On Arithmetical Formulas Whose Jacobians are Gröbner Bases

Charles Denis*
University at Buffalo

Kenneth W. Regan†
University at Buffalo

Abstract

We exhibit classes of polynomials whose sets of kth partial derivatives form Gröbner bases for all k, with respect to all term orders. The classes are defined by syntactic constraints on arithmetical formulas defining the polynomials. Read-once formulas without constants have this property for all k, while those with constants have a weaker "Gröbner-bounding" property introduced here. For $k = 1$ the same properties hold even with arbitrary powering of subterms of the formulas.

1 Introduction

One of the great unsolved problems of computational mathematics is finding lower bounds on the size of arithmetical circuits or formulas defining certain polynomial functions over a given field F. A famous example concerns the *determinant polynomials* d_n and *permanent polynomials* p_n in $F[x_1, \ldots, x_{n^2}]$, defined to be the determinant (respectively, permanent) of the $n \times n$ matrix M_n of variables $x_1, \ldots, x_{n^2}$ (in row-major order). It is known that the d_n have arithmetical circuits of polynomial size and arithmetical formulas of "quasi-polynomial" size $2^{O(\log^2 n)}$, with the same formulas working over any field (see [BCS97]). Valiant [Val79] proved that over any field F of characteristic other than 2, however, computing $p_n(A)$ for a given $n \times n$ 0-1 matrix A is NP-hard. In computational complexity theory this is considered strong evidence that the permanent polynomials do not have (quasi-)polynomial size circuits or formulas—and Valiant conjectured a $2^{\Omega(n)}$ lower bound on the size of both.

However, no lower bounds better than $\Omega(n \log n)$ for arithmetical circuits or even formulas, for any explicitly-given "natural" family of degree-$n^{O(1)}$ polynomials in n variables over an infinite field. The gap in our knowledge seems partly due to the difficulty of associating a mathematical invariant with the size complexity measure of circuits or formulas. The salient case of success—and almost the only one to date—is Strassen's famous "degree method," which applies for any infinite field. Strassen showed that the arithmetical circuit size of a polynomial map from F^n to F^m is bounded below by the logarithm (to base 2) of the *geometric degree* of the irreducible algebraic variety in F^{n+m} denoted by the graph of the map. (This extends to rational maps with appropriate localization; see [BCS97].) In the case of a single polynomial p, the circuit size of p is also Ω-of the logarithm of the geometric degree of the mapping defined by the n-many first partial derivatives of p. This was instrumental in the latest and best application of the degree method by Baur and Strassen [BS82]. The limitation, however, is that the geometric degree of a mapping by degree-d polynomials never exceeds d^n, and this explains why the best lower bounds obtained by this method for polynomials of degree $d = n^{O(1)}$ are $\Omega(n \log n)$.

*Supported in part by NSF grant CCR-9821040

†Supported in part by NSF grant CCR-9821040. Corresponding author—contact: regan@cse.buffalo.edu

The question becomes whether one can associate a mathematical invariant of higher magnitude than singly exponential to (ideals or varieties defined from) polynomials p, while preserving Strassen's connection to arithmetical circuit (or formula) size. A central development in the past two decades has been proofs of tight double-exponential bounds for many "complexity measures" of polynomial ideals. Most of these are connected with the degree and size of *Groöbner bases* for the ideals, but several can be stated without reference to Gröbner bases. These include the number of associated primes, the *Castelnuovo-Mumford regularity*, and the related notion of *arithmetical degree* propounded by Bayer and Mumford [BM93][1] Were Strassen's logarithmic relationship to circuit size to extend from geometric degree to arithmetic degree, this would have instantly afforded exponential lower bounds on circuit size. However, the double-exponential growth in all of these quantities is realizable by the so-called "Mayr-Meyer ideals" ([MM82]; see also [MM84, Huy86, BS88, Yap91]), and these can be defined by linearly-many formulas of constant size and degree! Moreover, the Mayr-Meyer ideals can be obtained via the first partial derivatives of polynomials p_n defined by multi-linear read-twice formulas of linear size (in unfactored form, i.e. Σ_2 form) and constant degree. Getting this growth from small-formula cases is actually instrumental to the complexity results (*viz.*, "exponential space completeness") in these papers. The conundrum is whether there is a mathematical quantity that is doubly exponential in the number of variables, and/or the *number* and/or *degree* of given generators for an ideal, but still only singly exponential in the formula or circuit size of these generators.[2]

We do not address this conundrum here, but instead go to the opposite end of the problem: Which classes of formulas have the *simplest* ideals? Here again our question is motivated by Valiant's permanent-versus-determinant problem and his general approach. For all n and k, and with respect to any "diagonal" term-order (i.e., one that extends the "is northwest of" relation of the n^2 variables when arranged into an $n \times n$ matrix), the kth partial derivatives of the determinant polynomials d_n form a Gröbner basis [Stu90, CGG90]. These are essentially the same as the $n-k$ by $n-k$ minors of the matrix of variables, and the so-called *determinantal ideals* they generate have many nice geometric properties and are a major topic of study. For the permanent polynomials p_n, however, the corresponding "permanental ideals" are far from nice, as studied by Laubenbacher and Swanson [LS98]. Computer runs on p_4 and p_5 suggest explosive growth in Gröbner basis size and degree.[3]

Here we ask, which other classes of formulas have the same "Gröbner-minimum" property as the determinant polynomials? We prove this for *read-once* (RO) formulas, namely those in which every literal is a different variable. In the case $k = 1$ of the first partial derivatives, we prove this for some notable generalizations of RO formulas. The read-once concept has been studied in other areas of complexity theory, and we were drawn to it here by the simple fact that every formula ϕ is a *Valiant projection* of the RO formula ϕ' obtained by replacing every occurrence of a variable or constant in ϕ by a different variable. The number s of variables in ϕ' is the same as the formula size of ϕ. A single-step projection either substitutes a field constant for a variable or identifies two variables; a Valiant projection is a composition of these. Every formula ϕ of size s is also known to

[1] That arithmetical degree is subject to the same lower bounds shown for several kinds of regularity in [BM93] is actually not observed in [BM93]; it is proved in [HT98] (p534) noting a gap in the literature.

