant (or permanent) of an $m \times m$ formal matrix with a "small" $s = o\left(\frac{m}{\log m}\right)$ then $k = 2^{\Omega(m)}$. Our lower bounds work for all fields $\mathbb{F}$. (Previous exponential lower bounds for depth-3 only work for nonzero characteristic.)

3. We present applications of our ideas to depth-4 circuits and an exponentially faster identity test for homogeneous diagonal circuits (deterministically in $poly(n\,k\log(d))$ field operations over finite fields).

1 Introduction

Identity Testing is the problem of checking whether a given arithmetic circuit $C(x_1,\ldots,x_n)$, computing a polynomial over a field $\mathbb{F}$, is the zero circuit. Ideally we would like to do identity testing deterministically in time polynomial in the size of the circuit C but no such algorithm is known. The simplest known general algorithm is randomized which was discovered independently by Schwartz [Sch80] and Zippel [Zip79]: it evaluates the given circuit at a random point and accepts if and only if the circuit evaluates to zero

ISSN 1433-8092

at that point. There are more involved randomized algorithms that use fewer random bits [CK00, LV98, AB03]. Besides being a natural algebraic problem, special cases of identity testing also appear in primality testing [AKS04], testing equivalence of read-once branching programs [BCW80], graph matching problems [Lov79], interpolating sparse multivariate polynomials [GKS90, CDGK91] and proving complexity theory results such as IP=PSPACE [LFK92, Sha92], NP=PCP($O(\log n)$, $O(1)$) [ALM$^+$98, AS98]. Solving identity testing becomes all the more important by the work of Impagliazzo and Kabanets [IK04] who showed that – finding a deterministic algorithm for identity testing is, roughly, equivalent to proving circuit lower bounds for NEXP.

In this paper we consider arithmetic circuits of depth 3 and solve the identity testing problem for a natural restricted case (we call them *diagonal circuits*)– when the circuit $C(x_1, \ldots, x_n)$ is a sum of powers of linear functions. Our basic technique is to express the multiplication gate $(a_0 + a_1x_1 + \cdots + a_nx_n)^d$ in a *dual* form:

$$\sum_j f_{j,1}(x_1) \cdots f_{j,n}(x_n)$$

which can then be viewed as a circuit in which the variables $x_1, \ldots, x_n$ do not commute. Thus, by the identity test for noncommutative formulas of Raz and Shpilka [RS05] we get a deterministic polynomial time identity test for diagonal circuits. Also, the lower bounds for pure circuits by Raz and Shpilka [RS05] apply and we get that a diagonal circuit can compute determinant or permanent only if it is of exponential size. We show that the identity test as well as the lower bounds generalize to depth-3 circuits of the form:

$$C(x_1, \ldots, x_n) := \sum_{i=1}^{k} \ell_{i,1}^{e_{i,1}} \cdots \ell_{i,s}^{e_{i,s}}$$

over any field provided the $max\{(1+e_{i,1}) \cdots (1+e_{i,s}) \mid 1 \leqslant i \leqslant k\}$ is at most a polynomial in $size(C)$. As an immediate corollary we get an identity test for general depth-3 circuits C that runs in time $poly(nk2^d)$ where d is the maximum degree of the polynomial computed by a multiplication gate in C. These results also generalize (to some extent) to depth-4 circuits. Our technique of computing the dual is a new way to unfold a multiplication gate in an arithmetic circuit. This dual computation is faster than a brute-force expansion and may have other applications. (Usage of the term “dual” is justified in Remark 18.)

1.1 Known Results

There are deterministic algorithms known for identity testing only over restricted classes of arithmetic circuits. Raz and Shpilka [RS05] gave a deterministic polynomial time identity test for noncommutative arithmetic formulas. Dvir and Shpilka [DS05] attempted a characterization of zero depth-3 circuits and obtained a $poly(n, 2^{\log^{k-1} d})$ time identity test. Kayal and Saxena [KS07] used Chinese remaindering over local rings and gave a $poly(nd^k)$ time identity test for depth-3 circuits which is clearly a polynomial time identity test if k, the top fanin of the circuit, is bounded. In this work we allow the top fanin to be unbounded but impose the restriction that each multiplication gate has only “few” *distinct* linear functions as input.

In this paper we also prove exponential lower bounds for computing determinant or permanent by certain restricted depth-3 circuits. These restricted depth-3 circuits are the ones for which we give a deterministic polynomial time identity test. Grigoriev, Karpinski and Razborov [GK98, GR00] have also shown such lower bounds for general depth-3 circuits but assuming a nonzero characteristic. Our lower bounds are new in the sense that they hold over all fields. Raz [Raz04] has shown super-polynomial lower bounds on the size of multi-linear formulas that compute determinant or permanent. Our lower bounds apply to diagonal depth-3 circuits which can be viewed as an extreme case orthogonal to that of multi-linear depth-3 circuits. There are many other lower bound results that are quite incomparable to ours – exponential lower bound for determinant and permanent on noncommutative formulas [Nis91]; exponential lower bound for symmetric polynomials and iterated matrix product on homogeneous depth-3 circuits [NW97]; quadratic lower bounds for determinant, symmetric polynomials and iterated matrix product on general depth-3 circuits [SW01].

1.2 Definitions and Statement of Results

We will use $poly(M, N)$ to refer to a real function in M and N whose value is upper bounded by $(MN)^{c_1}$ for all $M, N > c_2$ where $c_1, c_2 > 0$ are absolute constants. When using $poly(M, N)$ we will not specify the value of c_1, c_2 as our main interest in this paper is only in their existence. We will use $[n]$ to refer to the set $\{1, \ldots, n\}$. We will denote the characteristic of a field $\mathbb{F}$ (i.e. smallest integer $t > 0$ such that $t = 0$ in $\mathbb{F}$ or zero if there is no such t) by $char(\mathbb{F})$. An algebra R over a field $\mathbb{F}$ is simply a ring containing $\mathbb{F}$. In this paper only finite dimensional commutative algebras appear, i.e. there is an integer $N > 0$ and basis elements $b_1, \ldots, b_N \in R$ such that any element in R can be uniquely expressed as $\sum_{i=1}^{N} \alpha_i b_i$ with α_i's in $\mathbb{F}$. We call N the *dimension* of the algebra R over $\mathbb{F}$, denoted by $dim(R)$. It is a simple exercise to see that basic operations (e.g. multiplication of two elements) in R can be done using $poly(N)$ field operations (in $\mathbb{F}$).

Our main concern in this paper are depth-3 circuits. For the purposes of identity testing (also lower bounds for determinant and permanent) the hardest case is when the circuit has an addition gate at the top. These circuits are called $\Sigma\Pi\Sigma$. It is clear that the output of such a $\Sigma\Pi\Sigma$ circuit $C(x_1, \ldots, x_n)$ would be:

$$\sum_{i=1}^{k} \ell_{i,1} \cdots \ell_{i,d_i}$$

where, the $\ell_{i,j} = (a_{i,j,0} + a_{i,j,1}x_1 + \cdots + a_{i,j,n}x_n)$ are linear functions over a field $\mathbb{F}$. We call k the top fanin of C, d_i the degree of the i-th multiplication gate and $d = max_i\{d_i\}$ the degree of C. The size of the circuit C, $size(C)$, is dominated by knd. It is easy to see that by brute-force we can check whether a $\Sigma\Pi\Sigma$ circuit C is a zero circuit in time polynomial in $k \cdot \binom{n+d}{d}$ but this is generally exponential in $size(C)$.

