Folded Wronskian for Linear Independence Testing of Polynomials

1 Introduction

The Wronskian of a set of univariate polynomials $f_1, \ldots, f_n \in k[x]$ is defined as the matrix W whose entries are $d^{i-1} f_j / dx^{i-1}$. If the field k has characteristic 0, then a necessary and sufficient criterion for the polynomials to be linearly dependent is that the determinant of the Wronskian is the identically zero polynomial. This criterion fails for finite fields, since the derivatives of higher degree polynomials might be zero.

In order to fix this, Guruswami and Kopparty [2016] defined a variation of the Wronskian, which they call the $\gamma-$folded Wronskian. Here the matrix has entries $f_j(\gamma^{i-1}x)$ for some $\gamma \in k^\times$. They proved that the polynomials are linearly dependent if and only if the γ-folded Wronskain has identically zero determinant, as long as γ is a generator for $k^\times$, and $|k| > n$. The criterion was further generalised in Lokshtanov, Misra, Panolan, and Saurabh [2018], who proved that the criterion also works for any γ that has order $(n-1)d$, where d is the maximum degree of the polynomials.

We provide a simple proof of a slightly improved folded Wronskian criterion by imitating the proof of the regular Wronskian criterion from Bostan and Dumas [2010]. We first show that that the criterion is true in the case of monomials, and then argue that for any set of polynomials, the leading monomial of the folded Wronskian is the folded Wronskian of the leading monomials. Our proof allows us to relax the conditions on γ. We also give a criterion for linear dependence of multivariate polynomials, by generalising the Folded Wronskian in a manner similar to the way the usual Wronskian is generalised. However, unlike the previous works on the Folded Wronskian, we do not yet have an application for the improved criterion.

2 The Univaraite Criterion

We first formally state the criterion. Let $f_1, \ldots, f_n$ be a set of univariate polynomials in variable x. Let U be the vector space spanned by $f_1, \ldots, f_n$. Let $l_1, \ldots,$ be the set of trailing monomials of all vectors in U, arranged in increasing order of degree, and let $\nu := \deg l_n -$

$\deg l_1$. Let $\gamma \in \mathbb{F}$ be an element of the base field. Define matrix $W_\gamma(f_1, \dots, f_n)$ such that the i, j entry of $W_\gamma(\mathbf{f})$ is $f_j(\gamma^{i-1}x)$.

Lemma 2.1. *If* $\mathbf{f}$ *are linearly dependent over* $\mathbb{F}$*, then* $\det(W_\gamma(\mathbf{f})) = 0$ *for any* γ*. If* $\mathbf{f}$ *are linearly independent, then* $\det(W_\gamma(\mathbf{f})) \neq 0$ *as long as the order of* γ *is atleast* ν*.*

The proof of this lemma will require some intermediate results, which we first prove. These will essentially be proofs of the above lemma in special cases. The intuition for the condition on the order of γ is as follows. The Wronskian criterion is functional in nature, and if the base field is $\mathbb{F}_q$, it cannot distinguish between x and x^q, unless γ is from an extension of $\mathbb{F}_q$. The condition on the order of γ gives the smallest extension of the base field where the polynomials differ as functions.

We first prove the special case when the f_i are monomials. Note that monomials are linearly independent if and only if all of them have distinct degrees.

Lemma 2.2. *Suppose* $\mathbf{f}$ *is such that* $f_i = a_i x^{d_i}$*, with all* d_i *distinct. Then* $\det(W_\gamma(\mathbf{f})) \neq 0$ *as long as each* γ^{d_i} *is distinct.*

Proof of lemma 2.2. By definition, we have

$$W_\gamma(\mathbf{f}) = \begin{bmatrix} a_1 x^{d_1} & \dots & a_n x^{d_n} \\ a_1 \gamma^{d_1} x^{d_1} & \dots & a_n \gamma^{d_n} x^{d_n} \\ \vdots & \vdots & \vdots \\ a_n \gamma^{(n-1)d_1} x^{d_1} & \dots & a_n \gamma^{(n-1)d_n} x^{d_n} \end{bmatrix}.$$

Computing the determinant, we can factor out $a_i x^{d_i}$ from every row. We thus get

$$\det W_\gamma(\mathbf{f}) = \left(\prod_{i=1}^{n} a_i x^{d_i} \right) \times \det \left(\begin{bmatrix} 1 & 1 & 1 \\ \gamma^{d_1} & \dots & a_n \gamma^{d_n} \\ \vdots & \vdots & \vdots \\ \gamma^{(n-1)d_1} & \dots & \gamma^{(n-1)d_n} \end{bmatrix} \right).$$

The matrix on the right hand side of the above display is the Vandermonde matrix on $\gamma^{d_1}, \dots, \gamma^{d_n}$. This is non-zero as long as each γ^{d_i} is distinct. This completes the proof for the monomial case. □

The next lemma will show that we can reduce the general case to a triangular system without changing the non-zeroness of the folded Wronskian. Here, by a triangular system we mean that the lowest degree terms on each f_i will have a different degree, and this degree is increasing with i. In order words, the trailing monomials of the f_i form a strictly increasing sequence.