[2] The attraction is that such a quantity might evade a meta-mathematical obstacle to a proof of super-polynomial circuit size (or of NP $\neq$ Ptime) demonstrated by Razborov and Rudich [RR97]. To do so, it appears that the ideals in question would need to have formal descriptions of size polynomial in the parameter n with respect to which complexity is being measured. At present it seems that the ideals formed by the first partial derivatives of the permanent polynomials p_n would meet all requirements.

[3] Under grevlex order, the Hessian ideal of p_5 (generated by 3×3 permanental minors) took 37-1/4 days for *Singular* [GPS98] to output the unique minimum reduced Gröbner basis of size 257,576 on one processor of a 12-processor !!, while a conservative estimate is that the same computation given the 35 generators of $Jac(p_5)$ would take over 100 years to halt.

be a Valiant projection of the determinant polynomial d_{s+1} (see [Val79, Val82, vzG87]; the latter gives an elegant projection from d_{s+2}). The best lower bound on s_n such that the permanent polynomials p_n are *not* Valiant projections of d_{s_n}, however, is $s_n < \sqrt{2}n$ [Cai90]. It is possible that a good upper bound on the increase in some numerical invariant of polynomial ideals under a single-step projection, coupled with a good lower bound on the same quantity for the permanental ideals, could be used to improve the constant $\sqrt{2}$ in this lower bound—but owing to the Mayr-Meyer examples we do not see how to do better than that even here.

Section 2 defines the classes of formulas and gives the facts about Gröbner bases needed for our proofs, which come in Section 3. A concluding Section 4 re-visits the above motivations and gives some related mathematical problems.

2 Definitions and Background

We consider arithmetical formulas involving variables $x_1, x_2, \ldots$, arbitrary constants in the field F, and the operators $+$, $-$, and $*$. It is sometimes helpful to picture the formula as a binary tree directed toward the root whose leaves are the literals (i.e., variables or constants) and whose interior nodes are the operators. The root is called both the output node and the highest operator. An arithmetical circuit is obtained by allowing nodes to have arbitrarily many out-edges and (optionally, for higher-arity $+$ and $*$) in-edges, without introducing any directed cycles and keeping the root as the only sink. Then a formula is the same as a circuit of fanout 1. We define *formulas with powering* formally by introducing unary nodes, each having a positive integer for the power.

The *size* of a formula or circuit is standardly the number of operators, but for formulas we prefer to count the number of literals. Known results on eliminating divisions from formulas from polynomials (see [BCS97]) enable us to avoid considering the / operator here. Since our results distinguish between the presence or absence of constants, we chose to include the $-$ operation as a primitive, rather than simulate it by -1 and $*$. For any formula ϕ, let $Var(\phi)$ denote the set of distinct variables occurring in ϕ.

Definition 2.1. (a) *Read-once* (RO) formulas are inductively definable by:

(B1) Every variable x_i is an RO formula.

(I1) If ϕ_1 and ϕ_2 are RO formulas and $Var(\phi_1) \cap Var(\phi_2) = \emptyset$, then $\phi_1 + \phi_2$, $\phi_1 - \phi_2$, and $\phi_1 * \phi_2$ are RO formulas.

(b) Formulas that are *read-once with powers* (ROP) are defined by adding the induction clause

(I2) If ϕ_1 is an ROP formula and a is an integer ≥ 2, then ϕ_1^a is an ROP formula.

(c) Formulas that are *read-once with constants* (ROC) are defined by adding instead the second basis clause

(B2) For every constant $c \in F$, c is an ROC formula.

(d) Formulas that are *read-once with powers and constants* (ROPC) are defined by adding both clauses (I2) and (B2).

(e) A formula ϕ (of any kind) has *no additive constants* (NAC) if every subtree of a $+$ or $-$ node in ϕ has at least one variable. (Except for the triviality of multiplying together or powering a bunch of constants, this is the same as saying that no constant is a child of a $+$ or $-$ sign in ϕ.)

We try to maintain the distinction between a polynomial and a given formula for it, blurring the usage only when doing so is innocuous, and call a polynomial function read-once (etc.) if it has *some* RO (etc.) formula, talking with respect to a given or arbitrary field. For example, $x * (y + z)$ is an RO-formula of size 3, while $x * y + x * z$ is a formula of size 4 for the same polynomial that is not RO. The polynomial $xy + 2xz$ has no RO formula (except over fields of characteristic 2 or 3), but it has the ROC formula $x * (y + 2 * z)$, and both formulas are NAC. The formula $(x + 3)^2$ is ROPC but not NAC.

A *term order* $\succ$ is a well-ordering of monomials with 1 as least element that respects multiplication: $m_1 \succ m_2 \Longrightarrow m_1m_3 \succ m_2m_3$ for all monomials m_1, m_2, m_3. The *terms* of a polynomial p are well-defined by the unique expression for p over the monomial vector-space basis of $F[x_1, \ldots, x_n]$, and the one whose corresponding monomial is greatest under $\succ$ is the *leading term* $LT(p :\succ)$. We write $LT(p)$ when $\succ$ is understood, and also write $p = \ell + p'$ with $\ell = LT(p)$. Then the *S-polynomial* of two polynomials p_1 and p_2 is defined by

$$S(p_1, p_2) = mp'_1/\ell_1 - mp'_2/\ell_2$$

where m is the least common multiple of the monomial parts of the leading terms ℓ_1 and ℓ_2. If we write $LM(p)$ for the leading monomial itself, then this is equivalent to

$$S(p_1, p_2) = \frac{lcm(LM(p_1), LM(p_2))}{LT(p_1)} p_1 - \frac{lcm(LM(p_1), LM(p_2))}{LT(p_2)} p_2.$$