In this paper we solve the case when each of the multiplication gates in a $\Sigma\Pi\Sigma$ circuit $C(x_1, \ldots, x_n)$ has only "few" distinct linear functions as input. For instance, when each of the multiplication gates in C has only one distinct linear function as input then we call C a *diagonal* circuit and it looks like:

$$C(x_1, \ldots, x_n) = \sum_{i=1}^{k} b_i \cdot \ell_i^{d_i}$$

where the b_i's are in $\mathbb{F}$ and the ℓ_i's are linear functions.

Example 1. *A simple diagonal circuit that is zero over $\mathbb{F}_3$ is:*

$$C(x,y) = 2x^2 + 2y^2 + x^3 + 2y^3 - (x+y)^2 - (x-y)^2 + (2x+y)^3$$

In general, we assume that each of the multiplication gates in C has at most s distinct linear functions as input and then the circuit looks like:

$$C(x_1, \ldots, x_n) := \sum_{i=1}^{k} \ell_{i,1}^{e_{i,1}} \cdots \ell_{i,s}^{e_{i,s}} \tag{1}$$

The identity test and lower bounds we give for such circuits are more interesting when $max\{(1+e_{i,1})\cdots(1+e_{i,s}) \mid 1 \leqslant i \leqslant k\}$ is "small", i.e. at most a polynomial in $size(C)$. Our first main theorem is:

Theorem 2. *Over any field $\mathbb{F}$, let C be a circuit given as in Equation (1). Then we can deterministically check whether C is a zero circuit in $poly(nk, max\{(1+e_{i,1})\cdots(1+e_{i,s}) \mid 1 \leqslant i \leqslant k\})$ field operations.*

Depending on how big are s and the degrees $e_{i,j}$'s we get the following two immediate corollaries. When s is really small, say a constant, we get:

Corollary 3. *Over any field $\mathbb{F}$, let C be a depth-3 circuit given as in Equation (1) with a constant s. Then we can do identity testing in deterministic polynomial time ($poly(nkd^s)$ field operations).*

For the largest s, i.e. $s = d$, we get the following result which is better than the brute-force identity test.

Corollary 4. *Over any field $\mathbb{F}$, let C be a depth-3 circuit with n variables, top fanin k and degree d. Then we can do identity testing deterministically in $poly(nk2^d)$ field operations.*

The lower bounds that we get, basically show that if a depth-3 circuit computes determinant (or permanent) then either some of the multiplication gates have "lots" of distinct linear functions as inputs or the top fanin of the circuit is exponential. Our second main theorem is:

Theorem 5. *Over any field $\mathbb{F}$, if the circuit in Equation (1) expresses the determinant (or permanent) of a general $m \times m$ matrix with parameters $s = o\left(\frac{m}{\log m}\right)$, $n = m^2$ and $d = poly(m)$ then $k = 2^{\Omega(m)}$.*

As an immediate corollary we get the following nondiagonalization-of-determinant result.

Corollary 6. *Over any field $\mathbb{F}$, determinant (or permanent) cannot be expressed as a sum of polynomially-many powers of linear functions.*

The above two main theorems also generalize to depth-4 circuits of the form:

$$C(x_1, \ldots, x_n) = \sum_{i=1}^{k} L_{i,1}^{e_{i,1}} \cdots L_{i,s}^{e_{i,s}}$$

where the $L_{i,j}$'s are not linear functions but sums of univariate polynomials, i.e. for all $i \in [k], j \in [s]$:

$$L_{i,j}(x_1, \ldots, x_n) = g_{i,j,1}(x_1) + \cdots + g_{i,j,n}(x_n)$$

where $g_{i,j,j'} \in \mathbb{F}[x_{j'}]$.

1.3 Our Techniques

We use non-black-box methods, i.e. we heavily use the structure of the given circuit. We use tools that previously have been used to understand noncommutative formulas, for example by Nisan, Wigderson [Nis91, NW97], Raz and Shpilka [RS05]. We apply these old tools in a nontrivial way to understand depth-3 and depth-4 (commutative) circuits. For clarity let us present here the two old theorems in a form that we need.

A circuit $D(x_1, \ldots, x_n)$, over an algebra R over a field $\mathbb{F}$, is called noncommutative if each of its multiplication gate has ordered inputs and the variables $x_1, \ldots, x_n$ do not commute, i.e. for all $i \neq j$, $x_i \cdot x_j \neq x_j \cdot x_i$. The output $D(x_1, \ldots, x_n)$ is a formal expression in the ring $R\{x_1, \ldots, x_n\}$ of polynomials over noncommutative variables $x_1, \ldots, x_n$. Clearly, any commutative circuit $C(x_1, \ldots, x_n)$ can be turned into a noncommutative circuit $\tilde{C}(x_1, \ldots, x_n)$ by imposing an order on the inputs to its multiplication gates and assuming $x_i \cdot x_j \neq x_j \cdot x_i$ for all $i \neq j$. But now circuits C and $\tilde{C}$ are computing different polynomials and it may happen that C is a zero circuit but $\tilde{C}$ is a nonzero circuit. However, if $\tilde{C}$ is a zero circuit then C is surely a zero circuit as well. A circuit is called a *formula* if the fan-out of every gate in the circuit is at most one. Noncommutative formulas are easier to analyze compared to the commutative ones and the following identity test is relevant to us:

Theorem 7 (Theorem 2.5 of [RS05])**.** *Let R be an algebra over a field $\mathbb{F}$. Given a noncommutative formula $C(x_1, \ldots, x_n) \in R\{x_1, \ldots, x_n\}$ we can verify deterministically in $poly(size(C), dim(R))$ field operations whether C is zero.*

The second result relevant to us is a special case of Theorem 5.1 of [RS05] that proves lower bounds for pure circuits using the partial derivative space (see the proof idea in Lemma 5.3 of [RS05]).

Theorem 8 (by Theorem 5.1 of [RS05])**.** *Let R be an algebra over a field $\mathbb{F}$, $r \in R \setminus \{0\}$, $r' \in R$ and let $det(x_{1,1}, \ldots, x_{n,n})$ denote the determinant of a formal $n \times n$ matrix $((x_{i,j}))$. If $det(x_{1,1}, \ldots, x_{n,n}) \cdot r - r'$ can be expressed as a circuit:*

$$C(x_{1,1}, \ldots, x_{n,n}) = \sum_{i=1}^{k} f_{i,1,1}(x_{1,1}) \cdots f_{i,n,n}(x_{n,n})$$

where, the f_{i,j_1,j_2}'s are univariate polynomials over R. Then $k \cdot dim(R) = 2^{\Omega(n)}$. A similar lower bound holds for the permanent as well.

Our main contribution is a novel way to transform the multiplication gates of a depth-3 circuit, hence the overall circuit, to a form on which we can apply Theorems 7 and 8. Our basic technique is to express the multiplication gate $(a_0 + a_1x_1 + \cdots + a_nx_n)^d$ in a *dual* form:

$$\sum_j f_{j,1}(x_1) \cdots f_{j,n}(x_n)$$

where the $f_{j,j'}$'s are univariate polynomials over $\mathbb{F}$. Now this is a nice circuit as the variables $x_1, \ldots, x_n$ in it are "separated" and we can invoke the known tricks. For example, it can be viewed as a circuit in which the variables $x_1, \ldots, x_n$ do not commute, thus by Theorem 7 we get a deterministic polynomial time identity test for diagonal circuits. Also, by the lower bounds of Theorem 8 we get that a diagonal circuit can compute determinant or permanent only if it is of exponential size. These ideas easily generalize to circuits with $s > 1$ in Equation (1) but then we work on larger algebras instead of working on the base field $\mathbb{F}$.