Lemma 2.3. *Given* $\mathbf{f}$*, we can find an invertible matrix* A*, such that the polynomials* $\mathbf{g} = A\mathbf{f}$ *satisfy the following:* $\mathrm{TM}(g_1) \prec \mathrm{TM}(g_2) \prec \dots \prec \mathrm{TM}(g_n)$*. In addition, the matrix* A *also satisfies* $W_\gamma(\mathbf{g}) = AW_\gamma(\mathbf{f})$*.*

Proof of lemma 2.3. The idea is to perform Gaussian elimination. Treat each f_i as a vector F_i of coefficients of powers of x, that is a vector whose j^{th} entry is the coefficient of x^{j-1} in f_i. Construct the matrix M whose i^{th} row is F_i. Since the f_i are independent, the matrix M has full rank. We can apply elementary row operations on M to obtain a matrix M' which has row reduced echelon form of M. This corresponds to multiplying M on the left by a product of elementary matrices, say B. Each of the rows of M' correspond to polynomials. Call these polynomials $\mathbf{g}$. Since M' has row echelon form, $\mathbf{g}$ satisfy the trailing monomial condition. The required matrix A is then just B^T.

Finally, since the entries of A are constants, and for any polynomials a, b and constants α, β it holds that $(\alpha a + \beta b)(\gamma x) = \alpha a(\gamma x) + \beta b(\gamma x)$, we get $\mathbf{g}(\gamma^{j-1}x) = \mathbf{f}(\gamma^{j-1}x)A$, and thus $W_\gamma(\mathbf{g}) = W_\gamma(\mathbf{f})A$. □

In the above lemma, since A is invertible, it holds that $\det(W_\gamma(\mathbf{g})) \neq 0$ if and only if $\det(W_\gamma(\mathbf{f})) \neq 0$.

We will now prove the main lemma for triangular systems of polynomials.

Lemma 2.4. *Let* $\mathbf{f}$ *be a triangular system of independent polynomials. Define* d_i *such that* $\mathrm{TM}(f_i) = x^{d_i}$*. Then* $\det(W_\gamma(\mathbf{f})) \neq 0$ *as long as* γ *is such that all* γ^{d_i} *are distinct.*

Proof of lemma 2.4. By assumption, $d_1 < d_2 < \cdots < d_n$. Let $W := W_\gamma(\mathbf{f})$ for brevity. We have $\det(W) = \sum_\sigma (-1)^\sigma \prod W_{i\sigma(i)}$. For every σ, the term $\prod W_{i\sigma(i)}$ has the same trailing monomial, namely $x^{d_1+\cdots+d_n}$. This is because each column in W has polynomials with the same trailing monomial, namely x^{d_i}. We thus get $\mathrm{TT}(\det(W)) = \sum_\sigma (-1)^\sigma \prod \mathrm{TT}\left(W_{i\sigma(i)}\right)$. The expression on the right is just the determinant of the trailing terms of the entries of W, which is $\det(W_\gamma(\mathrm{TT}(\mathbf{f}))$. By assumption, the $\mathbf{f}$ have distrinct trailing monomials, and hence distinct trailing terms. By lemma 2.2 we get that $\det(W_\gamma(\mathrm{TT}(\mathbf{f}))$ is nonzero. Since $\det(W)$ has a nonzero trailing monomial, it itself is nonzero. This completes the proof of the lemma. □

Using these, we now prove the main lemma.

Proof of lemma 2.1. We first show the first assertion of the lemma. Suppose $\mathbf{f}$ are linearly dependent, and $\mathbf{c} \in \mathbb{F}^n$ is such that $\sum c_i f_i(x) = 0$, and $c_i \neq 0$ for some i. We then also have $\sum c_i f_i(\gamma^j x) = 0$ for any γ and j. This implies $W_\gamma(\mathbf{f})\mathbf{c} = 0$, whence the determinant of $W_\gamma(\mathbf{f})$ must be 0.