Any set $B = \{ p_1, \ldots, p_s \}$ forms a *basis* for the ideal $I = \{ \sum_{i=1}^{s} \alpha_i p_i : \alpha_1, \ldots, \alpha_s \in F[x_1, \ldots, x_n] \}$. We also write $I = \langle p_1, \ldots, p_s \rangle$ to emphasize the ideal generated by the set. Every polynomial ideal $I \subseteq F[x_1, \ldots, x_n]$ has a finite basis. An expression $p = \sum_{i=1}^{s} \alpha_i p_i$ for a polynomial $p \in I$ over B is *acceptable* (given a term order $\succ$) if for each i, $LT(\alpha_i p_i) \preceq LT(p)$. Intuitively, this says that the representation of p involves no cancellations of terms higher than the leading term of p. One also writes $p \rightarrow_B 0$ and says that p *reduces to* 0 *via* B. The basis is a *Gröbner basis* (GB) with respect to $\succ$ if every $p \in I$ has an acceptable representation over the basis. We employ the following well-known equivalent conditions:

Proposition 2.1 ((see [CLO96])) *For any set $B = \{ p_1, \ldots, p_s \}$ of polynomials, the following are equivalent:*

(a) B forms a Gröbner basis for the ideal I generated by B.

(b) For all $p \in I$, there exists i such that $LT(p_i)$ divides $LT(p)$.

(c) For all i and j, $S(p_i, p_j)$ has an acceptable representation over B, i.e. $S(p_i, p_j) \rightarrow_B 0$.

The following sufficient condition is also well known.

Lemma 2.2 *A basis $B = \{ p_1, \ldots, p_s \}$ is a Gröbner basis if for all distinct i, j at least one of the following holds:*

(a) $LT(p_i)$ and $LT(p_j)$ have no variable in common, or

(b) For some k distinct from i and j, $LT(p_k)$ divides the least common multiple of $LT(p_i)$ and $LT(p_j)$, and both $S(p_i, p_k)$ and $S(p_k, p_j)$ have acceptable representations over B.

For every polynomial ideal I and fixed $\succ$, there is a unique Gröbner basis $G = \{ g_1, \ldots, g_s \}$ of minimum cardinality s whose members g_i are all *reduced modulo* $G \setminus \{ g_i \}$; we need not define "reduced" here and say this only to write $\mathrm{GB}_{I,\succ}$ for this G. Finally, a basis is a *universal Gröbner basis* if it is a Gröbner basis with respect to *all* term orders $\succ$. Any superset of a [universal] Gröbner basis is again a [universal] Gröbner basis. Every polynomial ideal has a finite universal GB, but there are cases where every universal GB is bigger than $\mathrm{GB}_{I,\succ}$ for every term order $\succ$. The k-th order partial derivatives of the determinant polynomials d_n form a GB under any "diagonal" orderings $\succ$, but generally do not form a universal GB, as they fail to be a GB with respect to certain non-diagonal orderings.

We have not found the last definition in this section in the literature.

Definition 2.2. A basis $B = \{ p_1, \ldots, p_s \}$ for an ideal I is a *Gröbner-bounding basis* (GBB) if for all members g_i of $\mathrm{GB}_{I,\succ}$ there exists j such that $LT(g_i)$ divides $LT(p_j)$. B is a *universal GBB* if it is a GBB for every $\succ$.

That is, a GBB bounds the degrees leading terms in the unique minimum Gröbner basis, and so is "good enough" as an upper bound on Gröbner basis complexity. Its leading terms need not generate the leading-term ideal of I, however, as with a GB. For a simple example, $\{ x^2, x^2 + x \}$ is a GBB for the ideal generated by x, but not a GB.

3 Main Results

Formal partial derivatives of polynomials p are defined as usual even over finite fields, and *Fubini's Theorem* that $\partial^2 p/\partial x\partial y = \partial^2 p/\partial y\partial x$ of course holds. Given $k \geq 1$ we write $Jac^k(p)$ for both the set of kth-order partial derivatives and for the ideal they generate. The case $k = 1$ is called the *Jacobian ideal*, and $k = 2$ is called the *Hessian ideal*.

Theorem 3.1 *For every RO formula ϕ and $k \geq 1$, $Jac^k(\phi)$ forms a universal Gröbner basis. The same is true of ROC formulas provided they have no additive constants.*

Theorem 3.2 *For every ROP formula ϕ, and indeed every ROPC formula with no additive constants, $Jac(\phi)$ forms a universal Gröbner basis.*

Theorem 3.3 *For every ROPC formula ϕ, $Jac(\phi)$ forms a universal Gröbner-bounding basis.*

To separate these three theorems, first consider $\phi_1 = x(yz+1)$. Then $Jac(\phi_1) = \langle yz+1, xz, xy \rangle$. This is not a Gröbner basis because x is in the ideal; indeed, $\langle x, yz + 1 \rangle$ is the unique minimum GB for $Jac(\phi)$ under any term order. It is, however, a Gröbner-bounding basis. Thus Theorem 3.1 does not extend to RO(P)C formulas.

Now consider $\phi_2 = (x^2 + y^2)^2$. This is an ROP formula. Its Jacobian is $\langle x^2y + y^3, x^3 + xy^2 \rangle$. This indeed forms a universal GB. Its Hessian, however, is $\langle 3x^2 + y^2, 2xy, x^2 + 3y^2 \rangle$. This is not even a GBB (under any term order), because both x^2 and y^2 belong to $Hess(\phi_2)$. The larger example $\phi_3 = ((x^2 + y^2)^2 + z^4)^2$ shows a case where not even the degrees of a Gröbner basis for the Hessian are bounded. The monomial z^7 belongs to $Hess(\phi_3)$ while z^6 does not; hence every Gröbner basis for $Hess(\phi_3)$ must have entries of degree at least 7, whereas all entries of $Hess(\phi_3)$ have degree 6. So $Hess(\phi_3)$ is not "Gröbner-bounding" in any sense. Note that these last two examples are for homogeneous formulas and ideals—we shall see later that the inhomogeneity of additive constants is responsible for the first example.