1.4 Organization

The paper is organized as follows. In section 2 we present our results for the basic case of diagonal circuits over zero characteristic. In section 3 we show how to extend our results to general circuits of Equation (1) over zero characteristic. In section 4 we extend the previous results to nonzero characteristic, thus finishing the proof of our main Theorems 2 and 5. Finally, in section 5 we present some applications of our results to depth-4 circuit identity testing and an exponentially faster identity test for homogeneous diagonal circuits (deterministically in $poly(nk\log(d))$ field operations over finite fields).

2 The Diagonal Depth-3 Circuits

The aim of this section is to define a dual expression for multiplication gates of the form $(a_0 + a_1x_1 + \cdots + a_nx_n)^d$ and use that form to give an identity test for diagonal circuits and to prove lower bounds. We will assume throughout this section that the base field $\mathbb{F}$ is of characteristic zero.

2.1 Dual of a Multiplication Gate

Given a multiplication gate $(a_0 + a_1x_1 + \cdots + a_nx_n)^d$ we would like to express it as:

$$\sum_{i=1}^{t} f_{i,1}(x_1)\cdots f_{i,n}(x_n)$$

where the $f_{i,j}$'s are univariate polynomials over $\mathbb{F}$ and $t = poly(dn)$. This expression with variables $x_1, \ldots, x_n$ "separated" we call a *dual* of the multiplication gate. The following lemma shows that such a dual is easily computable.

Lemma 9. *Let $a_0, a_1, \ldots, a_n$ be in a field $\mathbb{F}$ of zero characteristic. Then we can compute univariate polynomials $f_{i,j}$'s in $poly(nd)$ field operations such that for $t = (nd + d + 1)$:*

$$(a_0 + a_1x_1 + \cdots + a_nx_n)^d \;=\; \sum_{i=1}^{t} f_{i,1}(x_1)\cdots f_{i,n}(x_n)$$

Proof. We will prove this using the formal power series: $\exp(x) = 1 + x + \frac{x^2}{2!} + \cdots$, where $\exp(x) = e^x$ and e is the base of natural logarithm. Define the degree d truncation of the series to be $E_d(x) = 1 + x + \cdots + \frac{x^d}{d!}$. Observe that:

$$\begin{aligned}(d!)^{-1}\cdot(a_0 + a_1x_1 + \cdots + a_nx_n)^d \;&=\; \text{coefficient of } z^d \text{ in } \exp\left((a_0 + a_1x_1 + \cdots + a_nx_n)\cdot z\right)\\ &=\; \text{coefficient of } z^d \text{ in } \exp(a_0z)\cdot\exp(a_1x_1z)\cdots\exp(a_nx_nz)\\ &=\; \text{coefficient of } z^d \text{ in } E_d(a_0z)\cdot E_d(a_1x_1z)\cdots E_d(a_nx_nz)\end{aligned}$$

The product $E_d(a_0z) \cdot E_d(a_1x_1z) \cdots E_d(a_nx_nz)$ can be viewed as a univariate polynomial in z of degree $(nd+d)$. Hence, its coefficient of z^d can be computed by evaluating the polynomial at $(nd+d+1)$ distinct points $\alpha_1, \ldots, \alpha_{nd+d+1} \in \mathbb{F}$ (remember $\mathbb{F}$ is large enough) and by interpolation we can compute $\beta_1, \ldots, \beta_{nd+d+1} \in \mathbb{F}$ such that:

$$\begin{aligned}&\text{coefficient of } z^d \text{ in } E_d(a_0z) \cdot E_d(a_1x_1z) \cdots E_d(a_nx_nz)\\ &= \sum_{i=1}^{nd+d+1} \beta_i \cdot E_d(a_0\alpha_i) \cdot E_d(a_1\alpha_ix_1) \cdots E_d(a_n\alpha_ix_n)\end{aligned}$$

This is the dual form of $(a_0 + a_1x_1 + \cdots + a_nx_n)^d$ as required. It is routine to verify that all the univariate polynomials $E_d(\cdot)$ in the above sum can be computed in $poly(nd)$ field operations. □

Remark 10. *The trick of looking at the coefficients of $exp(g(x_1, \ldots, x_n) \cdot z)$ is originally due to Newton and also occurs in [SW01] (proof of Theorem 5.3).*

2.2 Identity Test and Lower Bounds

The dual form of multiplication gates obtained in Lemma 9 is easy to analyze and test for zero. We give the ideas in the following theorem.

Theorem 11. *Over zero characteristic, identity testing for diagonal circuits can be done in deterministic polynomial time ($poly(nkd)$ field operations).*

Proof. Suppose we are given a diagonal circuit C:

$$C(x_1, \ldots, x_n) = \sum_{i=1}^{k} b_i \cdot \ell_i^{d_i}$$

Then by Lemma 9 we can compute the dual form of each of the k multiplication gates such that:

$$C(x_1, \ldots, x_n) = \sum_{i=1}^{k} \sum_{j=1}^{nd_i+d_i+1} f_{i,j,1}(x_1) \cdots f_{i,j,n}(x_n) \tag{2}$$

where the univariate polynomials $f_{i,j,j'}$'s are of degree at most d_i.

Now observe that the variables in the circuit on the RHS of Equation (2) can be assumed to be noncommutative without affecting the output, i.e. circuit C. Thus, if we apply the identity testing algorithm of Theorem 7 to the circuit on the RHS of Equation (2) we will correctly know whether C is zero or not. Hence, C can be verified for zeroness in deterministic $poly(nkd)$ field operations. □

The noncommutative form of the circuit on the RHS of Equation (2) also gives us a lower bound for determinant (and permanent) over diagonal circuits.

Theorem 12. *Over zero characteristic, if a diagonal circuit expresses the determinant (or permanent) of a formal $m \times m$ matrix with $n = m^2$ variables and degree $d = poly(m)$ then the top fanin $k = 2^{\Omega(m)}$.*

Proof. Suppose a diagonal circuit C computes the determinant of a general $m \times m$ matrix. Then by Lemma 9 determinant is being computed by a circuit as given in Equation (2). Now the exponential lower bound of Theorem 8 applies and we get that $poly(ndk) = 2^{\Omega(m)}$ implying $k = 2^{\Omega(m)}$. □

3 Extension to General Depth-3 Circuits

In this section we extend the results of the last section to general depth-3 circuits (with some success). We now define a dual expression for multiplication gates of the form $\ell_1^{e_1} \cdots \ell_s^{e_s}$ where the ℓ_i's are linear functions in $\mathbb{F}[x_1, \ldots, x_n]$. The proof is along the same lines as presented before but now we will work in algebras over $\mathbb{F}$ to get the dual form of a general multiplication gate. Finally, we use that form to give identity test and prove lower bounds. We will again assume throughout this section that the base field $\mathbb{F}$ is of characteristic zero.