We now prove the second assertion. Given input polynomials $f_1, \ldots, f_n$, we use lemma 2.3 to obtain polynomials $g_1, \ldots, g_n$ that form a triangular system. Further, it holds that $l_n = \mathrm{TT}(g_n)$. Since γ has order alteast ν, it holds that γ^{d_i} take distinct values where d_i is the degree of the trailing monomial of g_i. The polynomials $g_1, \ldots, g_n$ satisfy the requirements of lemma 2.4, an application of which gives that $\det W_\gamma(\mathbf{g}) \neq 0$. Finally, since $W_\gamma(\mathbf{g}) = AW_\gamma(\mathbf{f})$ with A invertble, we have the required result that $\det W_\gamma(\mathbf{f}) \neq 0$. □

3 Generalised Folded Wronskian

For multivariate polynomials, we try and define a generalised version of the folded Wronskian criterion, similar to the generalised version of the classical Wronskian criterion. For notational convenience, in this section we index some things from 0. The input polynomials will be $f_0, \ldots, f_{n-1}$. They will be in variables $x_1, \ldots, x_m$.

In the generalised classical Wronskian, one considers differential operators $\Delta_0, \Delta_1, \ldots, \Delta_{n-1}$, where each Δ_j is of the form $\partial_{x_{i_1}} \partial_{x_{i_2}} \ldots \partial_{x_{i_k}}$ with $k \leqslant j$. Note that $\Delta_0 = \text{id}$. Corresponding to these Δ_i, we can define a generalised classical Wronskian where the entry in row i and column j is $\Delta_i(f_j)$. Here both the row and columns are indexed from 0. There are finitely many sets of differential operators of the above kind. The generalised Wronskian criterion says that if the polynomials are linearly independent, then there exist some set of differential operators of the above kind such that the determinant of the corresponding generalised classical Wronskian is nonzero. We will call such sets of differential operators witnesses to the linear independence.

We now describe the criterion in the case of folded Wronskians. Fix some γ. Define the operator $\delta_i(f(x_1, \ldots, x_i, \ldots, x_m)) = f(x_1, \ldots, \gamma x_i, \ldots, x_m)$. It holds, similar to the partial derivation operator, that $\delta_i \delta_j = \delta_j \delta_i$. Let $\Delta_0, \ldots, \Delta_{n-1}$ be a set of operators such that $\Delta_j = \delta_{x_{i_1}} \ldots \delta_{x_{i_k}}$. Note that these differential operators can be seen as considering monomials in $k[y_1, \ldots, y_m]$ and substituting δ_i for y_i. We can also consider arbitrary polynomials in $k[\mathbf{y}]$ and substitute δ_i. For the criterion it suffices to look at monomial operators, but the proof will use these more general polynomial operators. Looking at them this way, we can assign a degree and a support to each operator, both in the natural way. If the operator is obtained by substituting in monomial $\mathbf{m}$, then the degree of the operator will be the total degree of $\mathbf{m}$, and the support of the operator will be the support of $\mathbf{m}$.

Define the generalised folded Wronskian $W(\mathbf{f})$ such that it has ij^{th} entry $\Delta_i(f_j)$. Let U be the vector space spanned by all of the $\mathbf{f}$. For a particular monomial ordering, we can consider the set of least terms $l_1, \ldots,$ of all elements in U. Each l_i is a monomial in $x_1, \ldots, x_m$. Suppose $l_i = x_1^{\beta_{i1}} \ldots x_m^{\beta_{im}}$. Define $\nu := \left(\max_{1 \leqslant i,j \leqslant n} \beta_{ij}\right) - \left(\min_{1 \leqslant i,j \leqslant n} \beta_{ij}\right)$. This ν depends only on the monomial ordering and the inputs $\mathbf{f}$. We can minimise ν over all possible monomial orderings. For the rest of the section, fix that monomial ordering which minimises ν.

We have the following two multivariate folded Wronskian criteria.

Lemma 3.1 (Degree Criterion)**.** *If* $\mathbf{f}$ *are linearly independent and if the order of* γ *is atleast* ν*, then we can find a set differential operators* $\Delta_0, \ldots, \Delta_{n-1}$ *such that* $\det(W(\mathbf{f})) \neq 0$*. The operators* $\Delta_0, \ldots, \Delta_{n-1}$ *further satisfy* $\deg \Delta_i = i$.