Finally, let us replace the additive constant in ϕ_1 by a variable, yielding the RO formula $\phi_4 = x(yz + w)$. Then $Jac(\phi_4) = \langle x, yz + w, xz, xy \rangle$. Although not a minimal Gröbner basis, this is certainly a (universal) Gröbner basis as it contains the minimum reduced GB $\langle x, yz + w \rangle$. What we draw attention to here is that the S-polynomial $S(\partial\phi_4/\partial x, \partial\phi_4/\partial y)$ does not reduce using $\partial\phi_4/\partial x$ and $\partial\phi_4/\partial y$ alone: $S(yz + w, xz) = wx$ and requires $\partial\phi_4/\partial w$ to be part of any acceptable representation. Put another way, the partials of ϕ_4 with respect to x and y do not form even a GBB by themselves. Hence Theorem 3.1 does not extend to any ideal formed by partial derivatives of read-once formulas, but "in general" requires having all the kth partials. The following technical property governs which partials are needed and plays a large role in the proofs.

Definition 3.1. Say a polynomial $p \in F[x_1, \ldots, x_n]$ is "J-nice" if there exist constants $a_1, \ldots, a_n \in F$ such that

$$p = \sum_{i=1}^{n} a_i x_i \frac{\partial p}{\partial x_i}.$$

That is, not only is $p \in \mathit{Jac}(p)$, but p has the particular acceptable representation shown. Note that if p is a nonzero constant, then p is not J-nice, and does not belong to $\mathit{Jac}(p)$ (which is the zero ideal) at all. A linear polynomial p with a nonzero constant term also fails to be J-nice, even though p *does* belong to $\mathit{Jac}(p)$ (which is the ideal 1).

Lemma 3.4 *(a) If p and q are J-nice with constants that agree on variables in $\mathit{Var}(p) \cap \mathit{Var}(q)$, then $p + q$ and $p * q$ are also J-nice.*

(b) Every homogeneous polynomial of degree $d > 0$ is J-nice.

(c) Every polynomial that has an ROPC formula with no additive constants is J-nice.

(d) If p is J-nice with $a_j \neq 1$, then $\partial p/\partial x_j$ is also J-nice.

(e) For every RO polynomial p and integer $k \geq 1$, such that all terms of p have degree at least k, p belongs to $\mathit{Jac}^k(p)$, with an acceptable representation over that basis.

Proof. For (a), without loss of generality, let $x_1, \ldots, x_\ell$ be the common variables and $x_{\ell+1}, \ldots, x_m$ the variables belonging only to p, with $0 \leq \ell \leq m \leq n$ ($\ell = 0$ means $\mathit{Var}(p) \cap \mathit{Var}(q) = \emptyset$). Then the constants can be notated as $(a_1, \ldots, a_m, 0, \ldots, 0)$ for p and $(a_1, \ldots, a_\ell, 0, \ldots, 0, a_{m+1}, \ldots, a_n)$ for q. Then $p + q = \sum_{i=1}^n a_i x_i (\partial(p + q)/\partial x_i)$ and $p * q = \sum_{i=1}^n (a_i/2) x_i (\partial(p + q)/\partial x_i)$.

Every monomial of degree d is J-nice with $a_i = 1/d$ for each i, and hence (b) follows from (a) for sums. For (c), first note that every power of a J-nice polynomial is also J-nice, as follows from (b) for products. This implies that an ROPC formula with no additive constants can be built up via binary sums and products of J-nice formulas with no common variables, and thus (c) follows. Part (d) follows by differentiating the formula $\sum_{i=1}^n a_i x_i (\partial p/\partial x_i)$ for p with respect to x_j and then solving for $\partial p/\partial x_j$.

Finally, (e) follows by induction on k because $\partial p/\partial x_i$ is always an RO formula, *unless* it is the constant 1 or -1. The condition on k prevents this from being an issue. □

To abstract things in a convenient way for the proofs, let δ stand for any composition of partial derivatives, and Δ for any set $\{ \delta_1, \ldots, \delta_m \}$ of such $\delta' s$. Then for any polynomial p, $\Delta(p)$ denotes the ideal generated by the m polynomials $\{ \delta_1(p), \ldots, \delta_m(p) \}$. Call Δ a "differential ideal operator." The Jacobian and Hessian ideals, and so on for higher k, are definable this way. The *sum* $I + J$ of two ideals I and J is generated by the union of any basis B_I for I and any basis B_J for J; we also write $I + J = \langle B_I, B_J \rangle$. Note that $\mathit{Jac}(p + q)$ is in general not the same as $\mathit{Jac}(p) + \mathit{Jac}(q)$, but the next lemma shows a relevant case where they co-incide.

Lemma 3.5 *For any polynomials p and q defined over disjoint variable sets, and any differential ideal operator Δ, $\Delta(p+q) = \langle \Delta(p), \Delta(q) \rangle$, and $\Delta(p*q) = \langle p*\Delta(q), q*\Delta(p) \rangle$.*

Proof. Let $\Delta = \{ \delta_1, \ldots, \delta_m \}$. All δ_i that differentiate with respect to some variable in $Var(p)$ and another in $Var(q)$ contribute a zero entry to both $\Delta(p+q)$ and $\Delta(p*q)$. Hence we need only consider δ_i that differentiate with respect to variables in $Var(p)$ only, and reason symmetrically for $Var(q)$. Since $\delta_i(p+q) = \delta_i(p)$ and $\delta_i(p*q) = q*\delta_i(p)$, the conclusions follow. ☐

Proof. (of Theorem 2.1). The proof proceeds by induction on both the formula size and the number of $+$ or $-$ signs in a given RO formula ϕ. Since no reference to any particular (kind of) term ordering will be needed, the conclusion will yield a universal GB.

The base case comprises all (RO, hence multilinear) monomials m. Since every $\delta_j(m)$ is a monomial, $\Delta(m)$ is a monomial basis. This automatically forms a universal Gröbner basis.