3.1 Dual of a Multiplication Gate

Given a multiplication gate $\ell_1^{e_1} \cdots \ell_s^{e_s}$, where the ℓ_i's are linear functions in $\mathbb{F}[x_1, \ldots, x_n]$, we would like to express it as an expression:

$$\sum_{i=1}^{t} f_{i,1}(x_1) \cdots f_{i,n}(x_n)$$

where the $f_{i,j}$'s are univariate polynomials over an $\mathbb{F}$-algebra R (unlike the diagonal case where we worked over $\mathbb{F}$) and $t = poly(nd)$ where $d = (e_1 + \cdots + e_s)$. This expression with variables $x_1, \ldots, x_n$ "separated" we call a *dual* of the multiplication gate. The following lemma shows that such a dual is computable but we pay a price in terms of the dimension of algebra R which is $(e_1 + 1) \cdots (e_s + 1)$.

Lemma 13. *Let $\ell_i = (a_{i,0} + a_{i,1}x_1 + \cdots + a_{i,n}x_n)$, for all $i \in [s]$, be linear functions over a field $\mathbb{F}$ of zero characteristic and $d = (e_1 + \cdots + e_s)$. Then we can compute univariate polynomials $f_{i,j}$'s over an algebra $R := \mathbb{F}[z_1, \ldots, z_s]/(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$ in $poly(n, dim(R))$ field operations such that for $t = (nd + d + 1)$:*

$$\ell_1^{e_1} \cdots \ell_s^{e_s} \cdot z_1^{e_1} \cdots z_s^{e_s} = \sum_{i=1}^{t} f_{i,1}(x_1) \cdots f_{i,n}(x_n) \quad \text{over } R$$

Proof. We will again prove this using the formal power series: $\exp(x) = 1 + x + \frac{x^2}{2!} + \cdots$, where $\exp(x) = e^x$ and e is the base of natural logarithm. Recall that the degree d

truncation of the series is $E_d(x) = 1 + x + \cdots + \frac{x^d}{d!}$. Observe that:

$$\begin{aligned}
&(e_1! \cdots e_s!)^{-1} \cdot \ell_1^{e_1} \cdots \ell_s^{e_s} \\
&\quad = \text{ coefficient of } z^d z_1^{e_1} \cdots z_s^{e_s} \text{ in } \exp(\ell_1 z_1 z) \cdots \exp(\ell_s z_s z) \\
&\quad = \text{ coefficient of } z^d z_1^{e_1} \cdots z_s^{e_s} \text{ in } \exp(\ell_1 z_1 z + \cdots + \ell_s z_s z) \\
&\quad = \text{ coefficient of } z^d z_1^{e_1} \cdots z_s^{e_s} \text{ in } \exp\left((a_{1,0} z_1 + \cdots + a_{s,0} z_s) z\right) \cdots \\
&\qquad\quad \cdots \exp\left((a_{1,1} z_1 + \cdots + a_{s,1} z_s) x_1 z\right) \cdots \exp\left((a_{1,n} z_1 + \cdots + a_{s,n} z_s) x_n z\right) \\
&\quad = \text{ coefficient of } z^d z_1^{e_1} \cdots z_s^{e_s} \text{ in } E_d\left((a_{1,0} z_1 + \cdots + a_{s,0} z_s) z\right) \cdots \\
&\qquad\quad \cdots E_d\left((a_{1,1} z_1 + \cdots + a_{s,1} z_s) x_1 z\right) \cdots E_d\left((a_{1,n} z_1 + \cdots + a_{s,n} z_s) x_n z\right) \qquad (3)
\end{aligned}$$

Note that the last product can be viewed as a univariate polynomial in z of degree $(nd+d)$. Hence, its coefficient of z^d can be computed by evaluating the polynomial at $(nd+d+1)$ distinct points $\alpha_1, \ldots, \alpha_{nd+d+1} \in \mathbb{F}$ (remember that $\mathbb{F}$ is large enough) and by interpolation we can compute $\beta_1, \ldots, \beta_{nd+d+1} \in \mathbb{F}$ such that:

$$\begin{aligned}
&\text{coefficient of } z^d z_1^{e_1} \cdots z_s^{e_s} \text{ in } E_d\left((a_{1,0} z_1 + \cdots + a_{s,0} z_s) z\right) \cdot E_d\left((a_{1,1} z_1 + \cdots + a_{s,1} z_s) x_1 z\right) \cdots \\
&\qquad \cdots E_d\left((a_{1,n} z_1 + \cdots + a_{s,n} z_s) x_n z\right) \\
&\ = \text{ coefficient of } z_1^{e_1} \cdots z_s^{e_s} \text{ in } \sum_{i=1}^{nd+d+1} \beta_i \cdot E_d\left((a_{1,0} z_1 + \cdots + a_{s,0} z_s) \alpha_i\right) \cdots \\
&\qquad \cdots E_d\left((a_{1,1} z_1 + \cdots + a_{s,1} z_s) x_1 \alpha_i\right) \cdots E_d\left((a_{1,n} z_1 + \cdots + a_{s,n} z_s) x_n \alpha_i\right)
\end{aligned}$$

Notice that the monomials having nonzero coefficients in the above sum are of the form $z_1^{t_1} \cdots z_s^{t_s}$ such that $t_1 + \cdots + t_s = d = e_1 + \cdots + e_s$. Thus, if we look at the above sum modulo the ideal $(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$ then the surviving monomials $z_1^{t_1} \cdots z_s^{t_s}$ would be those that have $t_1 \leqslant e_1, \ldots, t_s \leqslant e_s$ which together with $t_1 + \cdots + t_s = d = e_1 + \cdots + e_s$ uniquely determines the surviving monomial as $z_1^{e_1} \cdots z_s^{e_s}$. Consequently, we can summarize the above computations as:

$$\begin{aligned}
&(e_1! \cdots e_s!)^{-1} \cdot \ell_1^{e_1} \cdots \ell_s^{e_s} \cdot z_1^{e_1} \cdots z_s^{e_s} \\
&\quad = \sum_{i=1}^{nd+d+1} \beta_i \cdot E_d\left((a_{1,0} z_1 + \cdots + a_{s,0} z_s) \alpha_i\right) \cdot E_d\left((a_{1,1} z_1 + \cdots + a_{s,1} z_s) x_1 \alpha_i\right) \cdots \\
&\qquad\qquad \cdots E_d\left((a_{1,n} z_1 + \cdots + a_{s,n} z_s) x_n \alpha_1\right) \quad \text{over } R
\end{aligned}$$

This is the dual form of $\ell_1^{e_1} \cdots \ell_s^{e_s}$ as required. Notice that there is a nonconstant factor $z_1^{e_1} \cdots z_s^{e_s}$ appearing on the LHS but since this factor is a nonzero element of the algebra R, the dual form will be good enough for our purposes. It is routine to verify that the univariate polynomials $E_d(\cdot)$ over R in this sum can be computed in $poly(n, dim(R))$ field operations and that the dimension of R is $(e_1 + 1) \cdots (e_s + 1)$. □

3.2 Identity Test and Lower Bounds

Suppose that we are given a general depth-3 circuit C over a field $\mathbb{F}$ of zero characteristic:

$$C(x_1, \ldots, x_n) := \sum_{i=1}^{k} \ell_{i,1}^{e_{i,1}} \cdots \ell_{i,s}^{e_{i,s}}$$

We can now apply the dual form of Lemma 13 to each of the k multiplication gates and work on a bigger algebra. We formalize this idea in the following theorems.

Theorem 14. *Given a circuit C of degree d over a field $\mathbb{F}$ of zero characteristic:*

$$C(x_1,\ldots,x_n) = \sum_{i=1}^{k} \ell_{i,1}^{e_{i,1}} \cdots \ell_{i,s}^{e_{i,s}}$$

where the $\ell_{i,j}$'s are linear functions and (wlog) for all $i, e_{i,1} \neq 0$. We can test whether C is a zero circuit deterministically in poly $(nk, max\{(1+e_{i,1})\cdots(1+e_{i,s}) \mid 1 \leqslant i \leqslant k\})$ field operations.

