Equivalence test Of Design polynomials

Omkar Bhalchandra Baraskar *

Abstract

Given n-variate degree d homogenous polynomial f we want to decide whether there exists a invertible transform $A \in \mathbb{F}^{n \times n}$ such that there exists a (n, t, s, d)-design polynomial g such that $f(x) = g(Ax)$. This problem is commonly referred to as *Equivalence testing of Design Polynomials*. In this report we give an equivalence test for design polynomials which runs in time $\mathcal{O}(n^t)$ if $d > 3t$ and some technical assumptions on the size and characteristic of the field $\mathbb{F}$.

*Joint work with Agrim Dewan and Prof Chandan Saha

Contents

1 Introduction

1.1 Problem Statement and Results

Definition 1. *(Design Polynomials) A polynomial g is (n, t, s, d)-design polynomial is a degree d homogeneous polynomial with sparsity s, and additionally for every monomial m, n in g we have* ***deg*** $gcd(m, n) < t$.

Definition 2. *(Equivalence testing of Design Polynomials) Given black box access to a n-variate degree d homogenous polynomial f, decide whether there exists a invertible linear transform $A \in \mathbb{F}^{n \times n}$ such that $f = g(Ax)$ and g is (n, t, s, d)-design polynomial*

Our main result gives an equivalence testing algorithm for design polynomials satisfying some technical assumptions.

Theorem 1. *(Equivalence testing of design polynomials) There is a randomised algorithm given black box access to n-variate degree d polynomial f outputs n linear independent linear forms $L_1, \ldots, L_n$ and (n, t, s, d) design polynomial g s.t $f = g(L_1, \ldots, L_n)$ if f is in the orbit of a (n, t, s, d) design polynomial else it output "No". The running time of the algorithm is poly(n^t). The algorithm runs under the following technical assumptions, $d > 3t$, $|\mathbb{F}| > max(s^3, d^7)$ and* ***char***$(\mathbb{F}) = 0$ *or* $> d$

Our algorithm also works for "random" homogeneous degree d polynomials with some technical assumptions on the sparsity (Refer Section 6.2).

1.2 Previous Work

The previous work on equivalence tests used Hessian matrices and Lie Algebras, such as in [8]. Equivalence test algorithms for sum-product and power symmetric polynomial were given by using Hessian matrices which worked over $\mathbb{C}$, finite fields and $\mathbb{Q}$; Equivalence test for determinants and permanents over $\mathbb{C}$, finite fields and $\mathbb{Q}$ was given in [7] and [3] using Lie algebras. For design polynomials no equivalence test is known; In [5] equivalence test for the Nisan Wigderson design polynomial is given for block diagonal permutation scaling transformation over finite fields by analysing the lie algebra of NW polynomial. A better result is unlikely to be expected by this technique as the lie algebra of NW polynomial is "very weak". It seems unlikely that Hessian matrices and Lie algebra would help in designing an equivalence test. Hence we use the meta-framework mentioned in [4] to get an equivalence test for design polynomials.

1.3 Proof Techniques

The basis of the equivalence test is the vector space decomposition framework (particularly the meta-algorithm) developed in [4]. Briefly, the vector space decomposition framework itself is based on lower bound techniques used to learn circuits from black box access to a polynomial f. If f is of the form:

$$f = T_1 + T_2 + ... + T_s \tag{1}$$

Then learning circuits for the T_i's suffices for learning f. The authors in [4] reduce the problem of learning the T_i's to the vector space decomposition problem which, as stated in [4], is as follows :

Given the tuple $(\mathcal{L}, U, V)$ consisting of vector spaces U and V and a set of linear maps $\mathcal{L}$ from U to V , decompose U and V as:

$$U = U_1 \oplus \cdots \oplus U_s$$
$$V = V_1 \oplus \cdots \oplus V_s$$

such that $\langle \mathcal{L}(U_i) \rangle \subset V_i$ for $1 \leq i \leq s$.

By choosing an appropriate set of linear maps $\mathcal{L}_1$ and $\mathcal{L}_2$, one can define the spaces U and V for a polynomial f, where $V = \mathcal{L}_2(U)$, and then compute the vector space decomposition of U and V which can then be used to recover the monomials in f. However, this decomposition may not necessarily be unique. The criteria for the uniqueness of the decomposition has been laid down in [4] and are based on the Krull- Schimdt theorem.

Briefly, the uniqueness of decomposition can be established using the notion of adjoint algebra which is defined, for the tuple $(\mathcal{L}, U, V)$, as the set of pairs of linear operators (D, E) where $D : U \to U$, $E : V \to V$ and $\forall L \in \mathcal{L}$, $LD = EL$ and is denoted as $Adj(\mathcal{L}, U, V)$. If $(D, E) \in (\mathcal{L}, U, V)$ and are invertible operators, then $U = D(U_1) \oplus \cdots \oplus D(U_s)$ and $V = E(V_1) \oplus \cdots \oplus E(V_s)$ and it follows from the Krull Schimdt Theorem that the decomposition of U, V as mentioned is unique (upto permutations) under the action of the maps $\mathcal{L}$.

For our case, we can view the problem as trying to learn the linearly independent linear forms under which the polynomial, provided as a black box, is equal to some design polynomial. For any (n, t, s, d) design polynomial with $d > 3t$, it turns out that the direct sum structure and uniqueness of decomposition are satisfied, and this holds true for any polynomial in the orbit of such a design polynomial as well. This implies that the vector space decomposition framework can be used to recover the linear forms. The meta-algorithm for vector space decomposition is, as stated in [4]:

Algorithm 1 Meta algorithm

- **Input** - $g = T_1 + T_2 + ... + T_s$
- **Output** - $T'_1, T'_2 \ldots T'_s$ s.t. $T'_i = T_j$ where $j = \pi(i)$ π is a permutation on $[s]$.

1. Compute $U = \langle \mathcal{L}_1(f) \rangle$,$V = \langle \mathcal{L}_2(\mathcal{L}_1(f)) \rangle$
2. Obtain a vector space decomposition of U, V as $U = U_1 \oplus \cdots \oplus U_s$,$V = V_1 \oplus \cdots \oplus V_s$.
3. Recover T'_i from U_i.

The algorithm works under the following assumptions:

1. $\exists\, \mathcal{L}_1, \mathcal{L}_2$ s.t. $\forall L_1 \in \mathcal{L}_1,\ L_2 \in \mathcal{L}_2$, it holds that $U = \langle L_1(f) \rangle$, $V = \langle L_2(L_1(f)) \rangle$, $U_i = \langle L_1(T_i) \rangle$, $V_i = \langle L_2(L_1(T_i)) \rangle$

$$U = U_1 \oplus \cdots \oplus U_s$$
$$V = V_1 \oplus \cdots \oplus V_s$$

2. The aforementioned decomposition is unique up to permutation of the U_i's and V_i's.

3. There is an efficient algorithm to recover T_i from U_i.

The vector space decomposition algorithm of [2] can be used in step 2 and it works over $\mathbb{R}, \mathbb{C}$ and finite fields, although over $\mathbb{Q}$ it outputs a polynomial in an extension field. Section 4 gives a vector space decomposition algorithm based on the algorithm developed in [1] which works over $\mathbb{Q}$ as well.

