On Arithmetical Formulas Whose Jacobians are Gröbner Bases

Denis X. Charles*
University at Buffalo

Kenneth W. Regan†
University at Buffalo

Abstract

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

1 Introduction

This paper stems from unsolved problems about the computational complexity of arithmetical functions. These problems resemble famous questions such as "Is P = NP?" and seem to be just as difficult to resolve. A prime example concerns the determinant and permanent functions of an $n \times n$ matrix, both of which are degree-n polynomials in n^2 variables. Whereas the determinant has a simple polynomial-time algorithm and is expressible by arithmetical formulas of nearly-polynomial size [Ber84], the permanent was shown to be NP-hard by Valiant [Val79], and hence is considered unlikely to have a polynomial-time algorithm. Indeed, the $n \times n$ permanents are commonly conjectured to require $2^{\Omega(n)}$ size not only for arithmetical formulas but also for arithmetical *circuits*. However, no lower bounds better than $\Omega(N \log N)$ are known on the size of formulas, let alone circuits, for any family (over N) of natural N-variable degree-$O(N)$ polynomials p_N such as the above (where $N = n^2$). A recent text reference for all of these assertions is [BCS97].

A reason voiced for this great gap in our knowledge of lower bounds is the difficulty of associating "classical" mathematical quantities with complexity measures such as arithmetical circuit or formula size, or the running time of a Turing Machine. The known $\Omega(N \log N)$ lower bounds arise from one such association proved by Baur and Strassen [BS82]: the arithmetical circuit size of p_N (over any infinite field k) is bounded below by the base-2 logarithm of the geometric degree of the mapping from k^N to k^N defined by the N first partial derivatives of p_N. However, the geometric degree of such a mapping never exceeds d^N, where $d+1$ is the degree of f_N, and the log of such a "singly exponential" quantity is not much above linear. Another association with a similar limitation is to the number of connected components of algebraic sets, obtained in [Ben83, BLY92, Yao94] via Milnor-Thom bounds. However, many double-exponential quantities are known in algebraic geometry and serve informally as "complexity measures" of associated polynomial ideals. Our interest thus lies in connecting the computational complexity of a polynomial function p with the mathematical complexity of some ideal I_p associated to p, such as the *Jacobian ideal* $Jac(p)$ formed by the first partial derivatives of p.

This paper asks: Which polynomial functions p have the *simplest* ideals $I_p = Jac(p)$? The determinant and permanent functions again supply motivation. For all n and k, and with respect

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

to any "diagonal" term-order, the kth partial derivatives of the determinant polynomials form a Gröbner basis [Stu90, CGG90]—and the resulting so-called *determinantal ideals* they generate have many nice geometric properties and are a major topic of study. For the permanent polynomials however, the corresponding "permanental ideals" lack similar properties [LS98], and computer runs for $n = 3, 4, 5$ suggest explosive growth in Gröbner basis size and degree. Which other classes of formulas have the same "Gröbner-minimum" property as the determinant polynomials?

We prove that for *read-once* (RO) formulas, namely those in which every literal is a different variable, the Jacobian forms a Gröbner basis under any term order. This was originally motivated by the fact that every formula ϕ is a multi-step "Valiant projection" (see [Val82, SV85, BCS97]) of the read-once formula ϕ' of the same size obtained by replacing every occurrence of a variable or constant in ϕ by a different new variable. A good bound on the increase in some polynomial-ideal complexity measure under a single-step Valiant projection (namely, identifying two variables or replacing a variable by a constant) may yield an association useful for computational-complexity lower bounds with the results in this paper (or extensions of them) as the base case. We show that $Jac(p)$ forms a Gröbner basis also when p has a formula that is RO with constants allowed in the formula and with powering of arbitrary subterms, such as $p = (x+3y-4)^2(6-z^3)$. Our results are best-possible in the sense that *every* polynomial ideal I is an elimination ideal of $Jac(h)$ for some multi-linear read-twice formula h of size linear in the sum of the formula sizes of given generators $p_1, \ldots, p_s$ for I.[1] Thus Jacobians of read-twice formulas essentially embody all complexity features of ideals, including those of the notorious "Mayr-Meyer ideals" [CLM76, MM82, MM84, Huy86, BS88, Yap91], which have $s = O(n)$ and $p_1, \ldots, p_s$ of constant degree and size.