Proof. Let us apply the dual form of Lemma 13 to the i-th multiplication gate, of degree d_i, and compute the univariate polynomials f_{i,j_1,j_2}'s, for all $1 \leqslant j_1 \leqslant t_i = (nd_i + d_i + 1)$ and $j_2 \in [n]$, over the algebra $R_i := \mathbb{F}[z_{i,1},\ldots,z_{i,s}]/(z_{i,1}^{e_{i,1}+1},\ldots,z_{i,s}^{e_{i,s}+1})$ in $poly(n, dim(R_i))$ field operations such that:

$$\ell_{i,1}^{e_{i,1}} \cdots \ell_{i,s}^{e_{i,s}} \cdot z_{i,1}^{e_{i,1}} \cdots z_{i,s}^{e_{i,s}} \ = \ \sum_{j_1=1}^{t_i} f_{i,j_1,1}(x_1)\cdots f_{i,j_1,n}(x_n) \ \text{ over } R_i \tag{4}$$

With the aim of getting a dual form of the circuit C let us define a commutative algebra R that contains the algebras corresponding to each multiplication gate, i.e. $R_1,\ldots,R_k$, as "orthogonal" subalgebras and in which the following $(k-1)$ relations hold: $z_{1,1}^{e_{1,1}}\cdots z_{1,s}^{e_{1,s}} = \cdots = z_{k,1}^{e_{k,1}}\cdots z_{k,s}^{e_{k,s}}$. Explicitly, the algebra R is: $\mathbb{F}[z_{i,j} \mid \forall i \in [k], \forall j \in [s]]/\mathcal{I}$, where the ideal $\mathcal{I}$ is generated by the following three sets of relations:

- $z_{i,j}^{e_{i,j}+1} = 0$, for all $i \in [k], j \in [s]$.
- $z_{i,j} \cdot z_{i',j'} = 0$, whenever $i \neq i'$.
- $z_{i,1}^{e_{i,1}}\cdots z_{i,s}^{e_{i,s}} = z_{i',1}^{e_{i',1}}\cdots z_{i',s}^{e_{i',s}}$, for all $i, i' \in [k]$.

Note that the first set of relations just make $R_1,\ldots,R_k$ as subalgebras of R while the other two sets impose relations on certain zero-divisors in R ($e_{i,1} \neq 0$ implies that $z_{i,1}^{e_{i,1}}\cdots z_{i,s}^{e_{i,s}}$ is a zero-divisor of R). The second set of relations are put in so that the dimension of R gets down to roughly sum of the dimensions of $R_1,\ldots,R_k$. Note that the dimension of R over the base field $\mathbb{F}$ is exactly $\sum_{i=1}^{k}(1+e_{i,1})\cdots(1+e_{i,s}) - 2(k-1)$ which is nonzero. Clearly basic computations over R can be done in *poly* $(k, max\{(1+e_{i,1})\cdots(1+e_{i,s}) \mid 1 \leqslant i \leqslant k\})$ field operations.

Now by using the third set of relations in R and summing up Equation (4) for all the k multiplication gates, we get over the algebra R:

$$\begin{aligned} & C(x_1,\ldots,x_n)\cdot z_{1,1}^{e_{1,1}}\cdots z_{1,s}^{e_{1,s}} \\ = & \sum_{i=1}^{k} \ell_{i,1}^{e_{i,1}}\cdots\ell_{i,s}^{e_{i,s}} \cdot z_{i,1}^{e_{i,1}}\cdots z_{i,s}^{e_{i,s}} \\ = & \sum_{i=1}^{k}\sum_{j_1=1}^{t_i} f_{i,j_1,1}(x_1)\cdots f_{i,j_1,n}(x_n) \end{aligned} \tag{5}$$

This last expression can be viewed as a noncommutative formula in variables $x_1, \ldots, x_n$ over the algebra R. Clearly, it is zero *iff* $C(x_1, \ldots, x_n) \cdot z_{1,1}^{e_{1,1}} \cdots z_{1,s}^{e_{1,s}}$ is zero over R *iff* C is zero over $\mathbb{F}$. Thus, it is sufficient to test the circuit on the RHS of Equation (5) for zeroness. This can be done by applying the identity testing algorithm of Theorem 7, now working over the algebra R. Hence, we can deterministically verify whether C is zero in $poly(nk, dim(R))$ field operations as required. □

As happened in the case of diagonal circuits, the noncommutative form of the circuit in Equation (5) leads to a lower bound for determinant (and permanent) over depth-3 circuits that have a "small" s.

Theorem 15. *Over a field $\mathbb{F}$ of zero characteristic, if a depth-3 circuit C:*

$$C(x_1, \ldots, x_n) = \sum_{i=1}^{k} \ell_{i,1}^{e_{i,1}} \cdots \ell_{i,s}^{e_{i,s}}$$

expresses the determinant (or permanent) of a formal $m \times m$ matrix with parameters $s = o\left(\frac{m}{\log m}\right)$, $n = m^2$ and $d = poly(m)$ then $k = 2^{\Omega(m)}$.

Proof. Suppose the circuit C computes the determinant of a general $m \times m$ matrix. Recall that C has a dual form as given in Equation (5). Thus, we can apply Theorem 8 to deduce that $poly(ndk, dim(R)) = 2^{\Omega(m)}$ implying:

$$poly\left(ndk, max\{(1 + e_{i,1}) \cdots (1 + e_{i,s}) \mid 1 \leqslant i \leqslant k\}\right) = 2^{\Omega(m)}$$

As the $e_{i,j}$'s are at most $poly(m)$ the above implies $poly(ndk, m^s) = 2^{\Omega(m)}$ which using the hypothesis further implies $k = 2^{\Omega(m)}$. □

4 Extension to the Nonzero Characteristic Case

In the last section we defined the dual form of a multiplication gate $\ell_1^{e_1} \cdots \ell_s^{e_s}$, where the ℓ_i's are linear functions in $x_1, \ldots, x_n$ over a field $\mathbb{F}$ of zero characteristic. In this section we will show how to obtain the dual form when the characteristic of $\mathbb{F}$ is a prime $p > 1$. Note that over such a field the expressions used in the proof of Lemma 13 may not be defined, because for example if $p|d!$ then $\frac{1}{d!}$ is undefined in $\mathbb{F}$. We will show that such issues can be taken care of by a simple trick, thus finishing the proofs of our main Theorems 2 and 5.

For an $m \in \mathbb{Z}$, let us define a function $\iota_p(m)$ to be the largest integer $t \geqslant 0$ such that $p^t|m$. In general the base field $\mathbb{F}$ of characteristic $p > 1$, over which the input circuit does computation, will look like:

$$\mathbb{F} \cong \mathbb{F}_p(t_1, \ldots, t_c)[u_1, \ldots, u_{c'}]/(h_1(u_1, \ldots, u_{c'}), \ldots, h_{c''}(u_1, \ldots, u_{c'})) \tag{6}$$

where the h_i's are multivariate polynomials over $\mathbb{F}_p(t_1, \ldots, t_c)$. But in this section we will only describe a dual form working over $\mathbb{F} = \mathbb{F}_p$, as the techniques directly generalize to fields of Equation (6).