1.4 Roadmap of the report

Section 2 establishes some required preliminaries and the notations used.

In Section 3, we state the algorithm. We first prove it's correctness by proving that the direct sum condition and uniqueness of decomposition hold.

Section 4 describes the adjoint algebra in our case. We then show that the operators in the adjoint are simultaneously triangulable by exhibiting a basis. Using this an algorithm for vector space decomposition is given.

2 Preliminaries and Notations

A (n, t, s, d)-design polynomial is a degree d homogeneous polynomial with sparsity s and for every monomial m, n in the polynomial $\mathbf{deg\ gcd}(m, n) < t$.
The polynomial $g(x_1, \ldots, x_n)$ denotes a (n, t, s, d)-design polynomial design polynomial with $d > 3t$ i.e

$$g = g_1 + \cdots + g_s$$

where g_i's are monomials satisfying the design condition.
Let $f(x_1, \ldots, x_n)$ denotes a polynomial in the orbit of g i.e

$$f = T_1 + T_2 + \cdots + T_s$$

where $T_i = g_i(l_1, \ldots, l_s)$ (l_i's are linearly independent linear forms). Define

$$U := \langle \partial^t f \rangle \quad U' := \langle \partial^t g \rangle$$

$$U_i := \langle \partial^t g_i \rangle \quad U_i' := \langle \partial^t T_i \rangle$$

$$V := \langle \partial^{2t} f \rangle \quad V' := \langle \partial^{2t} g \rangle$$

$$V_i := \langle \partial^{2t} g_i \rangle \quad V_i' := \langle \partial^{2t} T_i \rangle$$

We will denote all the order k differential operators in $\mathbf{x}$ variables by ∂^k, and x^α denotes a degree k monomial where α is an $n-$tuple $\in \mathbb{Z}^n_{\geq 0}$ whose elements sum to k.

The following are some preliminary facts that we need in our algorithm:

1. **Black box access to Partial Derivative Space:** Given black box access to n-variate degree d polynomial $f(x_1, \ldots, x_n)$, we get black box to $\frac{\partial^k f}{\partial x^\alpha}$ in poly(n, d^k) time where $\mathbf{deg}\ \alpha = k$ (for more details check section 2.2 [9]).
2. **Finding coefficients w.r.t to a basis** Given a linearly independent set $f_1, \ldots, f_l \in \mathbb{F}[x]_d$, say that f lies in the span of the set then in randomised poly(n, l, d) we can compute β_i's s.t $f = \sum_{i=1}^{l} \beta_i f_i$(for more details check corollary 29 of [1]).

3 The algorithm

In this section, we give an algorithm for equivalence testing of design polynomials, we assume that we know the value of s, t, n.

Algorithm 2 Equivalence testing of design polynomials

Input: Black box access to $f = T_1 + \cdots + T_s$ which is in the orbit of an (n, t, s, d)-design polynomial.

Output: Circuits of $n+1$ independent linear form $L_1, \ldots, L_n$ and (n, t, s, d) design polynomial g of degree d s.t $f = g(L_1, \ldots, L_n)$.

Sub-routines:

1. Returns black boxes to all the t-order partial derivatives of a polynomial given the black box access to the polynomial (see preliminary 1)
2. Vector space decomposition algorithm (See Algorithm 3 in 4.3)
3. Say $U = U_1 \oplus \cdots \oplus U_s$ and we have a black box access to basis $\mathcal{B}_i$ of U_i for all $i \in [s]$. Then given black box access to $u = u_1 + \cdots + u_s$ s.t $u_i \in U_i$ it returns the black box of u_i's. (see preliminary 2)
4. Black box factorisation algorithm ([6])
5. Given black box access to polynomials $p_1, \ldots, p_n$ returns basis to $(p_1, \ldots, p_n)^{\perp}$. (section A.1 of [8])

1: Compute the black boxes to $U = \langle \partial^t f \rangle$ and $V = \langle \partial^t U \rangle$ using sub-routine 1.
2: Use the sub-routine 2 on (∂^t, U, V) to get a decomposition of $U = U'_1 \oplus \cdots \oplus U'_{s'}$ if $s \neq s'$ then output "No", else continue.
3: For each $\mathbf{x}^\alpha$ of degree t express $\frac{\partial^t f}{\partial \mathbf{x}^\alpha} = u'_{1\alpha} + \cdots + u'_{s\alpha}$ s.t $u'_{i\alpha} \in U'_i$ then use sub-routine 3 on $\frac{\partial^t f}{\partial \mathbf{x}^\alpha}$ and $\mathcal{B}'_i$'s (basis of U'_i) obtained from step 2 to get black boxes to $u'_{i\alpha}$.
4: For each $\mathbf{x}$ the black box P_i returns $\frac{(d-t)!}{d!} \sum_\alpha \binom{t}{\alpha_1 \ldots \alpha_n} \mathbf{x}^\alpha u'_{i\alpha}(\mathbf{x})$ ▷ Refer section 4.3 of [10]
5: For every $i \in [s]$ use sub-routine 4 to get irreducible factorisation of P_i, if the degree of any irreducible element is > 1 output "No", else evaluate the irreducible elements to get circuits of the linear forms $L_1, \ldots, L_n$ and the circuits for the g_i s.t $P_i = g_i(L_1, \ldots, L_n)$ can be obtained from the factorisation.
6: For $i \neq j$ compute $\mathbf{gcd}(g_i, g_j)$ using subroutine 4 if $\mathbf{deg\ gcd}(g_i, g_j) \geq t$ for any $i \neq j$ output "No". Use sub-routine 5 to check if $L_1, \ldots, L_n$ are linearly independent, if they are not output "No". Else return the circuits of $L_1, \ldots, L_n$ and $g = g_1 + \cdots + g_s$.

3.1 Correctness of the algorithm

Before we can prove the correctness of algorithm, we need the following lemma

Lemma 2. *If $l_1, \ldots, l_n$ are linearly independent then for any $t \leq k \leq d-t$ we have*

$$W = W_1 \oplus W_2 \oplus \cdots \oplus W_s$$

where $W = \langle \partial^k f \rangle$ and $W_i = \langle \partial^k T_i \rangle$ (similar to U and U_i as defined in section 2).

Proof. Since the linear forms are linearly independent thus from theorem 10 we have that $W \cong W' = \langle \partial^k g \rangle$ and for every $1 \leq i \leq s$ and $t \leq k \leq d-t$ we have $W_i \cong W_i' = \langle \partial^k g_i \rangle$. Hence we have $W = W_1 \oplus W_2 \oplus \cdots \oplus W_s$ iff $W' = W_1' \oplus W_2' \oplus \cdots \oplus W_s'$.

Now we will prove that $W' = W_1' \oplus \cdots \oplus W_s'$.Note that for any k we have $W' \subseteq W_1' + \cdots + W_s'$. For each i one can easily see that $\{\partial^k g_i\}$ is the spanning set of W_i'. Hence $\mathbf{dim}\ U_i \leq M_i = |\{\partial^k g_i\}|$ [1]. Now if $\mathbf{dim}\ W' = \sum_{i=1}^{s} M_i = M$ then it is clear that $W' = W_1' \oplus \cdots \oplus W_s'$.