If ϕ is not a monomial, then there is a highest $+$ or $-$ sign in ϕ. At the end of the proof we will explain the generalization to formulas with multiplicative constants, which embraces formulas with $-$ signs. Hence we may take the highest non-$*$ operator to be a $+$ sign and parse ϕ as $(f+g)*h$. Here f and g are RO formulas on disjoint variable sets, and either h is likewise or $h = 1$. The fact that 1 (or any constant) is not to be considered an RO formula leads us to consider the case $h = 1$ separately.

We need to show that for all distinct i and j, $S(\delta_i, \delta_j)$ has an acceptable representation over the basis $\Delta(\phi)$.

Additive Case: $\phi = f + g$. Then $\Delta(\phi) = \langle \Delta(f), \Delta(g) \rangle$. Consider any two distinct nonzero entries $\delta_i = \delta_i(\phi)$ and $\delta_j = \delta_j(\phi)$. If both belong to $\Delta(f)$, then by the inductive hypothesis on f we have $S(\delta_i, \delta_j) \to 0$ via $\Delta(f)$, and hence via $\Delta(\phi)$. If $\delta_i(\phi)$ belongs to $\Delta(f)$ and $\delta_j(\phi)$ belongs to $\Delta(g)$, then by $Var(f) \cap Var(g) = \emptyset$ their leading terms are relatively prime (even allowing one of them to be constant), and hence condition (a) of Lemma 2.2 holds. The remaining cases follow symmetrically.

Multiplicative Case: $\phi = (f+g)*h$ with h also an RO formula (hence non-constant). Let δ_i and δ_j be two distinct non-zero entries of $\Delta(\phi)$. It is tempting to rewrite $\phi = fh + gh$ and "hand-wave" that the common multiple h does not affect the reasoning in the previous paragraph. However, this would overlook the actual breakdown of cases that need to be considered. (Also, the resulting "too-simple" proof would use Lemma 2.2(a) only, and this in turn would imply that $S(\delta_i, \delta_j)$ has an acceptable representation involving δ_i and δ_j only, which we have seen is false even in the case of Jacobians.) With two applications of Lemma 3.5 we obtain

$$\Delta(\phi) = \langle h*\Delta(f), h*\Delta(g), (f+g)*\Delta(h) \rangle. \tag{1}$$

If both δ_i and δ_j belong to one of $\Delta(f)$, $\Delta(g)$, or $\Delta(h)$, or if one belongs to $\Delta(f)$ and the other to $\Delta(g)$, then the reasoning of the additive case does carry over—mainly because $S(h*p, h*q) = h*S(p,q)$ for any polynomials h, p, q with $LT(h)$ relatively prime to $LT(p)$ and $LT(q)$. The tricky cases are δ_j belonging to $\Delta(h)$ and δ_i belonging to $\Delta(f)$ or $\Delta(g)$. These two cannot quite be collapsed into one "by symmetry," because for any particular term order $\succ$, we will need to worry about whether the leading term of $f+g$ belongs to f or to g. We may suppose that $\delta_i = h*\delta_i(f)$ and $\delta_j = (f+g)*\delta_j(h)$ and break the two cases according to whether (i) $LT(f) \succ LT(g)$ or (ii) $LT(g) \succ LT(f)$. (The leading terms cannot be equivalent since $Var(f) \cap Var(g) = \emptyset$.) With reference to (1), we index $\Delta(f)$ as $(\delta_{i_1}(f), \ldots, \delta_{i_r}(f))$, $\Delta(h)$ as $(\delta_{j_1}(h), \ldots, \delta_{j_s}(h))$, and $\Delta(g)$ as $(\delta_{k_1}(g), \ldots, \delta_{k_t}(g))$. By Lemma 3.5, these index sets are disjoint. (For the Jacobian, these index sets are the same as the indices of variables in $Var(f)$, $Var(h)$, and $Var(g)$, respectively. We associate "k" to g to preserve notation from the eventual application of condition (b) of Lemma 2.2.)

We also need to maintain in the induction the following invariant on formulas ϕ' whose highest operator is a $*$. This is related to Definition 3.1 and its generalizations, and works in concert with them.

Inductive Invariant. For formulas of the form $\phi' = f * h$, and all i and j, there is an acceptable representation

$$S(f\delta_j(h), \delta_i(f)h) = \alpha_1\delta_{i_1}(f)h + \cdots + \alpha_r\delta_{i_r}(f)h + \beta_1 f\delta_{j_1}(h) + \cdots + \beta_s f\delta_{j_s}(h),$$

and a polynomial m such that

$$\begin{aligned} \frac{lcm(LM(\delta_i(f)h), LM(f\delta_j(h)))}{LT(f\delta_j(h))}\delta_j(h) - \beta_1\delta_{j_1}(h) - \cdots - \beta_s\delta_{j_s}(h) &= mh \\ &\text{and} \\ \frac{lcm(LM(\delta_i(f)h), LM(f\delta_j(h)))}{LT(\delta_i(f)h)}\delta_i(f) + \alpha_1\delta_{i_1}(f) + \cdots + \alpha_r\delta_{i_r}(f) &= mf. \end{aligned}$$

The base case for this is when f and h are monomials, and then it holds trivially with $m = 0$. To maintain this invariant, we need to show that this property holds for ϕ parsed as $(f+g)*h$, given that it holds for $\phi' = f * h$ and $\phi'' = g * h$.

Subcase (i): $LM(f) \succ LM(g)$.