Lemma 3.2 (Support Criterion)**.** *If* $\mathbf{f}$ *are linearly independent and if the order of* γ *is atleast* ν*, then we can find a set differential operators* $\Delta_0, \ldots, \Delta_{n-1}$ *such that* $\det(W(\mathbf{f})) \neq 0$*. The operators* $\Delta_0, \ldots, \Delta_{n-1}$ *further satisfy* $|\text{Supp}(\Delta_i)| \leqslant \log i$.

As in the univariate criterion, we will reduce a general instance to a monomial instance. The reduction will be the same as before, while the monomial instance will require some more work. We first prove the reduction, which is the same for both the lemma. We then prove each of lemma for monomial instances separately. The intuition for the condition on γ is also similar to the intuition for the univariate case: the lower bound on the order of γ forces us to go to a field extension where the f_i are guaranteed to be different as functions, and not just as formal polynomials.

Lemma 2.3 holds in the multivariate case exactly as stated, for every choice of derivative operators, and for every monomial ordering. For every choice of operators, and for every monomial ordering, it also holds that $\mathrm{TT}\left(\det W(\mathbf{f})\right) = \det W(\mathrm{TT}\left(\mathbf{f}\right))$. We thus only need to show the two lemma in the case of monomials. Let $f_i = \mathbf{x}^{\mathbf{e}_i} = \prod_{j=1}^{m} x_j^{e_{ij}}$ be linearly independent, or equivalently be such that that all the exponent vectors $\mathbf{e}$ are distinct. We put the proofs of each of the two lemma in separate subsections. The two proofs require looking at the operators differently, but this is only because I have not been able to unify them satisfactorily yet. The proofs of these two are modifications of the classical versions of the same lemma, from Bostan and Dumas [2010] and Forbes, Saptharishi, and Shpilka [2014] respectively.

3.1 Degree Criterion for Monomial Instances

We look at the operators Δ_i as integer vectors as follows. Each operator Δ_i is obtained by picking a monomial in $k\left[\mathbf{y}\right]$ and substituting δ_i for y_i. Let $\mathbf{ff}_i$ be the exponent vector of the monomial corresponding to Δ_i. If $\Delta_i = \delta_{x_{i_1}} \ldots \delta_{x_{i_k}} = \delta_{x_1}^{\alpha_{i1}} \delta_{x_2}^{\alpha_{i2}} \ldots \delta_{x_m}^{\alpha_{im}}$, then $\mathbf{ff}_i = (\alpha_{i1}, \ldots, \alpha_{im})$. The entry in the i^{th} row and j^{th} column of W is then just $\mathbf{x}^{\mathbf{e}_j} \left(\gamma^{e_{j1}}\right)^{\alpha_{i1}} \left(\gamma^{e_{j2}}\right)^{\alpha_{i2}} \ldots \left(\gamma^{e_{jm}}\right)^{\alpha_{im}}$. When considering the determinant, we can factor out the $\mathbf{x}^{\mathbf{e}_j}$ from the j^{th} column. We thus only need to consider the matrix where the ij^{th} entry is $\left(\gamma^{e_{j1}}\right)^{\alpha_{i1}} \left(\gamma^{e_{j2}}\right)^{\alpha_{i2}} \ldots \left(\gamma^{e_{jm}}\right)^{\alpha_{im}}$. To simplify notation, we set $c_{ij} := \gamma^{e_{ij}}$. By the assumption on the order of γ, if $e_{ij} \neq e_{kl}$ then $c_{ij} \neq c_{kl}$. Further let $\mathbf{c}_i := (c_{i1}, c_{i2}, \ldots, c_{im})$, generalising the exponent vectors.

Let $u_1, \ldots, u_m$ be new formal variables. Consider the linear forms $\nu_i := \sum_j u_j c_{ij}$. We now study the Vandermonde matrix of these linear forms. Call this matrix V. Since the exponent vectors $\mathbf{e}_i$ are all distinct, so are $\mathbf{c}_i$, and hence so are the ν_i. Therefore the matrix V has nonzero determinant. We now study this determinant.