Now what remains to show that $\mathbf{dim}\ \langle \partial^k g \rangle = M$. So, for some $i \in [s]$ let $u \in \{\partial^k g_i\}$, say $m = g_i/u$, since $\mathbf{deg}\ m \geq t$ thus $\frac{\partial g_j}{\partial m} = 0$ for $j \neq i$ by the design condition. Hence $\frac{\partial g}{\partial m} = u$. Thus we have $\{\partial^k g_i\} \subseteq \langle \partial^k g \rangle$. Let $\mathcal{B}_i = \{\partial^k g_i\}$, now if we show that $\mathcal{B}_i \cap \mathcal{B}_j = \phi$ then clearly $|\bigcup_{i=1}^{s} B_i| = M$ and also since B_i's is a set of monomials hence being disjoint is equivalent to saying that the union forms an independent set, now $\bigcup_{i=1}^{s} B_i \subseteq \langle \partial^k g \rangle$ hence the $\mathbf{dim}\ \langle \partial^k g \rangle = M$, and we will be done.
So, the only thing remaining to prove is that B_i's are pairwise disjoint. Say that for some $i \neq j$, $B_i \cap B_j \neq \phi$ then let b be in the intersection then $b|g_i$ and $b|g_j$, hence $\mathbf{deg}\ gcd(g_i, g_j) \geq \mathbf{deg}\ b$, now $\mathbf{deg}\ b = d - k \geq t$ which contradicts the design condition. Hence this completes the proof.

□

To prove the correctness we have to show :

1. $U = U_1 \oplus \cdots \oplus U_s$ and $V = V_1 \oplus \cdots \oplus V_s$
2. Uniqueness of vector space decomposition.

where U, U_i, V, and V_i are as defined earlier in Section 2.

3.1.1 Direct Sum Structure

Lemma 3. *$\langle \partial^t U \rangle = \langle \partial^{2t} p \rangle$ for any polynomial $p \in \mathbb{F}[\boldsymbol{x}]$ where $U = \langle \partial^t p \rangle$*

Proof. Let $v \in \langle \partial^t U \rangle$ now we have a monomial $\mathbf{x}^\alpha$ of degree t and $u \in U$ s.t $v = \frac{\partial^t u}{\partial \mathbf{x}^\alpha}$, now $u = \sum_{\mathbf{deg}\beta = t} c_\beta \frac{\partial^t p}{\partial \mathbf{x}^\beta}$, now $v = \sum_{\mathbf{deg}\beta = t} c_\beta \frac{\partial^{2t} p}{\partial \mathbf{x}^\beta \mathbf{x}^\alpha}$, hence $v \in \langle \partial^{2t} p \rangle$.

Now the spanning set for $\langle \partial^{2t} p \rangle$ is $\{\partial^{2t} p\}$, so if we show $\{\partial^{2t} p\} \subseteq \langle \partial^t U \rangle$ then $\langle \partial^{2t} p \rangle \subseteq \langle \partial^t U \rangle$. So let $v \in \{\partial^{2t} p\}$ then there is a monomial x^α of degree $2t$ s.t $v = \frac{\partial^{2t} p}{\partial x^\alpha}$, now write $\alpha = \alpha_1 \alpha_2$ where $\mathbf{deg}\ \alpha_1 = t$ then $u = \frac{\partial^t p}{\partial \mathbf{x}^{\alpha_1}} \in U$ and $v = \frac{\partial^t u}{\partial \mathbf{x}^{\alpha_2}} \in \langle \partial^t U \rangle$. Hence we are done. □

As $d \geq 3t \geq 2t$ then by lemma 2 we have $U = U_1 \oplus \cdots \oplus U_s$ and $V = V_1 \oplus \cdots \oplus V_s$ where $V_i = \langle \partial^{2t} f \rangle$. Now applying lemma 3 to f we get $V = \langle \partial^t U \rangle$, similarly applying 3 to T_i we get $V_i = \langle \partial^t U_i \rangle$. Hence we have $U = U_1 \oplus \cdots \oplus U_s$ and $V = V_1 \oplus \cdots \oplus V_s$ where $V_i = \langle \partial^t U_i \rangle$ and $V = \langle \partial^t U \rangle$.

[1] One can prove that $\mathbf{dim}\ U_i$ is maximum when the monomial is multilinear i.e $M_i \leq \binom{d}{k}$

3.1.2 Uniqueness Of Vector Space Decomposition

Now we have to show the uniqueness of the vector space decomposition (for definition refer Appendix A of [1]). Now to show this we it is enough to show that for any invertible $(D, E) \in Adj(\partial^t, U, V)$ we have $D(U_i) \subseteq U_i$ for all $i \in [s]$.(This method of showing uniqueness of decomposition using adjoint algebra is discussed in appendix A of [4]).

Now we will prove a corollary of theorem 10 which will help us prove uniqueness.

Corollary 4. *If* $\forall\ (D', E') \in Adj(\partial^t, U', V')$ *and* $\forall\ i \in [s]$ *we have* $D'(U'_i) \subseteq U'_i$ *then* $\forall\ (D, E) \in Adj(\partial^t, U, V)$ *and* $\forall\ i \in [s]$ *we have* $D(U_i) \subseteq U_i$.

Proof. First note that by theorem 10 we have $T : U' \to U$ given by $T(p) = p(l_1, \ldots, l_n)$ is a isomorphism, also note that $T(U'_i) = U_i$ for all $i \in [s]$. Now let $(D, E) \in Adj(\partial^t, U, V)$, now by proposition 25 of [1] we have $(D', E') \in Adj(\partial^t, U', V')$ s.t $D = TD'T^{-1}$. We have

$$\begin{aligned} D(U_i) &= (TD'T^{-1})(U_i) \\ &= TD'(U'_i) \\ &\subseteq T(U'_i) \\ &\subseteq U_i \end{aligned}$$

for all $i \in [s]$ and $(D, E) \in Adj(\partial^t, U, V)$. □

Now we are ready to prove the uniqueness of the decomposition.

Lemma 5. *For* $\forall\ (D, E) \in Adj(\partial^t, U, V)$ *we have* $D(U_i) \subseteq U_i$ *for all* $i \in [s]$

Proof. Now by corollary 4 it is enough to prove that $D'(U'_i) \subseteq U'_i$ for all $(D', E') \in Adj(\partial^t, U', V')$ and $i \in [s]$.

For $u \in U'_i$ $D'(u) = u'_1 + \cdots + u'_s$ s.t $u'_j \in U'_j$. Take $m_j | u'_j$ and $\mathbf{deg}\ m_j = t$. By the design condition we have $\frac{\partial u}{\partial m_k} = 0$ for all $i \neq k$ and $\frac{\partial u_j}{\partial m_k} = 0$ for all $j \neq k$.

Now for $j \neq i$ we have,

$$\begin{aligned} &\frac{\partial D'(u)}{\partial m_j} = \frac{\partial u'_j}{\partial m_j} \\ \implies &E'(\frac{\partial u}{\partial m_j}) = \frac{\partial u'_j}{\partial m_j} \\ \implies &E'(0) = \frac{\partial u'_j}{\partial m_j} \\ \implies &0 = \frac{\partial u'_j}{\partial m_j} \\ \implies &u'_j = 0 \end{aligned}$$

Hence we have $D'(U'_i) \subseteq U'_i$. This completes our proof. □

3.2 Time Complexity

Steps 1 and 2 are the dominant steps in the time complexity of the algorithm. Step 1 requires $\text{poly}(n, d^t)$ time as noted in 1. Step 2 uses subroutine 2, the complexity of which is $\text{poly}(s, n^t, d^t)$ as shown in Section 4.3.