Lemma 16. *Let $\ell_i = (a_{i,0} + a_{i,1}x_1 + \cdots + a_{i,n}x_n)$, for all $i \in [s]$, be linear functions in the field $\mathbb{F}_p$ and $d = (e_1 + \cdots + e_s)$. Then we can compute univariate polynomials $f_{i,j}$'s over an algebra $R := R_0[z_1, \ldots, z_s]/(z_1^{e_1+1}, \ldots, z_s^{e_s+1})$ in $poly(n(1+e_1)\cdots(1+e_s))$ field operations such that:*

$$\ell_1^{e_1} \cdots \ell_s^{e_s} \cdot z_1^{e_1} \cdots z_s^{e_s} \cdot p^b \;=\; \sum_{i=1}^{t} f_{i,1}(x_1) \cdots f_{i,n}(x_n) \quad \textit{over } R$$

where R_0 is the Galois ring $\mathbb{Z}_{p^{b+1}}[y]/(h(y))$ (i.e. polynomial $h(y)$ is irreducible modulo p) and t, b and $deg(h)$ are all at most $poly(n(1+e_1)\cdots(1+e_s))$.

Proof. We will imitate the proof of Lemma 13 and make changes to avoid dividing by p in the field $\mathbb{F}_p$. Note that the elements of $\mathbb{F}_p$ can be taken as $\{0, \ldots, (p-1)\}$ and so there is this natural embedding of $\mathbb{F}_p$ into $\mathbb{Q}$. We can work in this embedding over $\mathbb{Q}$ and again start from the formal power series: $\exp(x) = 1 + x + \frac{x^2}{2!} + \cdots$, where $\exp(x) = e^x$ and e is the base of natural logarithm. Recall that the degree d truncation of the series is $E_d(x) = 1 + x + \cdots + \frac{x^d}{d!}$. Observe that (over $\mathbb{Q}$):

$$\begin{aligned}
&(e_1! \cdots e_s!)^{-1} \cdot \ell_1^{e_1} \cdots \ell_s^{e_s} \\
&\quad = \text{coefficient of } z^d z_1^{e_1} \cdots z_s^{e_s} \text{ in } \exp(\ell_1 z_1 z) \cdots \exp(\ell_s z_s z) \\
&\quad = \text{coefficient of } z^d z_1^{e_1} \cdots z_s^{e_s} \text{ in } \exp(\ell_1 z_1 z + \cdots + \ell_s z_s z) \\
&\quad = \text{coefficient of } z^d z_1^{e_1} \cdots z_s^{e_s} \text{ in } \exp\left((a_{1,0}z_1 + \cdots + a_{s,0}z_s)z\right) \cdots \\
&\qquad\qquad \cdots \exp\left((a_{1,1}z_1 + \cdots + a_{s,1}z_s)x_1 z\right) \cdots \exp\left((a_{1,n}z_1 + \cdots + a_{s,n}z_s)x_n z\right) \\
&\quad = \text{coefficient of } z^d z_1^{e_1} \cdots z_s^{e_s} \text{ in } E_d\left((a_{1,0}z_1 + \cdots + a_{s,0}z_s)z\right) \cdots \\
&\qquad\qquad \cdots E_d\left((a_{1,1}z_1 + \cdots + a_{s,1}z_s)x_1 z\right) \cdots E_d\left((a_{1,n}z_1 + \cdots + a_{s,n}z_s)x_n z\right) \qquad (7)
\end{aligned}$$

Remember that in the above we are working over $\mathbb{Q}$ (treating all constants as living in $\mathbb{Q}$), now we want to return back to the field $\mathbb{F}_p$. The easiest way to almost achieve this is by clearing away factors of p in the denominators of Equation (7). To this effect, multiply both sides of Equation (7) by $p^{(n+1)v}$, where $v = max\{\iota_p(i!) \mid 1 \leqslant i \leqslant d\}$, and remove p from the denominator of the LHS and from the denominators of all the coefficients of $E_d(\cdot)$ in the RHS of Equation (7). Rewriting the new expression (over $\mathbb{Q}$) that is free of p in the denominators, we have that for some nonnegative b that is at most $poly(nd)$:

$$\begin{aligned}
&c \cdot \ell_1^{e_1} \cdots \ell_s^{e_s} \cdot p^b \\
&\quad = \text{coefficient of } z^d z_1^{e_1} \cdots z_s^{e_s} \text{ in } \tilde{E}_d\left((a_{1,0}z_1 + \cdots + a_{s,0}z_s)z\right) \cdots \\
&\qquad\qquad \cdots \tilde{E}_d\left((a_{1,1}z_1 + \cdots + a_{s,1}z_s)x_1 z\right) \cdots \tilde{E}_d\left((a_{1,n}z_1 + \cdots + a_{s,n}z_s)x_n z\right)
\end{aligned}$$

where $c \in \mathbb{Q}$ is free of p in the numerator and the denominator, and coefficients of $\tilde{E}_d(\cdot)$ are free of p in the denominators. Now we can reduce the above expression modulo p^{b+1} and still get a meaningful expression as all the denominators are p-free and LHS is nonzero (ofcourse if the input ℓ_i's were nonzero). Next we just rerun the proof of Lemma 13 following Equation (3), over $\mathbb{Z}_{p^{b+1}}$. We begin by extracting the coefficient of z^d in the above by interpolation. One issue that deserves mention here is that interpolation requires evaluating the above product at $(nd + d + 1)$ distinct points from the ring $\mathbb{Z}_{p^{b+1}}$.

If $\mathbb{Z}_p$ is large enough then interpolation will work by just evaluating at points from $\mathbb{Z}_p$ and working over $R_0 := \mathbb{Z}_{p^{b+1}}$. If $\mathbb{Z}_p$ is small then we need to go to a large enough field extension of $\mathbb{F}_p$, which can be done deterministically in *poly*$(\log(nd))$ time [AL86], and then our base ring is not $\mathbb{Z}_{p^{b+1}}$ but $R_0 := \mathbb{Z}_{p^{b+1}}[y]/(h(y))$, where the polynomial $h(y)$ is irreducible modulo p (this makes R_0 a *Galois ring*). Finally, by going over the algebra $R_0[z_1, \dots, z_s]/(z_1^{e_1+1}, \dots, z_s^{e_s+1})$ we get the expression for $\ell_1^{e_1} \cdots \ell_s^{e_s} \cdot z_1^{e_1} \cdots z_s^{e_s} \cdot p^b$ as promised. It is routine to verify that all this can be done in *poly*$(n(1+e_1)\cdots(1+e_s))$ field operations. □

The above proof together with the last section, essentially, give us a dual form for multiplication gates of depth-3 circuits over any field $\mathbb{F}$. This dual form, together with the versions of Theorems 7 and 8 over $\mathbb{Z}_{p^{b+1}}$, gives us our main Theorems 2 and 5.

5 Applications to Other Models

In this section we collect miscellaneous extensions of our identity test. The first extension is to restricted depth-4 circuits. The second extension is a faster identity test for diagonal circuits that runs in time *poly*$(nk\log(d))$, i.e. exponentially faster in terms of the degree of the circuit, over a finite field $\mathbb{F}$.