Section 2 defines the classes of formulas and gives the facts about Gröbner bases needed for our proofs, which come in Sections 3–5. A concluding Section 6 re-visits the above motivations and gives some related mathematical problems.

2 Definitions and Main Results

We consider arithmetical formulas involving variables $x_1, x_2, \ldots$, arbitrary constants in the field F, and the operators $+$, $-$, and $\cdot$. 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 $\cdot$) 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, sometimes not counting operators one of whose arguments is a constant, 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, referencing its simulation by -1 and $\cdot, +$. 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.

[1] To wit, let $p'_1, \ldots, p'_s$ be defined by replacing each jth occurrence of a variable x_i in p_k by a new variable $y_{i_{jk}}$, treating constants similarly. Re-labeling these new variables as $y_1, \ldots, y_m$, let $z_1, \ldots, z_{s+m}$ be further new variables and define $h = z_1 p'_1 + \ldots z_s p'_s + z_{s+1}(x_1 - y_1) + \ldots + z_{s+m}(x_n - y_m)$.

(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 $\phi_1 \cdot \phi_2$ 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 $\geq$ 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, $x\cdot(y+z)$ is an RO-formula of size 3, while $x\cdot y + x\cdot z$ 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 $x\cdot(y + 2\cdot z)$, 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 $F[x_1, \ldots, x_n]$. The term whose corresponding monomial is greatest under $\succ$ is the *leading term* $LT(p, \succ)$, and the monomial itself is the *leading monomial* $LM(p, \succ)$. We write $LT(p)$ or $LM(p)$ when $\succ$ is understood. We also extend the notation $LM(p_1, p_2)$ to mean the least common multiple of $LM(p_1)$ and $LM(p_2)$. Then the *S-polynomial* of two polynomials p_1 and p_2 is defined by

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

Note that $LM(S(p_1, p_2)) \prec LM(p_1, p_2)$ since the leading terms of the two fractions cancel.

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.

Definition 2.2. Let $B = \{ p_1, \ldots, p_s \}$ generate a polynomial ideal I, and let $\succ$ be a term order.

(a) Given a monomial m and a polynomial $q \in I$, an expression

$$q = \sum_{i=1}^{s} \alpha_i p_i$$

is an *m-representation* over B if for all i, $LT(\alpha_i p_i) \preceq m$.

(b) The representation is *good* (or *standard*) if $m \preceq LM(q)$.

(c) If q is an S-polynomial $S(p_1, p_2)$, the representation is *fair* if $m \prec LM(p_1, p_2,)$.

(d) B is a *Gröbner basis* (GB) if every $q \in I$ has a good representation over B.

Intuitively, a Gröbner basis gives every $q \in I$ a representation that involves no cancellations of terms higher than the leading term of q. It is necessary and sufficient for this that for every $q \in I$ there exists a p_i in B such that $LM(p_i)$ divides $LT(q)$. The famous *Buchberger S-pair condition* for B to be a GB is usually stated (e.g. in Theorem 3 on p102 of [CLO92]) as every S-polynomial $S(p_i, p_j)$ having a good representation over B, but in fact it suffices for every $S(p_i, p_j)$ to have a fair representation, as shown by Theorem 5.64 in [BW93]. In this paper it is convenient to employ the following:

Lemma 2.1 ((see [BW93])) *A set $B = \{ p_1, \dots, p_s \}$ of polynomials forms a Gröbner basis if (and only if) for all distinct p_i, p_j in B at least one of the following holds*

(a) $S(p_i, p_j)$ has a fair representation over B.