Step 3 uses subroutine 3 with $O(sd^t)$ many linearly independent polynomials (since $|\mathcal{B}| \leq s\binom{d}{t} = O(sd^t)$) of degree $d-t$, hence requires $\text{poly}(n, s, d^t)$ time.

The remaining steps use Kaltofen's black box factorisation algorithm s times to factor P_i, which is of degree d, compute the gcd of the g_i monomials (from the recovered circuits) which are of degree d and also use Sub-routine 5 on n linear forms. Hence, these steps require $\text{poly}(s, n, d))$ time (including recovering the circuits of the linear forms).

Thus, the overall complexity of the algorithm is $\text{poly}(s, n^t, d^t)$. Usually $n > d^2$ for a design polynomial and s can be at most n^t for a t-design polynomial,therefore the complexity is $\text{poly}(n^t)$.

4 Adjoint Algebra of design polynomials

The adjoint algebra for the polynomials considered in [4] and [1] was trivial, which means the operators in the adjoint were scalar multiples of the identity map. This was used to obtain a vector space decomposition algorithm which works over rationals as well by computing the eigenspaces of the operators. Note that if the adjoint is trivial in some basis of the spaces U and V, then it would be trivial in any basis of these spaces. Hence, if there is an operator which does not even have a diagonal representation in some basis, then the adjoint is non-trivial.

In the case of non-multilinear polynomials, the adjoint is not necessarily trivial, we will start by giving an example of a polynomial with non-trivial adjoint algebra, then we give a structural result and then using this result we give a vector space decomposition algorithm for design polynomials.

4.1 Characterisation of Adjoint algebra

By lemma 5 we know that elements of $Adj(\partial^t, U, V)$ are block diagonal matrices hence to understand their structure it is enough to understand individual blocks, i.e it is enough to understand $D|_{U_i}$'s. Hence in this section we will focus our attention on each individual block.

Note that by theorem 10 we know that $Adj(\partial^t, U_i, V_i) \cong Adj(\partial^t, U_i', V_i')$, so in this section we will be working with $Adj(\partial^t, U_i', V_i')$, so for the sake of simplicity we will denote U_i' by U, V_i' by V, g_i by g and $Adj(\partial^t, U_i', V_i')$ by $Adj(\partial^t, U, V)$.

4.1.1 Non-trivial Adjoint Algebra

So, given any matrix $D' : U' \to U'$ what conditions should we impose on D' to ensure that $\exists\ E' : V' \to V'$ s.t $(D', E') \in Adj(\partial^t, U', V')$? The following lemma answers the question.

Define $\mathcal{D}_k = \{m \mid m \in \mathbb{F}[\mathbf{x}],\ \textbf{deg}\ m = k \text{ and } m|g\}$

Lemma 6. *The following statements are equivalent:-*

(a) $(D', E') \in Adj(\partial^t, U', V')$

(b) For every $i \in [s]$, $m, n \in \mathcal{D}_t$ *we have*

$$\frac{\partial}{\partial m} D'(\frac{\partial g}{\partial m'}) = \frac{\partial}{\partial n} D'(\frac{\partial g}{\partial n'}) \tag{2}$$

$\forall m, m'$ *s.t* $mm' = nn'$ *and* $mm', nn' \in \mathcal{D}_{2t}$ *else*

$$\frac{\partial}{\partial m} D'(\frac{\partial g}{\partial m'}) = 0 \tag{3}$$

Proof. Say if $(D', E') \in Adj(\partial^t, U', V')$ then $\frac{\partial}{\partial m} D'(\frac{\partial g}{\partial m'}) = E'(\frac{\partial g}{\partial mm'}) = E'(\frac{\partial g}{\partial nn'}) = \frac{\partial}{\partial n} D'(\frac{\partial g}{\partial n'})$ so if $mm' \in \mathcal{D}_{2t}$ then $\frac{\partial}{\partial m} D'(\frac{\partial g}{\partial m'}) = \frac{\partial}{\partial n} D'(\frac{\partial g}{\partial n'})$ else $\frac{\partial}{\partial m} D'(\frac{\partial g}{\partial m'}) = \frac{\partial}{\partial n} D'(\frac{\partial g}{\partial n'}) = 0$.

Say $D' : U' \to U'$ satisfies the conditions mentioned in (b) then define $E' : V' \to V'$ as

$$E'(\frac{\partial g}{\partial m}) = \begin{cases} \frac{\partial}{\partial m_1} D'(\frac{\partial g}{\partial m_2}) & m \in \mathcal{D}_{2t} \text{ and } m_1, m_2 \in \mathcal{D}_t \\ 0 & \text{otherwise} \end{cases}$$

where $m_1 m_2 = m$, this is well-defined because of condition (b).
Now we will prove that $(D', E') \in Adj(\partial^t, U', V')$. Let $L = \frac{\partial}{\partial m}$, now we wish to show that $LD'(\frac{\partial g}{\partial m'}) = E'(L(\frac{\partial g}{\partial m'}))$, now there are two cases here,

- Say $mm' \in \mathcal{D}_{2t}$ now $LD'(\frac{\partial g}{\partial m'}) = \frac{\partial}{\partial m} D'(\frac{\partial g}{\partial m'}) = E'(\frac{\partial g}{\partial mm'}) = E'(L(\frac{\partial g}{\partial m'}))$
- Say $mm' \notin \mathcal{D}_{2t}$ now $E'(L(\frac{\partial g}{\partial m'})) = E'(\frac{\partial g}{\partial mm'}) = 0$ and $LD'(\frac{\partial g}{\partial m'}) = \frac{\partial}{\partial m} D'(\frac{\partial g}{\partial m'}) = 0$.

Since m, m' are arbitrary, this completes the proof.

□

Now, we will use the above lemma to show that $g = x_1^6 x_2^2$ has a non-trivial adjoint algebra. Say $(D', E') \in Adj(\partial^{=2}, U', V')$, now by lemma 6 it is equivalent to saying D' satisfies 2,3; these gives us a system of linear equations whose solutions are as follows

$$Adj(\partial^{=2}, U', V') = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & \frac{12}{5}b \\ 0 & 0 & a \end{pmatrix}, \begin{pmatrix} a & \frac{3}{2}b & \frac{5}{2}c \\ 0 & a & 4b \\ 0 & 0 & a \end{pmatrix} \ : \ a, b, c \in \mathbb{F} \right\}$$

4.1.2 Structural Result

In this section we show that diagonal entries of an element in the adjoint algebra are the same and look at a sufficient condition which tells us when the off-diagonal entries of an element in adjoint algebra is 0.

For the sake of simplicity $D(m_i)[m_j]$ denotes the coefficient of $\frac{\partial g}{\partial m_j}$ in $D(\frac{\partial g}{\partial m_i})$ for the rest of the section.