5.1 Restricted Depth-4 Circuits

Suppose we are given a depth-4 circuit of the form:

$$C(x_1, \dots, x_n) = \sum_{i=1}^{k} L_{i,1}^{e_{i,1}} \cdots L_{i,s}^{e_{i,s}} \tag{8}$$

where the $L_{i,j}$'s are not linear functions but sums of univariate polynomials, i.e. for all $i \in [k], j \in [s]$:

$$L_{i,j}(x_1, \dots, x_n) = g_{i,j,1}(x_1) + \cdots + g_{i,j,n}(x_n)$$

where the $g_{i,j,j'}$'s are in $\mathbb{F}[x_{j'}]$. We will show in this section that our results of identity testing and lower bounds hold for these circuits too. For these purposes it will be sufficient to define the dual form of a multiplication gate of the form:

$$(g_{1,1}(x_1) + \cdots + g_{1,n}(x_n))^{e_1} \cdots (g_{s,1}(x_1) + \cdots + g_{s,n}(x_n))^{e_s} \tag{9}$$

Lemma 17. *Let $M(x_1, \dots, x_n)$ be the multiplication gate of Equation (9) over a field $\mathbb{F}$ of zero characteristic and $e = (e_1 + \cdots + e_s)$. Then we can compute univariate polynomials $f_{i,j}$'s over an algebra $R := \mathbb{F}[z_1, \dots, z_s]/(z_1^{e_1+1}, \dots, z_s^{e_s+1})$ in poly$(size(M), dim(R))$ field operations such that for $t = (ne+1)$:*

$$M(x_1, \dots, x_n) \cdot z_1^{e_1} \cdots z_s^{e_s} \;=\; \sum_{i=1}^{t} f_{i,1}(x_1) \cdots f_{i,n}(x_n) \quad \textit{over } R$$

Remark 18. *Note that we can informally describe the above equation as: a product-of-sums-of-univariates can be written as a sum-of-products-of-univariates. This justifies our continued usage of the phrase "dual form".*

Proof. We will run through a part of the proof of Lemma 13 to demonstrate that it works for the gate M too. Let $L_1, \ldots, L_s$ be the factors of M (that are now not linear functions but sums of univariate polynomials).

$$\begin{aligned}
&(e_1! \cdots e_s!)^{-1} \cdot M(x_1, \ldots, x_n) \\
&\;= \text{ coefficient of } z^e z_1^{e_1} \cdots z_s^{e_s} \text{ in } \exp(L_1 z_1 z) \cdots \exp(L_s z_s z) \\
&\;= \text{ coefficient of } z^e z_1^{e_1} \cdots z_s^{e_s} \text{ in } \exp(L_1 z_1 z + \cdots + L_s z_s z) \\
&\;= \text{ coefficient of } z^e z_1^{e_1} \cdots z_s^{e_s} \text{ in } \exp\left((g_{1,1} z_1 + \cdots + g_{s,1} z_s) z\right) \cdots \exp\left((g_{1,n} z_1 + \cdots + g_{s,n} z_s) z\right) \\
&\;= \text{ coefficient of } z^e z_1^{e_1} \cdots z_s^{e_s} \text{ in } E_e\left((g_{1,1} z_1 + \cdots + g_{s,1} z_s) z\right) \cdots E_e\left((g_{1,n} z_1 + \cdots + g_{s,n} z_s) z\right)
\end{aligned}$$

Eventually, just like in Lemma 13 we get (putting e instead of d):

$$\begin{aligned}
&(e_1! \cdots e_s!)^{-1} \cdot L_1^{e_1} \cdots L_s^{e_s} \cdot z_1^{e_1} \cdots z_s^{e_s} \\
&\quad = \sum_{i=1}^{ne+1} \beta_i \cdot E_e\left((g_{1,1} z_1 + \cdots + g_{s,1} z_s)\alpha_i\right) \cdots E_e\left((g_{1,n} z_1 + \cdots + g_{s,n} z_s)\alpha_i\right) \text{ over } R
\end{aligned}$$

Remember that $E_e\left((g_{1,1} z_1 + \cdots + g_{s,1} z_s)\alpha_i\right)$ is a univariate polynomial in $R[x_1]$ and so on. Thus, this is a dual form of the multiplication gate M as the variables $x_1, \ldots, x_n$ are "separated" in each summand of the above sum. It is routine to check that the univariate polynomials $E_e(\cdot)$ over R in the above sum can be obtained deterministically in $poly(size(M), dim(R))$ field operations. □

Lemma 17 sets the stage for identity testing and proving lower bounds for the depth-4 circuits of Equation (8). We can use the dual form in a way analogous to previous sections to get the following results:

Theorem 19. *Over any field $\mathbb{F}$, let C be a circuit given as in Equation (8). Then we can deterministically check whether C is a zero circuit in $poly(size(C), max\{(1+e_{i,1}) \cdots (1+e_{i,s}) \mid 1 \leqslant i \leqslant k\})$ field operations.*

Theorem 20. *Over any field $\mathbb{F}$, if the circuit in Equation (8) expresses the determinant (or permanent) of a formal $m \times m$ matrix with parameters $s = o\left(\frac{m}{\log m}\right)$, $n = m^2$ and $d = poly(m)$ then $k = 2^{\Omega(m)}$.*

Remark 21. *Theorem 20 is not really new because if determinant can be expressed as:*

$$C(x_1, \ldots, x_n) = \sum_{i=1}^{k} L_{i,1}^{e_{i,1}} \cdots L_{i,s}^{e_{i,s}}$$

where the $L_{i,j}$'s are a sum of univariate polynomials: $g_{i,j,1}(x_1) + \cdots + g_{i,j,n}(x_n)$. Then we can drop the degree two and higher terms in the univariate polynomials g_{i,j_1,j_2}'s, as determinant is a multilinear polynomial, and then apply the lower bound of Theorem 5.

5.2 A Faster Identity Test for Diagonal Circuits

In this subsection we will show how we can make the identity test for homogeneous diagonal circuits exponentially faster in the degree of the circuit. Unfortunately, we only know how to do this over a finite field $\mathbb{F}$ with an extra assumption that $d < char(\mathbb{F})$ (we do believe it should be possible to do this in general). The main idea to speed up the identity test is that if the degree d of a diagonal circuit C is large compared to fanin k then $C = 0$ only in "trivial" ways. This is formalized by the following result (also see Theorem 2 of [CSWM01]):

Theorem 22. *Let $\mathbb{F}$ be a finite field with $d < char(\mathbb{F})$. Suppose $d \geqslant (k-1)$ and $\sum_{i=1}^{k} b_i \cdot \ell_i^d = 0$ where ℓ_i are linear forms over $\mathbb{F}$ and b_i's are not all zero elements of $\mathbb{F}$. Then there exist distinct $i, j \in [k]$ and a $c \in \mathbb{F}$ such that $\ell_j = c \cdot \ell_i$.*

Proof. We sketch the proof of the contrapositive statement in brief.

Write ℓ_i as $(a_i x_1 + f_i)$ where we assume wlog that $a_i \neq 0$ and f_i is a nonzero linear form in $\mathbb{F}[x_2, \ldots, x_n]$, for all $i \in [k]$. Then by the hypothesis:

$$\sum_{i=1}^{k} b_i \cdot (a_i x_1 + f_i)^d = 0$$

Define a $k \times (d+1)$ matrix V having $a_i^{d-j+1} f_i^{j-1}$ in the (i,j)-th position. Now observe that the above equation implies the following matrix equation:

$$[b_1 \cdots b_k] \cdot V = 0$$

Since V is a Vandermonde matrix we deduce by our assumptions that its rows are linearly independent over $\mathbb{F}$. Hence, the above matrix equation implies that $[b_1 \cdots b_k] = 0$ which yields a contradiction. □

The above classification easily gives us an exponential speed-up.