Simplifying the S-polynomial we have that

$$\begin{aligned} &S((f+g)\delta_j(h), \delta_i(f)h) = \\ &\quad \frac{lcm(LM((f+g)\delta_j(h)), LM(\delta_i(f)h))}{LT((f+g)\delta_j(h))}(f+g)\delta_j(h) - \frac{lcm(LM((f+g)\delta_j(h)), LM(\delta_i(f)h))}{LT(\delta_i(f)h)}\delta_i(f)h \\ &= \frac{lcm(LM(f\delta_j(h)), LM(\delta_i(f)h))}{LT(f\delta_j(h))}(f+g)\delta_j(h) - \frac{lcm(LM(f\delta_j(h)), LM(\delta_i(f)h))}{LT(\delta_i(f)h)}\delta_i(f)h, \end{aligned}$$

since $LM((f+g)\delta_j(h)) = LM(f\delta_j(h))$. Similarly,

$$\begin{aligned} &S((f+g)\delta_j(h), \delta_i(f)h) = \\ &\quad \frac{lcm(LM(f\delta_j(h)), LM(\delta_i(f)h))}{LT(f\delta_j(h))}f\delta_j(h) - \frac{lcm(LM(f\delta_j(h)), LM(\delta_i(f)h))}{LT(\delta_i(f)h)}\delta_i(f)h \\ &+ \frac{lcm(LM(\delta_i(f)h), LM(f\delta_j(h)))}{LT(f\delta_j(h))}g\delta_j(h). \end{aligned}$$

Since $S(f\delta_j(h), \delta_i(f)h) \rightarrow_{\Delta(fh)} 0$ by inductive hypothesis, we have
$S(f\delta_j(h), \delta_i(f)h) =$

$$\begin{aligned} &\frac{lcm(LM(f\delta_j(h)), LM(\delta_i(f)h))}{LT(f\delta_j(h))}f\delta_j(h) - \frac{lcm(LM(f\delta_j(h)), LM(\delta_i(f)h))}{LT(\delta_i(f)h)}\delta_i(f)h \\ = \; &\alpha_1\delta_{i_1}(f)h + \cdots + \alpha_r\delta_{i_r}(f)h + \beta_1 f\delta_{j_1}(h) + \cdots + \beta_s f\delta_{j_s}(h). \end{aligned}$$

Now we claim that by using the coefficients β_r for the basis entries of the form $(f+g)\delta j_r(h)$, we obtain an acceptable representation of $S(\delta_i(f)h, (f+g)\delta_j(h))$. We have from the above that $S(\delta_i(f)h, f\delta_j(h)) =$

$$\begin{aligned} &\alpha_1\delta_{i_1}(f)h + \cdots + \alpha_r\delta_{i_r}(f)h + \beta_1(f+g)\delta_{j_1}(h) + \cdots + \beta_l(f+g)\delta_{j_s}(h) \\ - \; &\beta_1 g\delta_{j_1}(h) - \cdots - \beta_s g\delta_{j_s}(h), \quad \text{and} \end{aligned}$$

$S(\delta_i(f)h, (f+g)\delta_j(h)) =$

$$\begin{aligned} & \alpha_1\delta_{i_1}(f)h + \cdots + \alpha_r\delta_{i_r}(f)h + \beta_1(f+g)\delta_{j_1}(h) + \cdots + \beta_l(f+g)\delta_{j_s}(h) \\ - \quad & \beta_1 g\delta_{j_1}(h) - \cdots - \beta_l g\delta_{j_s}(h) + \frac{lcm(LM(\delta_i(f)h), LM(f\delta_j(h)))}{LT(f\delta_j(h))} g\delta_j(h). \end{aligned}$$

We show that the last part

$$-(\beta_1 g\delta_{j_1}(h) + \cdots + \beta_l g\delta_{j_s}(h)) + \frac{lcm(LM(\delta_i(f)h), LM(f\delta_j(h)))}{LT(f\delta_j(h))} g\delta_j(h)$$

belongs to $\langle \delta_{k_1}(g)h, \cdots, \delta_{k_t}(g)h\rangle$. The conclusion will then follow from the fact that $\{\, \delta_{k_1}(g)h, \cdots, \delta_{k_t}(g)h \,\}$ itself is a Gröbner basis (by inductive hypothesis).

By the invariant maintained for the product case, applied to $S(\delta_i(f)h, f\delta_j(h))$,

$$\frac{lcm(LM(\delta_i(f)h), LM(f\delta_j(h)))}{LT(f\delta_j(h))}\delta_j(h) - \beta_1\delta_{j_1}(h) - \cdots - \beta_s\delta j_s(h) = mh$$

and

$$\frac{lcm(LM(\delta_i(f)h), LM(f\delta_j(h)))}{LT(\delta_i(f)h)}\delta_i(f) + \alpha_1\delta_{i_1}(f) + \cdots + \alpha_r\delta_{i_r}(f) = mf.$$

Hence

$$\frac{lcm(LM(\delta_i(f)h), LM(f\delta_j(h)))}{LT(f\delta_j(h))} g\delta_j(h) - (\beta_1 g\delta j_1(h) + \cdots + \beta_s g\delta_{j_s}(h)) = mgh.$$

By Lemma 3.4 we know that $g \in \Delta(g)$ so $mgh \in \Delta(g)\cdot\langle h\rangle = \langle \delta_{k_1}(g)h, \ldots, \delta_{k_t}(g)h\rangle$, where s (as above) is the number of nonzero entries in $\Delta(g)$. So the above polynomial has an acceptable representation as $mh(\gamma_1\delta_{k_1}(g) + \cdots \gamma_t\delta_{k_t}(g))$. Thus we have an acceptable representation for $S((f+g)\delta_j(h), \delta_i(f)h)$ as

$$\begin{aligned} S(\delta_i(f)h, (f+g)\delta_j(h)) &= \alpha_1\delta i_1(f)h + \cdots + \alpha_r\delta_{i_r}(f)h + \beta_1(f+g)\delta_{j_1}(h) + \cdots + \beta_s(f+g)\delta_{j_s}(h) \\ &\quad + m\gamma_1\delta_{k_1}(g)h + \cdots + m\gamma_t\delta_{k_t}(g)h. \end{aligned}$$

Thus $\Delta((f+g)h)$ is a Gröbner basis.