(b) There is a polynomial h dividing p_i and p_j such that $LM(p_i/h)$ and $LM(p_j/h)$ are relatively prime.

(c) There exists a p_k in B such that $LM(p_k)$ divides $LM(p_i, p_j)$ and both $S(p_i, p_k)$ and $S(p_k, p_j)$ have fair representations over B.

Proof. Proposition 5.70 in [BW93] shows that for any $S(p_i, p_j)$ statement (c) implies (a). For (b) $\Longrightarrow$ (a) we can employ the same analysis as in the proof of Lemma 5.66 in [BW93], which is the case $h = 1$, since $S(p_i, p_j) = hS(p_i/h, p_j/h)$. □

For later remarks we note that in case (b) one in fact obtains a good representation over $\{ p_i, p_j \}$ alone, not needing other parts of B.

For every polynomial ideal I and fixed $\succ$, there is a unique Gröbner basis $G = \{ g_1, \dots, g_s \}$ such that no term t of a polynomial in G is a multiple of any $LT(g_i)$, other than $t = LT(g_i)$ itself, and the leading terms $LT(g_i)$ have coefficient 1 (i.e., are monomials). Then s is the minimum cardinality of any Gröbner basis for I, and we 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 2.3. A basis $B = \{ p_1, \dots, p_s \}$ 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.

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 $Jac(p + q)$ is in general not the same as $Jac(p) + Jac(q)$. Now we can state our main results.

Theorem 2.2 *For every RO formula ϕ, $Jac(\phi)$ forms a universal Gröbner basis.*

This basic result is extended in two different directions.

Theorem 2.3 *For every ROPC formula with no additive constants, $Jac(\phi)$ forms a universal Gröbner basis.*

Theorem 2.4 *For every ROPC formula ϕ, $Jac(\phi)$ forms a universal Gröbner-bounding basis.*

To separate these extensions, consider $\phi = x(yz + 1)$. Then $Jac(\phi) = \langle yz + 1, xz, xy\rangle$. 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 2.2 does not extend to ROC formulas.

3 Membership in Differential Ideals

We begin with the Jacobian ideal, and then generalize the idea for later reference in the Conclusions section.

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 $p \in Jac(p)$, but p has the particular good representation shown. Note that if p is a nonzero constant, then p is not J-nice, and does not belong to $Jac(p)$ (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 $Jac(p)$ (which is the ideal 1).

Lemma 3.1 *(a) If p and q are J-nice with constants that agree on variables in $Var(p) \cap Var(q)$, then $p + q$ and $p{\cdot}q$ 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 the ideal $Jac^k(p)$ generated by all the kth partial derivatives, with a good 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 $Var(p) \cap Var(q) = \emptyset$). 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 $p{\cdot}q = \sum_{i=1}^{n}(a_i/2)x_i(\partial(p + q)/\partial x_i)$.

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. □

The following abstraction provides both a stronger form of (e). 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.

Definition 3.2. Given a differential ideal operator $\Delta = \{\delta_1, \ldots, \delta_s\}$, a polynomial q is "Δ-nice" if there are non-negative rational constants $a_1, \ldots, a_s$ such that $p = \sum_{j=1}^{s} a_j m_j \delta_j(p)$, where for each j, m_j is the monomial corresponding to the partial derivatives taken in δ_j. (That is, if $\delta_j = (\partial/\partial x_i) \circ \delta'_j$, then $m_j = x_i m'_j$, based on $m'_j = 1$ if δ'_j is the identity.)

4 A Decoupling Invariant

The final ingredient of our proofs is the following property of ideals of the form $qJac(p) + pJac(q)$. If we write p_i as short for $\partial p/\partial x_i$, then this equals $\langle qp_i, pq_i : 1 \leq i \leq n \rangle$. In general this is not the same as $Jac(pq)$, but it equals $Jac(pq)$ *if* $Var(p) \cap Var(q) = \emptyset$.