Lemma 7. *For $m_i, m_j \in \mathcal{D}_t$ we have*

(a) $D(m_i)[m_j] = 0$ *if* $\{\partial^t(\frac{\partial g}{\partial m_j})\} \not\subseteq \{\partial^t(\frac{\partial g}{\partial m_i})\}$

(b) $D(m_i)[m_i] = D(m_j)[m_j]$

Proof. We will apply lemma 6 to prove this,

(a) We are given that $\{\partial^t(\frac{\partial g}{\partial m_j})\} \not\subseteq \{\partial^t(\frac{\partial g}{\partial m_i})\}$ hence we can find a monomial n of degree t s.t $m_j n \in \mathcal{D}_{2t}$ and $\frac{\partial g}{\partial n m_j} \notin \{\partial^t(\frac{\partial g}{\partial m_i})\}$. Now we have two cases

- Say $m_i n \notin \mathcal{D}_{2t}$ then

$$\begin{aligned} & \frac{\partial}{\partial n} D(\frac{\partial g}{\partial m_i}) = 0 \\ \implies & \frac{\partial}{\partial n} (\sum_{r \in \mathcal{D}_t} \alpha_r \frac{\partial g}{\partial r}) = 0 \\ \implies & \sum_{m \in \mathcal{D}_t} \alpha_r \frac{\partial g}{\partial nr} = 0 \end{aligned}$$

Since $m_jn \in \mathcal{D}_{2t}$ we have $\frac{\partial g}{\partial m_jn} \neq 0$. Now $\alpha_{m_j} = D(m_i)[m_j]$ is the coefficient of $\frac{\partial g}{\partial m_jn}$ in the sum and since $\frac{\partial g}{\partial m_jn} \neq 0$ we have $D(m_i)[m_j] = 0$.

- Say $m_in \in \mathcal{D}_{2t}$ then we have $\frac{\partial}{\partial n}D(\frac{\partial g}{\partial m_i}) = \frac{\partial}{\partial m_i}D(\frac{\partial g}{\partial n})$, On L.H.S of the equation the coefficient of $\frac{\partial g}{\partial m_jn}$ is $D(m_i)[m_j]$ and on the R.H.S the coefficient of $\frac{\partial g}{\partial m_jn}$ is 0 because $\frac{\partial g}{\partial nm_j} \notin \{\partial^t(\frac{\partial g}{\partial m_i})\}$. Since $m_jn \in \mathcal{D}_{2t}$ we have $\frac{\partial g}{\partial m_jn} \neq 0$, hence $D(m_i)[m_j] = 0$.

(b) As $d > 2t$ we have a monomial r s.t $\mathbf{deg}\ r = t$ and $r|\frac{g}{\delta}$ where $\delta = \frac{m_im_j}{\mathbf{gcd}(m_i,m_j)}$ now it is clear that $m_ir, m_jr \in \mathcal{D}_{2t}$. Now by lemma 6 we have the following

$$\frac{\partial}{\partial m_i}D(\frac{\partial g}{\partial r}) = \frac{\partial}{\partial r}D(\frac{\partial g}{\partial m_i})$$

Now the coefficient of $\frac{\partial g}{\partial m_ir}$ on the L.H.S is $D(r)[r]$ and on the R.H.S is $D(m_i)[m_i]$ and since $\frac{\partial g}{\partial m_ir} \neq 0$ we have $D(m_i)[m_i] = D(r)[r]$. Similarly we get $D(m_j)[m_j] = D(r)[r]$. Hence we have $D(m_i)[m_i] = D(m_j)[m_j]$.

□

4.2 Simultaneously Upper Triangulation

In this section we will construct a basis for U' such that for any $(D', E') \in Adj(\partial^t, U', V')$ the representation of D' in the basis is block-diagonal and upper triangular.

Let's introduce a graph $G = (V, E)$ where $V = \bigcup_{i=1,\ldots,s} \mathcal{D}_{i,t}$ where $\mathcal{D}_{i,t} = \{m_j \mid \mathbf{deg}(m_j) = t \text{ and } m_j|g_i\}$ and $E = \{(m_i, m_j) \mid \partial^t(\frac{\partial g}{\partial m_i}) \subset \partial^t(\frac{\partial g}{\partial m_j})\}$. A few quick observations we get are as follows:-

1. All the $\mathcal{D}_{i,t}$ are disjoint because of the design condition as $\mathbf{deg}\ \mathbf{gcd}(g_i, g_j) < t$.
2. Again by design condition we have $\frac{\partial g}{\partial m_i} = \frac{\partial g_i}{\partial m_i}$ for each $i \in [s]$.

By the 2 observation we have $E = \bigcup_{i=1,\ldots,s} E_i$ where $E_i = \{(m_j, m_k) \mid \partial^t(\frac{\partial g_i}{\partial m_j}) \subset \partial^t(\frac{\partial g_i}{\partial m_k}) \text{ and } m_j, m_k \in \mathcal{D}_{i,t}\}$ and E_i's are disjoint.

Let's say G has a cycle $m_{i1}, \ldots.m_{in}$, by definition of the edge set, this is equivalent to saying that $\partial^t(\frac{\partial g}{\partial m_{i1}}) \subset \partial^t(\frac{\partial g}{\partial m_{in}}) \subset \partial^t(\frac{\partial g}{\partial m_{i1}})$ but it is not possible; thus G is acyclic.

Let $\mathbf{Top}(.)$ denote the to topological sort of a graph. Now since $\mathcal{D}_{i,t}$'s and E_i's are disjoint thus we have,

$$\mathbf{Top}(G) = \bigcup_{i=1\ldots s} \mathbf{Top}(\mathcal{D}_{i,t}, E_i)$$

Define $\mathbf{Top}_i = \mathbf{Top}(\mathcal{D}_{i,t}, E_i) = \{t_1, \ldots, t_b\}$, where $b = \mathbf{dim}\ U'_i$. Say $D \in Adj(\partial^t, U', V')$, then $D(t_i)[t_j] = 0$ (recall that this notation denotes the coefficient of t_j in $D(t_i)$) if if $i < j$ because else $\partial^t(\frac{\partial g}{\partial m_{t_j}}) \subset \partial^t(\frac{\partial g}{\partial m_{t_i}})$ which would mean there is an edge from t_j to t_i when $i < j$ which contradicts the fact that $\mathbf{Top}_i$ is a toplogical sort.

Let $\mathbf{Rev}(\{a_1, \ldots, a_n\}) = \{a_n, \ldots, a_1\}$ now notice that $\mathcal{B} = \bigcup_{i=1\ldots s} \mathbf{Rev}(\mathbf{Top}_i)$ is the basis of U', since $D'(t_i)[t_j] = 0$ for $i < j$ thus the representation of D' in the basis $\mathcal{B}$ is upper-triangular and by the uniqueness of the decomposition it is also block diagonal.

Algorithm 3 Vector Space Decomposition Algorithm

Input: Black box access to vector spaces $U = U_1 \oplus \cdots \oplus U_s$ and $V = U_1 \oplus \cdots \oplus U_s$ where (∂^t, U, V) form a vector space decomposition structure (for definition see section 1.1.2 of [4]).
Output: Black box access to $W_1, \ldots, W_s$ s.t $W_i = U_{\pi(i)}$ for some permutation π.