Each entry in the i^{th} row of V is of the form $\left\langle \mathbf{u}, \mathbf{c}_j \right\rangle^i$. For a fixed j, this is a homogeneous polynomial both in $\mathbf{u}$ and in $\mathbf{c}_j$. Upon expanding, we get a sum of monomials, each of total degree i in the $\mathbf{u}$. In particular, we get a monomial corresponding to each vector of natural numbers $[k_1, \ldots, k_m]$ whose entries sum to i. Let $\mathcal{M}_i$ be the set of all such vectors, and let $a_{\mathbf{m}}$ denote the corresponding multinomial coefficients. [1] We can write the i^{th} row

[1] Depending on the characteristic, some of these coefficients can be 0, but this does not affect the criterion.

as

$$V_i = \sum_{\mathbf{m} \in \mathcal{M}_i} \left(a_{\mathbf{m}} \mathbf{u}^{\mathbf{m}} \left[\mathbf{c}_1^{\mathbf{m}} \quad \mathbf{c}_2^{\mathbf{m}} \quad \cdots \quad \mathbf{c}_n^{\mathbf{m}} \right] \right).$$

We now use the multilinearity of the determinant. Each row of V is the sum of vectors of the above form. The determinant of V can be written as the sum of determinants of V_j, where each V_j corresponds to a choice from the summands for each row. If for a fixed V_j, the choices of $\mathbf{m}$ for the rows is $\mathbf{m}_0, \ldots, \mathbf{m}_{n-1}$, then the determinant of V_j, after factoring out the multinomial coefficients and the variables $\mathbf{u}$, will be exactly the determinant of the generalised Wronskian obtained by picking $\Delta_i := \mathbf{m}_i(\delta_1, \ldots, \delta_m)$. If all of the generalised Wronskians had 0 determinant, so would V, which is a contradiction.

3.2 Support Criterion for Monomial Instances

We will need some intermediate lemma. The first of these is about univariate monomials x^{d_i}. Defining δ to be the univariate operator that multiplies the argument by γ, it says that we can find polynomials in the operator δ that act as indicator functions for various monomials x^{d_i}.

Lemma 3.3. *Fix an integer d which is atmost the order of γ. For each $0 \leqslant j < d$, there exists a polynomial $I_j \in k[y]$ of degree atmost $d-1$ such that for every $0 \leqslant i, j < d$, $(I_j(\delta)(x^i))(1)$ is 1 if and only if $i = j$, and is 0 otherwise.*

Proof of lemma 3.3. Let D be a zero indexed matrix, defined as $D_{ij} = (\delta^j x^i)(1)$. This matrix is invertible, since it is the Vandermonde matrix on $1, \gamma, \gamma^2, \ldots, \gamma^{d-1}$. Let C be its inverse. Define I_j as $I_j = \sum_k C_{j,k} y^k$. We then have

$$\begin{aligned}
(I_j(\delta)(x^i))(1) &= \sum_k C_{j,k} \delta^k (x^i)(1) \\
&= \sum_k C_{j,k} \gamma^{ik} \\
&= \sum_k C_{j,k} D_{k,i}.
\end{aligned}$$

The final term is the ij^{th} entry of the identity matrix, since C and D are the inverses of each other. Thus it is 1 if and only if $i = j$, and 0 otherwise. □

We now extend this to the multivariate case, by repeated applications of the univariate case. Fix a particular monomial $\mathbf{m} := x_1^{b_1} x_2^{b_2} \ldots x_m^{b_m}$. Consider the polynomial I_{b_1} obtained from lemma 3.3. Note that we satisfy the requirements of the lemma due to the assumption on the order of γ. We have $I_{b_1}(\delta_1)(\mathbf{m})(1, x_2, \ldots, x_m) = x_2^{b_2} \ldots x_m^{b_m}$. Further, for any other monomial $\mathbf{m}' = x_1^{c_1} \ldots x_m^{c_m}$ with $c_1 \neq b_1$ we have $I_{b_1}(\delta_1)(\mathbf{m}')(1, x_2, \ldots, x_m) = 0$.

If we now consider the operator $I_{\mathbf{m}} := I_{b_1}(\delta_1)I_{b_2}(\delta_2)\dots I_{b_m}(\delta_m)$, then $I_{\mathbf{m}}(\mathbf{m})(1,\dots,1) = 1$, and for any other monomial $I_{\mathbf{m}}(\mathbf{m}')(1,\dots,1) = 0$. Therefore operators of this form act as indicators for multivariate monomials. If we pick operators corresponding to the monomials $\mathbf{e}_i$ and construct the Wronskian, we will get a matrix whose determinant evaluates to 1 at $1,\dots,1$, and thus the determinant has to be nonzero. However, each of these operators are polynomial operators and not monomial operators. Further they are of full support. They do not therefore give us the required result. We now improve this to show that we can come up with log support operators that can weakly separate monomials from a fixed set.