Definition 4.1. An S-polynomial $S(qp_i, pq_j)$ *decouples* if it has a fair representation over $qJac(p) + pJac(q)$ of the form $S(qp_i, pq_j) = \sum_{k=1}^{n} \alpha_k qp_k + \beta_k pq_k$ such that for some monomial m,

$$\frac{LM(qp_i, pq_j)}{LT(qp_i)} p_i - \sum_k \alpha_k p_k \quad = \quad mp, \tag{1}$$

$$\frac{LM(qp_i, pq_j)}{LT(pq_j)} q_j + \sum_k \beta_k q_k \quad = \quad mq \tag{2}$$

We note that (2) actually follows from (1), because on multiplying the latter by p and the former by q, the left-hand sides are equal. Intuitively this says that half of the fair representation of the S-polynomial leads to a representation of a multiple of p, and the other half to q, "decoupling" into p and q in this sense.

Lemma 4.1 *Suppose there exist i and j such that $LM(p_i)$ divides $LM(p)$, $LM(q_j)$ divides $LM(q)$, $Jac(p)$ and $Jac(q)$ are Gröbner bases, and $S(qp_i, pq_j)$ decouples over $pJac(q) + qJac(p)$. Then all S-polynomials decouple over $pJac(q) + qJac(p)$.*

Proof. Take any a, d, $1 \leq a \leq b$, and note the identity

$$S(qp_{i'}, pq_{j'}) = \frac{LM(qp_a, pq_d)}{LM(qp_a, qp_i)} S(qp_a, qp_i) + \frac{LM(qp_a, pq_d)}{LM(qp_i, pq_j)} S(qp_i, pq_j) + \frac{LM(qp_a, pq_d)}{LM(qp_a, pq_d)} S(pq_j, pq_d).$$

In all three monomial fractions, the denominator divides the numerator owing to the hypotheses on i and j. Noting that $S(qp_a, qp_i) = qS(p_a, p_i)$ and similarly for $S(pq_j, pq_d)$, we may obtain from

$Jac(p)$ and $Jac(q)$ being GBs the following fair representations of these S-polynomials:

$$
\begin{aligned}
S(qp_a, qp_i) &= \sum_{k=1}^{n} q\gamma_k p_k, \\
S(pq_j, pq_d) &= \sum_{\ell=1}^{n} p\delta_\ell q_\ell.
\end{aligned}
$$

Take the decoupling representation with monomial m for $S(qp_i, pq_j)$ as in Definition 4.1. Substituting yields a representation of $S(qp_{i'}, pq_{j'})$ that is fair, again owing to divisibility in the three fractions. To show that it decouples, we can group the α_k and γ_k, and need only show that for some monomial m',

$$
m'p = \frac{LM(qp_a, pq_d)}{LT(qp_a)} p_a - \sum_k \frac{LM(qp_a, pq_d)}{LM(qp_a, qp_i)} \gamma_k p_k - \sum_k \frac{LM(qp_a, pq_d)}{LM(qp_i, pq_j)} \alpha_k p_k
$$

By decoupling for $S(qp_i, pq_j)$, we have

$$
\frac{LM(qp_i, pq_j)}{LT(qp_i)} p_i - \sum_k \alpha_k p_k = mp.
$$

This follows with $m' = LM(qp_a, pq_j)/LM(qp_a, qp_i)$. $\square$

It follows also that $pJac(q) + qJac(p)$ is a Gröbner basis. To apply this result to read-once formulas, we observe:

Lemma 4.2 *For every RO formula ϕ and term order $\succ$, there exists a variable x_i such that $LM(\partial\phi/\partial x_i)$ divides $LM(\phi)$.*

Proof. The base case of ϕ a monomial is clear, as any variable can be chosen. If $\phi = f + g$, then if $LM(\phi)$ belongs to $Var(f)$ choose the "good" variable that exists by induction in f, else choose the one in g. If $\phi = f \cdot g$, then one may choose *either* a "good" variable in f or a good variable in g. $\square$

5 Proofs of the main results

Proof of Theorem 2.2. 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 property of a given term ordering $\succ$ will be needed, the conclusion will yield a universal GB.