1: Find the basis $D_1, \ldots, D_b$ of $Adj(\partial^t, U, V)_1 = \{D \mid (D, E) \in Adj(\partial^t, U, V)\}$ by solving the system of linear equation given by $KD = EK$ for all $K \in \partial^t$.
2: Randomly pick $c_1, \ldots, c_b$ from a set S and let $D = c_1 D_1 + \cdots + c_b D_b$.
3: Find the eigenvalues of D, if there are s distinct eigenvalues call them $\lambda_1, \ldots, \lambda_s$ else abort.
4: Set $W_i = \mathbf{Ker}(D - \lambda_i I)^{\mathbf{dim}\ U}$ and output $W_1, \ldots, W_s$.

4.3 Vector Space Decomposition Algorithm

Now, we will design a randomised algorithm using the basis $\mathcal{B}$ constructed in the previous section.

4.3.1 Correctness Of Algorithm

To prove the correctness[2] of the algorithm, we have to prove a few lemmas. In the remaining section, we will use the notation defined in the algorithm without stating explicitly. Also, let $T : U' \to U$ be as defined in theorem 10.

First, let's make the following observations:-

1. Let $(D, E) \in Adj(\partial^t, U, V)$, now by theorem 10 and proposition 25 of [1] we have $(D', E') \in Adj(\partial^t, U', V')$ such that $D' = TDT^{-1}$. Now D and D' have the same eigenvalues. Express D' in the basis $\mathcal{B}$. In this representation of D', the eigenvalues are diagonal entries as it is upper triangular. We also know that D' is block diagonal with s blocks, and lemma 7 tells us that all diagonal entries of a block are the same.

2. Assume that the blocks of D' have pairwise distinct diagonal entries (which, because of the upper triangular nature, happen to be the eigenvalues of D') denoted by $\lambda_1, \ldots, \lambda_s$. In $(D' - \lambda_i I)$, the diagonal entry of the i-th block is 0; now we know that diagonal-less upper triangular matrix is nilpotent with order less than the dimension of the matrix. Hence the blocks in $(D' - \lambda_i I)^{dim U}$ have non-zero diagonal entries except the i-th block, which is as a whole 0. Thus by construction of $\mathcal{B}$ we have $\mathbf{Ker}(D' - \lambda_i I)^{\mathbf{dim}\ U} = U'_i$.

Lemma 8. *D has s distinct eigenvalues with probability $\geq 1 - \frac{\binom{s}{2}}{|S|}$*

Proof. By observation 1, it is enough to show that the blocks of D' have different diagonal entries. Denote the diagonal entry of the i-th block by $D'_i(c_1, \ldots, c_b) = \sum_{j=1}^{b} c_j D_j[i][i]$ (Look at D'_i as a linear form in $c_1, \ldots, c_b$).

Now we have $D'_i - D'_j \neq 0$ (as linear forms) as $a\mathbb{1}\big|_{U'_i} + b\mathbb{1}\big|_{U'_j}$ for $a \neq b$ is a member of $Adj(\partial^t, U, V)$ and since $D_1, \ldots, D_b$ is the basis of $Adj(\partial^t, U, V)$ there exists a b-tuple $\mathbf{c}_0$ s.t $(D'_i - D'_j)(c_0) = a - b \neq 0$. Hence by Schwartz-Zippel lemma, we have for a random b-tuple c, $(D'_i - D'_j)(c) \neq 0$ with a probablity $\geq 1 - \frac{1}{|S|}$.The analysis is true for arbitrary i, j; hence by union bound, the blocks of D have pairwise distinct with probability $\geq 1 - \frac{\binom{s}{2}}{|S|}$. □

Lemma 9. *$W_i = U_{\pi(i)}$ for some permutation π.*

[2] By that, we mean showing the algorithm gives the desired result with high probability

Proof. By observation 2 we have $\mathbf{Ker}(D' - \lambda_i I)^{dim\ U} = U_i'$ and by observation 1 we have $D' = TDT^{-1}$. Since T is invertible, we have the following

$$\begin{aligned}
\mathbf{Ker}(D' - \lambda_i I)^{\mathbf{dim}\ U} &= U_i' \\
\mathbf{Ker}(TDT^{-1} - \lambda_i I)^{\mathbf{dim}\ U} &= U_i' \\
\mathbf{Ker}(T(D - \lambda_i I)T^{-1})^{\mathbf{dim}\ U} &= (U_i') \\
\mathbf{Ker}(T(D - \lambda_i I)^{\mathbf{dim}\ U}T^{-1}) &= (U_i') \\
\mathbf{Ker}(T(D - \lambda_i I))^{\mathbf{dim}\ U} &= T(U_i'), \text{Since } T \text{ is invertible} \\
\mathbf{Ker}(D - \lambda_i I)^{\mathbf{dim}\ U} &= U_i
\end{aligned}$$

As we don't know the order in which we will get the eigenvalues, hence there exists a permutation π s.t $W_i = U_{\pi(i)}$. □

Hence lemma 8 and 9 proves that algorithm 2 works with probability $\geq 1 - \frac{\binom{s}{2}}{|S|}$.

Time Complexity: The dominant time cost is that of step 1, which involves solving a linear system of equations in $\mathbf{dim}(U)^2 + \mathbf{dim}(V)^2$ variables with $\binom{n+t-1}{t} \cdot \mathbf{dim}(V) \cdot \mathbf{dim}(U)$ many equations. Since $\mathbf{dim}(U) \leq s\binom{d}{t} < sd^t$ and $\mathbf{dim}(V) \leq s\binom{d}{2t} < sd^{2t}$,therefore there are $poly(s, n^t, d^t)$ many linear equations and poly(s, d^t) many variables in this system. Thus, such a system can be solved in poly(s, n^t, d^t) time.

5 Conclusions and future work

We have designed an equivalence test for design polynomials with some mild technical assumptions. A natural learning question which now arises is that if can we efficiently learn lower rank projections[3] of a design polynomial in the non-degenerate. Immediately one can see that there are important structural properties in the full-rank case that don't hold in the low-rank case. In our case, we proved the direct sum condition and uniqueness of decomposition using the properties of base polynomials as for full-rank projections the adjoint algebra of the projected polynomial is isomorphic to the adjoint algebra of the base polynomial (Even coming with up a reasonable non-degeneracy condition for which these conditions are satisfied is not trivial). Even though we can't use these properties, but for the low-sparsity case it seems like we can use the meta-framework of [4] to design a learning algorithm.

References

[1] Vishwas Bhargava, Ankit Garg, Neeraj Kayal, and Chandan Saha. Learning generalized depth three arithmetic circuits in the non-degenerate case. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2022)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2022.

[2] Alexander Chistov, Gábor Ivanyos, and Marek Karpinski. Polynomial time algorithms for modules over finite dimensional algebras. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, ISSAC '97, page 68–74, New York, NY, USA, 1997. Association for Computing Machinery.

[3] Ankit Garg, Nikhil Gupta, Neeraj Kayal, and Chandan Saha. Determinant equivalence test over finite fields and over Q. In *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, July 9-12, 2019, Greece*, volume 132 of *LIPIcs*, pages 62:1–62:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[3] By that we mean substituting linear forms in m variable in n-variate design polynomial where $m < n$

[4] Ankit Garg, Neeraj Kayal, and Chandan Saha. Learning sums of powers of low-degree polynomials in the non-degenerate case. In *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020*, pages 889–899. IEEE, 2020.