Theorem 23. *Let $\mathbb{F}$ be a finite field with $d < char(\mathbb{F})$. Given a diagonal circuit $C(x_1, \ldots, x_n) = \sum_{i=1}^{k} b_i \cdot \ell_i^d$, we can deterministically test it for zeroness in $poly(nk \log(d))$ field operations.*

Proof. We can assume wlog that the ℓ_i's are nonzero and not multiples of each other (otherwise we can simplify C and get a diagonal circuit with a smaller k). Now if $d \geqslant (k-1)$ then by Theorem 22: $C = 0$ iff $b_i = 0$ for all $i \in [k]$. Thus, when $d \geqslant (k-1)$ we can check C for zeroness in $poly(nk \log(d))$ field operations.

So the nontrivial case is when $d < (k-1)$. In this case we can do identity testing (by Theorem 2) in $poly(nk)$ field operations.

Thus, in both the cases we can do identity testing in $poly(nk \log(d))$ field operations. □

Remark 24. *The classification Theorem 22 is also true when $char(\mathbb{F}) = 0$ and $d > 0$. But the identity test in the proof of Theorem 23 needs to check whether an expression like $\sum_{i=1}^{k} \alpha_i^d$ is zero (where the α_i's are in $\mathbb{F}$). We do not know how to do this deterministically in $poly(k \log(d))$ field operations even for $\mathbb{F} = \mathbb{Q}$.*

6 Conclusion

In this work we gave a deterministic polynomial time identity test for depth-3 circuits that are sums of powers of linear functions. Our basic idea was to define a dual operation on the multiplication gates in a depth-3 circuit that converts a product gate into a sum of product of univariate polynomials. This dual is efficiently computable when the multiplication gate has "few" distinct linear functions as input. In the case of a general multiplication gate of a depth-3 circuit of degree d the dual computation takes exponential time: $poly(n2^d)$. This dual computation can be viewed as a new way to unfold a given depth-3 circuit better than the direct brute-force expansion. We leave it as an open question to improve this duality to solve the identity testing problem for general depth-3 circuits.

Kayal [Kay07] has observed that Theorems 2 and 5 can be obtained in an alternative way using the space of partial derivatives first defined by Nisan and Wigderson [NW97]. The basic reason is that the space of partial derivatives of a diagonal circuit has "low" rank and this can be exploited for doing identity testing and proving lower bounds. It is not clear however, how to use this space of partial derivatives in the case of depth-4 circuits (to prove Theorem 19) that in general has "high" rank.

Acknowledgements

I would like to thank Harry Buhrman and Ronald de Wolf for various useful discussions during the course of this work. I also want to thank Neeraj Kayal and Avi Wigderson for providing insightful observations on a preliminary version of this paper.

References

[AB03] M. Agrawal and S. Biswas, *Primality and identity testing via Chinese remaindering*, Journal of the ACM **50** (2003), no. 4, 429–443.

[AKS04] M. Agrawal, N. Kayal, and N. Saxena, *Primes is in P*, Annals of Mathematics **160** (2004), no. 2, 781–793.

[AL86] L. M. Adleman and H. W. Lenstra, *Finding irreducible polynomials over finite fields*, Proceedings of the eighteenth annual ACM Symposium on Theory of Computing, ACM Press, 1986, pp. 350–355.

[ALM$^+$98] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, *Proof verification and the hardness of approximation problems*, Journal of the ACM **45** (1998), no. 3, 501–555.

[AS98] S. Arora and S. Safra, *Probabilistic Checking of Proofs: A New Characterization of NP*, Journal of the ACM **45** (1998), no. 1, 70–122.

[BCW80] M. Blum, A.K. Chandra, and M.N. Wegman, *Equivalence of free Boolean graphs can be tested in polynomial time*, Information Processing Letters **10** (1980), 80–82.

[CDGK91] M. Clausen, A. Dress, J. Grabmeier, and M. Karpinski, *On zero-testing and interpolation of k-sparse multivariate polynomials over finite fields*, Theoretical Computer Science **84** (1991), no. 2, 151–164.

[CK00] Z. Chen and M. Kao, *Reducing randomness via irrational numbers*, SIAM Journal of Computing **29** (2000), no. 4, 1247–1256.

[CSWM01] A. Chlebowicz, A. Sladek, and M. Wolowiec-Musial, *Automorphisms of certain forms of higher degree over ordered fields*, Linear algebra appl. **331** (2001), 145–153.

[DS05] Z. Dvir and A. Shpilka, *Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits.*, Proceedings of the 37th Annual ACM Symposium on Theory of Computing, 2005, pp. 592–601.

[GK98] D. Grigoriev and M. Karpinski, *An exponential lower bound for depth 3 arithmetic circuits*, Proceedings of the 30th Annual ACM Symposium on Theory of Computing, 1998, pp. 577–582.

[GKS90] D. Y. Grigoriev, M. Karpinski, and M. F. Singer, *Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields*, SIAM Journal on Computing **19** (1990), no. 6, 1059–1063.

[GR00] D. Grigoriev and A. A. Razborov, *Exponential lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields*, Appl. Algebra Eng. Commun. Comput. **10** (2000), no. 6, 465–487.

[IK04] R. Impagliazzo and V. Kabanets, *Derandomizing polynomial identity tests means proving circuit lower bounds*, Computational Complexity **13** (2004), no. 1/2, 1–46.

[Kay07] N. Kayal, 2007, Private Communication, Summer 2007.

[KS07] N. Kayal and N. Saxena, *Polynomial identity testing for depth 3 circuits*, Computational Complexity **16** (2007), no. 2, 115–138.

[LFK92] C. Lund, L. Fortnow, and H. Karloff, *Algebraic methods for interactive proof systems*, Journal of the ACM **39** (1992), no. 4, 859–868.

[Lov79] L. Lovasz, *On determinants, matchings, and random algorithms*, Akademia-Verlag, 1979.

[LV98] D. Lewin and S. Vadhan, *Checking polynomial identities over any field: towards a derandomization?*, Proceedings of the 30th annual ACM Symposium on Theory of Computing, ACM Press, 1998, pp. 438–447.

[Nis91] N. Nisan, *Lower bounds for non-commutative computation*, Proceedings of the twenty-third annual ACM Symposium on Theory of Computing, ACM Press, 1991, pp. 410–418.

[NW97] N. Nisan and A. Wigderson, *Lower bounds on arithmetic circuits via partial derivatives*, Computational Complexity **6** (1997), no. 3, 217–234.

[Raz04] R. Raz, *Multi-linear formulas for permanent and determinant are of super-polynomial size*, Proceedings of the thirty-sixth annual ACM Symposium on Theory of Computing, ACM Press, 2004, pp. 633–641.

[RS05] R. Raz and A. Shpilka, *Deterministic polynomial identity testing in non-commutative models*, Computational Complexity **14** (2005), no. 1, 1–19.

[Sch80] J. T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, Journal of the ACM **27** (1980), no. 4, 701–717.

[Sha92] A. Shamir, *IP=PSPACE*, Journal of the ACM **39** (1992), no. 4, 869–877.

[SW01] A. Shpilka and A. Wigderson, *Depth-3 arithmetic circuits over fields of characteristic zero*, Computational Complexity **10** (2001), no. 1, 1–27.

[Zip79] R. Zippel, *Probabilistic algorithms for sparse polynomials*, International Symposium on Symbolic and Algebraic Computation, Lecture Notes in Computer Science, vol. 72, Springer-Verlag, 1979, pp. 216–226.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/