Basis: Here ϕ is a monomial, and since all entries of $Jac(p)$ are monomials, the conclusion is clear.

Induction: 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-$\cdot$ operator to be a $+$ sign and parse ϕ as $(f + g)\cdot h$. 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, one of Lemma 2.1(a,b,c) holds for $S(\phi_i, \phi_j)$.

Additive Case: $\phi = f + g$. Then $Jac(\phi) = \langle Jac(f), Jac(g)\rangle$. Consider any two distinct entries ϕ_i and ϕ_j. If both belong to $Jac(f)$, then by the inductive hypothesis on f, $S(\phi_i, \phi_j) \to 0$ has a fair representation over $Jac(f)$, and hence over $Jac(\phi)$. If ϕ_i belongs to $Jac(f)$ and ϕ_j belongs to $Jac(g)$, then by $Var(f) \cap Var(g) = \emptyset$ their leading terms are relatively prime, and hence condition (b) of Lemma 2.1 holds. The other possibilities are handled similarly.

Multiplicative Case: $\phi = (f + g)\cdot h$ with h also an RO formula (hence non-constant). 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.[2] In

$$Jac(\phi) = \langle h\cdot Jac(f), h\cdot Jac(g), (f + g)\cdot Jac(h)\rangle, \tag{3}$$

if both ϕ_i and ϕ_j belong to one of $hJac(f)$, $hJac(g)$, or $(f + g)Jac(h)$, or if one belongs to $hJac(f)$ and the other to $hJac(g)$, then the reasoning of the additive case does carry over, using Lemma 2.1(b) with this h. The tricky cases are ϕ_j belonging to $(f+g)Jac(h)$ and ϕ_i belonging to $hJac(f)$ or to $hJac(g)$. These two cases cannot immediately 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. By symmetry the cases can be re-labeled (i) $LM(f) \succ LM(g)$ and (ii) $LM(g) \succ LM(f)$.

The idea in case (i) is to find a fair representation of $S(hf_i, (f+g)h_j)$ by induction on $Jac(fh)$ for the corresponding S-polynomial $S(hf_i, fh_j)$. In case (ii) this same analysis via induction on $Jac(gh)$ yields a fair representation of $S(hg_k, (f+g)h_j)$ where $x_k \in Var(g)$, and the idea is to apply Lemma 2.1(c) to obtain a fair representation for $S(hf_i, (f+g)h_j)$ in terms of that and $S(hf_i, hg_k)$.

However, we find that most of this work has already been done for us in Lemma 4.1. Hence we strengthen the induction in the product case by showing that the decoupling invariant (4.1) extends from all S-polynomials in $Jac(fh)$ and $Jac(gh)$ to those in $Jac((f + g)h)$. As remarked there, this implies that $Jac((f + g)h)$ is a Gröbner basis. The basis of the induction is when ϕ is a monomial.

For the induction step, by Lemma 4.1, it suffices to choose one variable $x_\ell \in Var(f) \cup Var(g)$ such that $\partial(f+g)/\partial x_\ell$ divides $LM(f+g)$, together with some $x_{j'}$ such that $\partial h/\partial x_{j'}$ divides $LM(h)$. In point of fact we can work by induction with the given j in place of j'. *Now* we obtain the final symmetry: in case (i) we choose $x_\ell \in Var(f)$ such that $LM(\partial f/\partial x_\ell)$ divides $LM(f)$, while in case (ii) we similarly choose $x_\ell \in Var(g)$ instead.