[5] Nikhil Gupta and Chandan Saha. On the symmetries of and equivalence test for design polynomials. In *44th International Symposium on Mathematical Foundations of Computer Science, MFCS 2019, August 26-30, 2019, Aachen, Germany*, volume 138 of *LIPIcs*, pages 53:1–53:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[6] Erich Kaltofen and Barry M. Trager. Computing with polynomials given byblack boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *Journal of Symbolic Computation*, 9(3):301–320, 1990. Computational algebraic complexity editorial.

[7] Neeraj Kayal. Affine projections of polynomials. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:61, 01 2011.

[8] Neeraj Kayal. Efficient algorithms for some special cases of the polynomial equivalence problem. In *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '11, page 1409–1421, USA, 2011. Society for Industrial and Applied Mathematics.

[9] Neeraj Kayal, Vineet Nair, Chandan Saha, and Sébastien Tavenas. Reconstruction of Full Rank Algebraic Branching Programs. In *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, pages 21:1–21:61, 2017.

[10] Neeraj Kayal and Chandan Saha. Reconstruction of non-degenerate homogeneous depth three circuits. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23-26, 2019*, pages 413–424. ACM, 2019.

6 Appendix

6.1 Adjoint Isomorphism

In this section, we will show that the adjoint algebra of a polynomial (in the sense defined in theorem 10) does not change under invertible transformations and translations.

The definitions used in this section can be found in appendix A of [1].

Theorem 10. *Let $g \in \mathbb{F}[\boldsymbol{x}]$, $\boldsymbol{x} = \{x_1, \ldots, x_n\}$, $h = g(l_1, \ldots, l_n)$ where $l_1, \ldots, l_n$ are linearly independent. Then $Adj(\partial^k, U_d, U_{d+k}) \cong Adj(\partial^k, U'_d, U'_{d+k})$ where $U_d = \langle \partial^{=d} g \rangle$ and $U'_d = \langle \partial^{=d} h \rangle$*

Proof. Define $T_d : U_d \to U'_d$ s.t $T_d(p) = p(l_1, \ldots, l_n)$. This map is injective as the map $p \to p(l'_1, \ldots, l'_n)$ is the left inverse of T_d where $(l'_1, \ldots, l'_n)$ is the inverse of $(l_1, \ldots, l_n)$ when seen as matrices. We will prove by induction on d that $\mathbf{im}(T_d) = U'_d$. For $d = 0$ it is clear that this holds. Let is be true for $d = q$ now for $d = q + 1$ we have,

Consider the identity

$$\frac{\partial(p(l_1, \ldots, l_n))}{\partial x_i} = \sum_{j=1}^{n} (\frac{\partial p}{\partial x_j})(l_1, \ldots, l_n) \frac{\partial l_j}{\partial x_i} \tag{4}$$

Since $l_1, \ldots, l_n$ are linearly independent thus we have $\langle \{\frac{\partial(p(l_1,\ldots,l_n))}{\partial x_i}\}_{i\in[n]} \rangle = \langle \{\frac{\partial p}{\partial x_i}(l_1, \ldots, l_n)\}_{i\in[n]} \rangle$

Let $u' \in \{\partial^{=q+1} g\}$ then we have a monomial m of degree $q + 1$ s.t $u' = \frac{\partial g}{\partial m}$, now $T_{q+1}(u') = \frac{\partial g}{\partial m}(l_1, \ldots, l_n)$. Now for some $i \in [n]$ we have $x_i | m$ and let $m' = \frac{m}{x_i}$ then define $u = \frac{\partial g}{\partial m'}$. Now $T_{q+1}(u') = \frac{\partial u}{\partial x_i}(l_1, \ldots, l_n) \in \langle \{\frac{\partial(u(l_1,\ldots,l_n))}{\partial x_i}\}_{i\in[n]} \rangle = \langle \{\frac{\partial(T_q(u))}{\partial x_i}\}_{i\in[n]} \rangle$ hence by induction hypothesis we have $T_{q+1}(u') \in U'_{q+1}$. Since u' is arbitary and $\{\partial^{=q+1} g\}$ is spanning set of U_{q+1} thus we have $\mathbf{im}(T_{q+1}) \subseteq U'_{q+1}$.
Let $v \in \{\partial^{=q+1} h\}$ then we have a monomial m of degree $q + 1$ s.t $v = \frac{\partial h}{\partial m}$. Now for some $i \in [n]$ we have $x_i | m$ and let $m' = \frac{m}{x_i}$, define $u' = \frac{\partial h}{\partial m'} \in U'_q$ now by induction hypothesis we have a $u \in U_q$ s.t $T_q(u) = u'$. Now we know that

$$\begin{aligned}
&\langle \{\frac{\partial(u(l_1, \ldots, l_n))}{\partial x_i}\}_{i\in[n]} \rangle = \langle \{\frac{\partial u}{\partial x_i}(l_1, \ldots, l_n)\}_{i\in[n]} \rangle \\
\implies &\langle \{\frac{\partial u'}{\partial x_i}\}_{i\in[n]} \rangle = \langle \{T_{q+1}(\frac{\partial u}{\partial x_i})\}_{i\in[n]} \rangle \\
\implies &v \in \langle \{T_{q+1}(\frac{\partial u}{\partial x_i})\}_{i\in[n]} \rangle
\end{aligned}$$

Since v is arbitary and $\{\partial^{=q+1} h\}$ is the spanning set of U_{q+1} thus we have $U'_{q+1} \subseteq \mathbf{im}(T_{q+1})$. This completes our proof of $U'_{q+1} = \mathbf{im}(T_{q+1})$.

We have isomorphic maps $T_d : U_d \to U'_d$ and $T_{d+k} : U_{d+k} \to U'_{d+k}$. Let $m = y_1 \cdots y_k$ ($y_1, \ldots, y_k$ are not necessarily distinct) and $\mathbf{deg}\ m = k$, now we have

$$\begin{aligned}\frac{\partial T_d(p)}{\partial m} &= \frac{\partial(p(l_1,\ldots,l_n))}{\partial m}\\ &= \sum_{i_1,\ldots,i_k=1}^{n}(\frac{\partial p}{\partial x_{i_1}\cdots x_{i_k}})(l_1,\ldots,l_n)\big[\frac{\partial l_{i_1}}{\partial y_1}\cdots\frac{\partial l_{i_k}}{\partial y_k}\big]\\ &= (\sum_{i_1,\ldots,i_k=1}^{n}(\frac{\partial p}{\partial x_{i_1}\cdots x_{i_k}})\big[\frac{\partial l_{i_1}}{\partial y_1}\cdots\frac{\partial l_{i_k}}{\partial y_k}\big])(l_1,\ldots,l_n)\\ &= T_d(\phi_k(\frac{\partial}{\partial m})p)\end{aligned}$$

where

$$\phi_k(\frac{\partial}{\partial m}) = \sum_{i_1,\ldots,i_k=1}^{n}\big[\frac{\partial l_{i_1}}{\partial y_1}\cdots\frac{\partial l_{i_k}}{\partial y_k}\big]\frac{\partial}{\partial x_{i_1}\cdots x_{i_k}} \tag{5}$$

Now, we show that ϕ_k is an invertible linear transformation. We first show that

$$\big\langle\{\frac{\partial p}{\partial m}(l_1,\ldots,l_n)\}_{\mathbf{deg}m=k}\big\rangle = \big\langle\{\frac{\partial p(l_1,\ldots,l_n)}{\partial m}\}_{\mathbf{deg}m=k}\big\rangle \tag{6}$$

Note that the L.H.S of equation 6 is just $\mathbf{im}(U_k)$ and R.H.S is U'_k, since $\mathbf{im}(U_k) = U'_k$, thus equation 6 holds. Now notice that coefficients of 5 is the coefficients of change of basis between the $L.H.S$ and $R.H.S$ of equation 6. Hence ϕ_k is invertible.