Now we have

$$\alpha_1\delta_{i_1}(f) + \cdots + \alpha_r\delta_{i_r}(f) + \frac{lcm(LM(\delta_i(f)h), LM(f\delta_j(h)))}{LT(\delta_i(f)h)}\delta_i(f) = mf$$

and

$$m(\gamma_1\delta_{k_1}(g) + \cdots \gamma_t\delta_{k_t}(g)) = mg,$$

so

$$\frac{lcm(LM(\delta_i(f)h), LM(f\delta_j(h)))}{LT(\delta_i(f)h)}\delta_i(f) + \alpha_1\delta_{i_1}(f) + \cdots + \alpha_r\delta_{i_r}(f) + m(\gamma_1\delta_{k_1}(g) + \cdots \gamma_t\delta_{k_t}(g)) = m(f+g).$$

Since we already had

$$\frac{lcm(LM(\delta_i(f)h), LM(f\delta_j(h)))}{LT(f\delta_j(h))}\delta_j(h) - (\beta_1\delta_{j_1}(h) + \cdots + \beta_s\delta_{j_s}(h)) = mh,$$

our invariant holds inductively for the S-polynomial of $(f+g)h$, namely for $S((f+g)\delta_j(h), \delta_i(f)h)$.

Subcase (ii): $LM(f) \succ LM(g)$.

Here

$$lcm(LM(\delta_i(f)h), LM((f+g)\delta_j(h))) = LM(\delta_i(f))LM(g)lcm(h, \delta_j(h)),$$

as the variable sets are disjoint.

Now we have that there exists $k \in \{k_1, \ldots, k_t\}$ such that $LM(\delta_k(g)) \setminus LM(g)$, since we can consider the partial derivatives with respect to any of the variables occurring in $LM(g)$. Clearly $LM(\delta_k(g)h) \setminus LM(\delta_i(f))LM(g)lcm(h, \delta_j(h))$.

Also $S(\delta_i(f)h, h\delta_k(g)) \rightarrow_{\Delta(fgh)} 0$ using induction hypothesis on the ideal $\Delta(fgh)$ (obtained by fewer addition operations with the same formula size), the same entries are also present in $\Delta((f+g)h)$ so

$$S(\delta_i(f)h, h\delta_k(g)) \rightarrow_{\Delta((f+g)h)} 0.$$

Using the induction hypothesis on a subcase we have already handled, $S(h\delta_k(g), (f+g)\delta_j(h)) \rightarrow_{\Delta((f+g)h)} 0$. Now using the analysis in Lemma 2.2(b) we are done. This completes the proof of the multiplicative case.

To finish the proof of the theorem, we need only explain how the above calculations are (not) affected by the presence of multiplicative constants c in ϕ. Because $\delta_i(cf) = c\delta_i(f)$ for any δ and f, the only difference is that some entries in $\delta(\phi)$ are multiplied by products of these constants. The fact that ϕ is read-once ensures that the only constants in the entries are these products, and in particular that no cancellations occur. Thus $\delta(\phi)$ is an equivalent basis for the ideal $\delta(\phi')$ where ϕ' is obtained from ϕ by setting all constants equal to 1. $\square$

Proof. of Theorem 2.1). We use the same reasoning as at the end of the last proof. The base case of monomials is unchanged. The additive case now becomes formulas $\phi = (f+g)^a$ where $a > 1$, while the multiplicative case becomes $\phi = (f+g)^a h$. In both cases, $Jac(\phi) = (f+g)^{a-1} * Jac(\phi')$, where ϕ' is obtained from ϕ by setting $a = 1$. The basis obtained for $Jac(\phi)$ is also the same as that obtained for $Jac(\phi')$, except that the entries for variables in $Var(f) \cup Var(g)$ are multiplied by a. This does not change any of the S-polynomials. $\square$

For higher derivatives, however, the analogous "multipliers" of entries are no longer constants, and the reasoning does not hold—nor does the statement, as we have seen.

Proof. of Theorem 3.3). Let ϕ stand for a formula that is read-once-in-powers with constants $c_1, \ldots, c_k$. We prove by induction on k that $Jac(\phi)$ is a GBB. If ϕ has no additive constants (or even if some c_j is a multiplicative constant) then by the analysis at the end of the proof of Theorem 3.1, the multiplicative constant does not affect the relevant division properties for the ideal $Jac(\phi)$. Hence we may let $c \in \{c_1, \ldots, c_k\}$ stand for an occurrence of an additive constant in ϕ. Then ϕ has a subterm $(\beta + c)$ with $Var(\beta) \neq \emptyset$. Define ψ to be the formula obtained by replacing c by a new variable y. By induction hypothesis (IH), $Jac(\psi)$ forms a GBB.

Let $p \in Jac(\phi)$, and let $\succ$ be any admissible ordering on monomials over $\{x_1, \ldots, x_n\}$. We need to find a polynomial $q \in Jac(\phi)$ such that $LT(q)$ divides both $LT(p)$ and $LT(\partial\phi/\partial x_i)$ for some i, $1 \leq i \leq n$. By $p \in Jac(\phi)$, we have a (not necessarily acceptable) representation

$$p = \sum_{i=1}^{n} \alpha_i \frac{\partial \phi}{\partial x_i}$$

with each $\alpha_i \in F[x_1, \ldots, x_n]$. Now define

$$p' = \sum_{i=1}^{n} \alpha_i \frac{\partial \psi}{\partial x_i}.$$

Then $p = p'[y \mapsto c]$. We extend $\succ$ to an admissible ordering $\succ'$ on monomials over $\{ x_1, \ldots, x_n \} \cup \{ y \}$ such that $\tau \succ y$ for every non-constant term τ over $\{ x_1, \ldots, x_n \}$. By IH there exists a polynomial $q' \in Jac(\psi)$ such that, taking leading terms with regard to $\succ'$, $LT(q')$ divides $LT(p')$ and: either $LT(q')$ divides $LT(\partial\psi/\partial x_i)$ for some i, $1 \leq i \leq n$, or $LT(q')$ divides $LT(\partial\psi/\partial y)$. Taking any representation

$$q' = \gamma_0 \frac{\partial \psi}{\partial y} + \sum_{i=1}^{n} \gamma_i \frac{\partial \psi}{\partial x_i}$$

with $\gamma_0, \ldots, \gamma_n \in F[x_1, \ldots, x_n, y]$, we define

$$q'' = \sum_{i=1}^{n} \gamma_i \frac{\partial \psi}{\partial x_i}$$

(i.e., $q'' = q' - \gamma_0 \partial\psi/\partial y$) and $q = q''[y \mapsto c]$. Then $q \in Jac(\phi)$, and we argue that q is the required polynomial. For this we make the following observations.