Thus the two cases do fold into one. We may suppose that $LM(f+g) = LM(f)$, choose x_i such that $LM(\partial f/\partial x_i)$ divides $LM(f)$, and finish the proof by showing merely that $S(hf_i, (f + g)h_j)$ decouples over $Jac(\phi)$. We can do this using the induction hypothesis that $S(hf_i, fh_j)$ decouples over $Jac(fh)$.

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 $\delta(cf) = c\delta(f)$ for any f and chain δ of partial derivatives, the only difference is that some entries in $Jac(\phi)$ 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. □

[2] Also, the resulting "too-simple" proof would use Lemma 2.1(b) 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.

The proof of the second main result now follows quickly.

Proof of Theorem 2.3. 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, $Jac(\phi) = (f+g)^{a-1} \cdot Jac(\phi')$, 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—we will note in the Conclusions that the ROP case actually fails.

Proof. of Theorem 2.4. 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. $\square$

6 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. For which formulas ϕ do the higher-derivative ideals $Jac^k(\phi)$ $(k \geq 2)$ form Gröbner bases?

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

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

We suspect that our theorems extend to higher-derivative ideals for RO formulas—and for ROC formulas without additive constants—but have not been able to prove this. To see that our other theorems do *not* extend to higher derivatives, consider $\phi = (x^2 + y^2)^2$. 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 $\phi' = ((x^2+y^2)^2 + z^4)^2$ shows a case where not even the degrees of a Gröbner basis for the Hessian are bounded. The monomial z^7 belongs to $Hess(\phi')$ while z^6 does not; hence every Gröbner basis for $Hess(\phi')$ must have entries of degree at least 7, whereas all entries of $Hess(\phi')$ have degree 6. So $Hess(\phi')$ 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, as indication that the proof will not be trivial even for RO formulas, consider $\phi'' = x(yz + w)$. Then $Jac(\phi'') = \langle x, yz + w, xz, xy \rangle$. Although not a minimal Gröbner basis, this is a universal Gröbner basis because its subset $\{ x, yz + w \}$ is the minimum reduced GB under any term order. What we draw attention to here is that with regard to any term order $\succ$ making $yz \succ w$, the S-polynomial $S(\partial\phi''/\partial x, \partial\phi''/\partial y)$ does not reduce using $\partial\phi''/\partial x$ and $\partial\phi''/\partial y$ alone: $S(yz + w, xz) = wx$ and requires $\partial\phi''/\partial w$ to be part of any good representation. Put another way, the partials of ϕ'' with respect to x and y do not form even a GBB by themselves, under $\succ$. Hence Theorem 2.2 seems not extend to many ideals formed by "differential ideal operators Δ," even applied to a read-once formula, but "in general" would seem to require having *all* the kth partials.

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

References

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

[Ben83] M. Ben-Or. Lower bounds for algebraic computation trees. In *Proc. 15th Annual ACM Symposium on the Theory of Computing*, pages 80–86, 1983.

[Ber84] S. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Inf. Proc. Lett.*, 18:147–150, 1984.

[BLY92] A. Björner, L. Lovász, and A. Yao. Linear decision trees: volume estimates and topological bounds. In *Proc. 24th Annual ACM Symposium on the Theory of Computing*, pages 170–177, 1992.

[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.

[BW93] T. Becker and V. Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra*, volume 141 of *Graduate Texts in Mathematics*. Springer Verlag, 1993.

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

[CLM76] E. Cardoza, R. Lipton, and A. Meyer. Exponential space complete problems for Petri nets and commutative semigroups. In *Proc. 8th Annual ACM Symposium on the Theory of Computing*, pages 50–54, 1976.

[CLO92] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Springer Verlag, 1992.

[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.

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

[SV85] S. Skyum and L. Valiant. A complexity theory based on Boolean algebra. *J. Assn. Comp. Mach.*, 32:484–502, 1985.

[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.

[Yao94] A. Yao. Decision tree complexity and Betti numbers. In *Proc. 26th Annual ACM Symposium on the Theory of Computing*, pages 615–624, 1994.

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