□

Theorem 11. *Let $g \in \mathbb{F}[\boldsymbol{x}]$, $\boldsymbol{x} = \{x_1,\ldots,x_n\}$, $h = g(\boldsymbol{x}+\boldsymbol{b})$ where $b = (b_1,\ldots,b_n) \in \mathbb{F}$. Then $Adj(\partial^k, U_d, U_{d+k}) \cong Adj(\partial^k, U'_d, U'_{d+k})$ where $U_d = \langle\partial^{=d}g\rangle$ and $U'_d = \langle\partial^{=d}h\rangle$*

Proof. Define $T_d : U_d \to U'_d$ s.t $T_d(p) = p(\mathbf{x}+\mathbf{b})$. This map is injective as the map $p \to p(\mathbf{x}-\mathbf{b})$ is the left inverse of T_d. Now we will show that T_d is surjective. Say $p \in U'_d$ then

$$\begin{aligned}p &= \sum_{\mathbf{deg}\ m=d} c_m\frac{\partial h}{\partial m}\\ &= \sum_{\mathbf{deg}\ m=d} c_m\frac{\partial g(\mathbf{x}+\mathbf{b})}{\partial m}\\ &= (\sum_{\mathbf{deg}\ m=d} c_m\frac{\partial g}{\partial m})(\mathbf{x}+\mathbf{b})\\ &= T_d(\sum_{\mathbf{deg}\ m=d} c_m\frac{\partial g}{\partial m})\end{aligned}$$

Hence $p \in \mathbf{im}(T_d)$, thus the map is surjective. Define $\phi : \langle\partial^k\rangle \to \langle\partial^k\rangle$ to be the identity function, then clearly it is invertible. Moreover, $\phi(L)T_d = T_{d+k}L$, $\forall L \in \langle\partial^k\rangle$, hence proved. □

6.2 Random Homogeneous Polynomial

In this section, we would like an average case estimate of t for a "Random homogeneous polynomial". We establish the conditions on s,t,d and n, under which a random homogeneous degree d polynomial of with s monomials has is a t design polynomial with high probability.

A random n-variate homogeneous degree d polynomial with s monomials is a polynomial where each one of the s monomials is selected independently of the others. By selecting a monomial, we mean choosing d variables from the n variables uniformly and independently with repetition allowed for each variable to form a degree d monomial.

Lemma 12. *A random n-variate homogeneous degree d polynomial with s monomials is a t-design polynomial with probability at most $1-\epsilon$, if $t \geq \frac{2log(\frac{s}{\sqrt{\epsilon}})}{log(\frac{n}{d^2})}$*

Proof. Let $E_{i,j}$ denote the event that for monomials m_i,m_j **deg gcd(** m_i,m_j) $\geq t$.

Clearly, **deg gcd(** m_i,m_j) $\geq t$ if and only if $\exists m$ such that **deg** $m \geq t$ and $m|m_i$ and $m|m_j$.

Now,

$$Pr[m|m_i, \textbf{deg } m = t] = \frac{\binom{n+d-t-1}{d-t}}{\binom{n+d-1}{d}}$$

This is because m_i is formed by choosing d variables uniformly at random with repetition, which can be done in $\binom{n+d-1}{d}$ ways. When $m|m_i$, then m_i is some multiple of m. In this case, m_i can be formed by selecting $d-t$ variables uniformly (as **deg** $m = t$), which can be done in $\binom{n+d-t-1}{d-t}$ ways.

Since m_i and m_j are selected independently of one another, therefore

$$Pr[m|m_i, m|m_j] = \frac{\binom{n+d-t-1}{d-t}^2}{\binom{n+d-1}{d}^2}$$

By using union bound on all $\binom{n+t-1}{t}$ many possible degree t monomials which can divide both m_i and m_j, we have

$$Pr[E_{i,j}] \leq \frac{\binom{n+t-1}{t}\binom{n+d-t-1}{d-t}^2}{\binom{n+d-1}{d}^2}$$

For a polynomial with s monomials, using union bound (on the $\binom{s}{2}$ possible pairs of monomials) we have:

$$Pr[\exists\ i,j \in [s]\ E_{i,j}] \leq \sum_{1 \leq i < j \leq s} \frac{\binom{n+t-1}{t}\binom{n+d-t-1}{d-t}^2}{\binom{n+d-1}{d}^2}$$

$$\leq \binom{s}{2} \frac{\binom{n+t-1}{t}\binom{n+d-t-1}{d-t}^2}{\binom{n+d-1}{d}^2}$$

$$\leq s^2 \frac{(n+t-1)!}{(n-1)!t!} \frac{(n+d-t-1)!^2}{(n-1)!^2(d-t)!^2} \frac{(n-1)!^2 d!^2}{(n+d-1)!^2}$$

$$= s^2 \frac{(n+t-1)!}{(n-1)!t!} \frac{(n+d-t-1)!^2}{(n+d-1)!^2} \frac{d!^2}{(d-t)!^2}$$

$$\leq s^2 \frac{(n+t-1)^t}{t!} \frac{d^{2t}}{(n+d-t)^{2t}}$$

$$= s^2 \frac{d^{2t}}{t!} \frac{(n+t-1)^t}{(n+d-t)^{2t}}$$

$$\leq s^2 \frac{d^{2t}}{t!} \frac{(2n)^t}{n^{2t}}$$

$$\leq \frac{s^2 d^{2t}}{n^t}$$

We need this probability to be small (say $\leq$ some ϵ). Thus,

$$s^2 \frac{d^{2t}}{n^t} \leq \epsilon$$

$$\frac{n^t}{d^{2t}} \geq \frac{s^2}{\epsilon}$$

$$t \geq \frac{2log(\frac{s}{\sqrt{\epsilon}})}{log(\frac{n}{d^2})}$$

The inequality in the last step holds as $n > d^2$. □

Our equivalence test works for (n, d, s, t) polynomial if it satisfies some technical conditions on the base field and $d > 3t$. From the above lemma we can see that a "random" homogeneous polynomial of degree $\delta t > d > 3t$ and sparsity $s < \sqrt{\epsilon(\frac{n}{d^2})^{\frac{d}{\delta}}}$ is t-design with a probability of $1-\epsilon$. So in this sense, we have an equivalence test for "random" homogeneous polynomial with some technical assumption on sparsity.