Let f_i be monomials as before. All of the exponent vectors $\mathbf{e}_i$ are distinct. We want to find some particular f_{i_0}, and a subset $S \subset [m]$ of size $\log n$, such that $\mathbf{e}_{i_0}$ restricted to the indices S is distinct from all other $\mathbf{e}_j$ restricted to the indices S. To do this, start with an index where not all the $\mathbf{e}_i$ agree, say without loss of generality that this is 1. There must be atleast two distinct values taken by e_{i1} as we run over all the i. Therefore, there must be some value that is taken by atmost half the exponent vectors in this index. Among these exponent vectors, we can find another index where they do not all agree, and a value taken by atmost half of them. We will need to do this atmost $\log n$ many times before we end up with a single exponent vector $\mathbf{e}_k$, and a set of indices of $\log n$ size such that $\mathbf{e}_k$ differs from the rest of the $\mathbf{e}_j$ when restricted to these indices. Setting $i_0 = k$ and S to be this index set, we have what we wanted.

Consider now the monomial $\mathbf{m}$ obtained by starting with f_{i_0} and setting all x_j with $j \notin S$ to 1. This is a monomial with $\log n$ many variables. We can construct operator $I_{\mathbf{m}}$ as before, due to the assumption on the order of γ. By the construction of S and the choice of i_0, we have that $I_{\mathbf{m}}(f_{i_0})(1,\dots,1) = 1$, and for all other f_j we have $I_{\mathbf{m}}(f_j)(1,\dots,1) = 0$. We have thus managed to separate f_{i_0} from the remaining monomials, using an operator of support only $\log n$. Now we induct. Without loss of generality assume that $i_0 = 0$. Consider now the $n-1$ monomials $f_1,\dots,f_{n-1}$. There is some i_1, say $i_1 = 1$ and an operator $I_{\mathbf{m}'}$ of $\log n - 1$ support that can separate f_1 from $f_2,\dots,f_{n-1}$. Note that this operator might not be able to separate f_1 and f_0, which is why we call this separation weak. By repeating this, and after potentially rearranging the monomials, we can obtain a sequence of operators $I_{\mathbf{m}_0},\dots,I_{\mathbf{m}_{n-1}}$ such that for every i, $I_{\mathbf{m}_i}$ is able to separate f_i from $f_{i+1},\dots,f_{n-1}$, in the sense described above. Further, $I_{\mathbf{m}_i}$ has support size $\log n - i$. Consider the matrix V whose entry in position ij is $I_{\mathbf{m}_i}(f_j)$. When evaluated at $1,\dots,1$, this matrix is lower triangular, with diagonals all 1. Therefore the matrix has non-zero determinant.

The only remaining step is to go from polynomial operators $I_{\mathbf{m}_i}$ to monomial operators. Each operator $I_{\mathbf{m}_i}$ is a sum of monomial operators. Further, by the linearity of δ_i, for any two operators J, J' and monomial $\mathbf{m}$ we have $(J + J')(\mathbf{m}) = J(\mathbf{m}) + J'(\mathbf{m})$. Using this fact, along with the multilinearity of the determinant operator, we can write the determinant of V as the sum of determinants of matrices V_i, where in each of the V_i, the operator applied to each row is a monomial operator. Since $\det V \neq 0$, one of these V_i must have non-zero determinant. Let the monomial operators corresponding to V_i be $J_0,\dots,J_{n-1}$.

Setting $\Delta_i = J_{n-1-i}$ gives us the required witness.

4 Bibliography

Alin Bostan and Philippe Dumas. Wronskians and linear independence. *The American Mathematical Monthly*, 117(8):722–727, 2010. doi: 10.4169/000298910X515785. URL https://doi.org/10.4169/000298910X515785.

Michael A. Forbes, Ramprasad Saptharishi, and Amir Shpilka. Hitting sets for multilinear read-once algebraic branching programs, in any order. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 867–875, 2014. doi: 10.1145/2591796.2591816. URL https://doi.org/10.1145/2591796.2591816.

Venkatesan Guruswami and Swastik Kopparty. Explicit subspace designs. *Combinatorica*, 36(2):161–185, Apr 2016. ISSN 1439-6912. doi: 10.1007/s00493-014-3169-1. URL https://doi.org/10.1007/s00493-014-3169-1.

Daniel Lokshtanov, Pranabendu Misra, Fahad Panolan, and Saket Saurabh. Deterministic truncation of linear matroids. *ACM Trans. Algorithms*, 14(2):14:1–14:20, March 2018. ISSN 1549-6325. doi: 10.1145/3170444. URL http://doi.acm.org/10.1145/3170444.