- For any variable x_i occurring in β, $\partial\psi/\partial y$ divides $\partial\psi/\partial x_i$. This relies on the fact that x_i occurs only inside β, and is the only place the read-once condition is used. Hence $LT(\partial\psi/\partial y)$ divides $LT(\partial\psi/\partial x_i)$. It follows that for some (possibly different) i, $LT(q')$ divides $LT(\partial\psi/\partial x_i)$, and also that $LT(q'') = LT(q')$.

- For any i, $LT(partial\psi/\partial x_i)$ does not involve y: Regardless of whether x_i is a variable in β or not, every occurrence of y in $partial\psi/\partial x_i$ occurs inside a subterm $(\beta + y)^a$ for some power $a \geq 1$. Since $Var(\beta) \neq \emptyset$, the leading term τ of β majorizes y under $\succ'$, and this carries through to $\partial\psi/\partial x_i$ itself.

- It also follows that $LT(p')$ does not involve y, since the α_i are y-free. Thus $LT(q')$, which equals $LT(q'')$, does not involve y.

From the last point, it follows that $LT(p' :\succ') = LT(p :\succ)$ and $LT(q'' :\succ') = LT(q :\succ)$, and so $LT(q)$ divides $LT(p)$. Finally, we have $LT(q'')$ dividing $LT(\partial\psi/\partial x_i)$ for some i from the first point. Let r abbreviate $\partial\psi/\partial x_i$. Then $\partial\phi/\partial x_i = r[y \mapsto c]$, and by the second point, we obtain $LT(\partial\phi/\partial x_i) = LT(r)$. Thus $LT(q)$ divides $LT(\partial\phi/\partial x_i)$. Since $\succ$ was arbitrary, this completes the demonstration that $Jac(\phi)$ is a universal Gröbner bounding basis. $\square$

4 Conclusions

Since multilinear read-twice formulas ϕ allow any ideal I to be an elimination ideal of $Jac(\phi)$, our results are best possible in terms of limited-read formulas. There remains scope for the following investigations:

1. What further geometric properties do the ideals $Jac(\phi)$ in this paper have?

2. What properties of arithmetical formulas and their derivatives keep the expansion in Gröbner basis complexity bounded, e.g. singly exponential?

Answers may aid the search for an invariant that has the same properties as Strassen's but extends to higher complexity levels, and thus can provide better lower bounds.

References

[BCS97] P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory.* Springer Verlag, 1997.

[BM93] D. Bayer and D. Mumford. What can be computed in algebraic geometry? In D. Eisenbud and L. Robbiano, editors, *Computational Algebraic Geometry and Commutative Algebra, Cortona, 1991*, pages 1–48. Cambriddge University Press, 1993.

[BS82] W. Baur and V. Strassen. The complexity of partial derivatives. *Theor. Comp. Sci.*, 22:317–330, 1982.

[BS88] D. Bayer and M. Stillman. On the complexity of copmputing syzygies. *Journal of Symbolic Computation*, 6:135–147, 1988.

[Cai90] J.-Y. Cai. A note on the determinant and permanent problem. *Inform. and Comp.*, 84:119–127, 1990.

[CGG90] L. Caniglia, J.A. Guccione, and J.J. Guccione. Ideals of generic minors. *Commutative Algebra*, 18:2633–2640, 1990.

[CLO96] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms, Second Edition.* Undergraduate Texts in Mathematics. Springer Verlag, 1996.

[GPS98] G.-M. Greuel, G. Pfister, and H. Schönemann. Singular version 1.2 User Manual . In *Reports On Computer Algebra*, volume 21. Centre for Computer Algebra, University of Kaiserslautern, June 1998. `http://www.mathematik.uni-kl.de/~zca/Singular`

[HT98] Le Tuan Hoa and Ngo Viet Trung. On the Castelnuovo-Mumford regularity and the arithmetic degree of monomial ideals. *Mathematische Zeitschrift*, 229:519–537, 1998.

[Huy86] D. Huynh. A superexponential lower bound for Gröbner bases and Church-Rosser commutative Thue systems. *Inform. and Control*, 68:196–206, 1986.

[LS98] R. Laubenbacher and I. Swanson. Permanental ideals, 1998. Submitted for publication.

[MM82] E. Mayr and A. Meyer. The complexity of the word problem for commutative semigroups and polynomial ideals. *Advenaces in Math.*, 46:305–329, 1982.

[MM84] H. Möller and F. Mora. Upper and lower bounds for the degree of Gröbner bases. In *Proceedings of EUROSAM'84*, volume 174 of *Lect. Notes in Comp. Sci.*, pages 172–183, 1984.

[RR97] A. Razborov and S. Rudich. Natural proofs. *J. Comp. Sys. Sci.*, 55:24–35, 1997.

[Stu90] B. Sturmfels. Gröbner bases and Stanley decompositions of determinantal rings. *Mathematische Zeitschrift*, 209:137–144, 1990.

[Val79] L. Valiant. The complexity of computing the permanent. *Theor. Comp. Sci.*, 8:189–201, 1979.

[Val82] L. Valiant. Reducibility by algebraic projections. *L'Enseignement mathématique*, 28:253–268, 1982.

[vzG87] J. von zur Gathen. Feasible arithmetic computations: Valiant's hypothesis. *Journal of Symbolic Computation*, 4:137–172, 1987.

[Yap91] C. Yap. A new lower bound construction for commutative Thue systems with applications. *Journal of Symbolic Computation*, 12:1–27, 1991.