Canad. J. Math. Vol. **61** (4), 2009 pp. 930–949

Prolongations and Computational Algebra

Jessica Sidman and Seth Sullivant

Abstract. We explore the geometric notion of prolongations in the setting of computational algebra, extending results of Landsberg and Manivel which relate prolongations to equations for secant varieties. We also develop methods for computing prolongations that are combinatorial in nature. As an application, we use prolongations to derive a new family of secant equations for the binary symmetric model in phylogenetics.

1 Introduction

The notion of *prolongation* originated with Cartan in the context of differential geometry [4, 10, 12]. We give the simplest formulation of the definition below. Since we are using differential operators, we will assume that our ground field $\mathbb{K}$ has characteristic zero.

Definition 1.1 Let $S = \mathbb{K}[x_1, \ldots, x_n]$, and let $A \subseteq S_d$ be a vector space of polynomial forms of degree d. The r-th *prolongation* of A, denoted by $A^{(r)}$, is

$$\left\{ f \in S_{d+r} \;\middle|\; \frac{\partial^r f}{\partial \mathbf{x}^{\boldsymbol{\beta}}} \in A \text{ for all } \boldsymbol{\beta} \in \mathbb{N}^n \text{ with } |\boldsymbol{\beta}| = r \right\}.$$

In this paper our interest lies not in the role of prolongation in differential geometry, but instead in exploring the applications of purely algebraic reformulations of the definition to three areas: algebraic geometry, commutative algebra, and phylogenetics. In particular, we will explain and generalize results of Landsberg and Manivel [13] connecting prolongations and secant varieties, as well as apply these ideas to the computation of some nontrivial secant equations arising in phylogenetics.

Recall that if $X \subset \mathbb{P}^{n-1}$ is a projective variety, $\mathrm{Sec}^r(X) = X^{\{r\}}$ is the Zariski closure of the union of all $r-1$ planes spanned by r points in X. Let $I = I(X)$ and suppose that the smallest degree of a minimal generator of I is d. If $A = I_d$, the significance of the prolongation $A^{(r)}$ comes from connections to secant ideals of I.

Theorem 1.2 *Let $X \subseteq \mathbb{P}^{n-1}$ be a variety over an algebraically closed field of characteristic 0, with $I = I(X) \subseteq \langle x_1, \ldots, x_n \rangle^d$ and $A = I_d$. Then $A^{((d-1)(r-1))}$ is the degree $r(d-1)+1$ piece of the ideal of the secant variety $X^{\{r\}}$.*

Theorem 1.2 generalizes [13, Lemma 2.2] which concerned prolongations of spaces of quadratic forms. In a subsequent paper [14], Landsberg and Manivel allude to a generalization of their lemma for higher degrees, but never give a precise

Received by the editors November 21, 2006; revised April 3, 2007.
Sidman was partially supported by NSF grant DMS-0600471 and the Clare Boothe Luce Program.
AMS subject classification: Primary: 13P10; secondary: 14M99.

statement. At the heart of the proof of Theorem 1.2 are connections relating prolongations to polarizations of homogeneous forms and to symbolic powers of ideals. Relationships between symbolic powers and secant ideals are not new; for example, containment of secant ideals in symbolic powers appears explicitly in[6, Proposition 2.1] and [20, Corollary 4.8] shows that if X is smooth, a graded piece of a high enough symbolic power cuts out its secant line variety set-theoretically.

One reason that Theorem 1.2 is useful is that it allows for the straightforward computation of equations that belong to the secant ideals $I(X^{\{r\}})$ using linear algebra. Note that by [15], $r(d-1)+1$ is the lowest degree in which there can exist a nonzero polynomial in $I(X^{\{r\}})$. Even if I is generated by $A = I_d$, it need not be the case that $A^{((d-1)(r-1))}$ generates $I(X^{\{r\}})$. In spite of this, in several instances of practical interest, the prolongation provides many nontrivial equations in secant ideals that are difficult to derive directly from the definition of the secant variety. Thus, prolongation at least brings us one graded piece closer to understanding secant ideals.

We conclude the paper by returning to our original motivation, which was the relationship to algebraic statistics, where algebraic varieties are interpreted as statistical models. Passing to the secant variety in algebraic geometry amounts to taking a mixture model in statistics. We will use prolongations as a tool for describing nontrivial secant equations for the binary symmetric model in phylogenetics, which has received attention recently in the algebraic geometry community [5, 17].

This paper is organized as follows. We describe several equivalent definitions of prolongation in Section 2, ending with a proof of the relationship between prolongations and symbolic powers. In Section 3, we describe algorithms for computing prolongations. Theorem 1.2, which connects prolongations and secant equations, will follow from results in Section 4. Part of our proof follows along the lines of ideas from [13, 14], which we attempt to make more explicit, and part of the proof depends on a new application of the join of two ideals. We derive some nontrivial secant equations for the binary symmetric models in Section 5.

Notations and Conventions

Since we are working with differential operators, unless explicitly stated, we assume that $\mathbb{K}$ is a field of characteristic zero. In situations where we need $\mathbb{K}$ to be algebraically closed, we explicitly state this.

All varieties X are projective and reduced, but they need not be irreducible, that is, we assume that the ideal $I(X)$ is homogeneous and radical, but not necessarily prime.

Let $\mathbb{N}$ denote the non-negative integers. If $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, then $\boldsymbol{\alpha}! = \alpha_1! \cdots \alpha_n!$. If $|\boldsymbol{\alpha}| = d$, we let $\binom{d}{\boldsymbol{\alpha}}$ denote the multinomial coefficient with parts $\alpha_1, \ldots, \alpha_n$. We write $\mathbf{1}$ to denote a vector in which each coordinate is 1. A monomial in the polynomial ring $\mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}]$ is given by an element $\boldsymbol{\alpha} \in \mathbb{N}^n$ where $\mathbf{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

2 Prolongations: Equivalent Definitions

In this section we focus on making explicit the translations between purely algebraic descriptions of prolongation and Definition 1.1. The importance of the algebraic

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

definitions is that they allow us to connect the notion of prolongations to commutative algebra and algebraic geometry, specifically, to symbolic powers and equations defining secant varieties.

In the interest of keeping our introduction to prolongations self-contained, we briefly review the definition of the symmetric algebra in terms of the tensor algebra as well as the basics of polarization, although this material will be well known to some. We define prolongations from the quotient algebra point of view in Section 2.1. We translate the definition into the language of polarization in Section 2.2. Finally, we illustrate how thinking of prolongation in terms of polarization leads to connections with symbolic powers.

2.1 Prolongations and the Symmetric Algebra

In this section we will recast the definition of prolongation in terms of the symmetric algebra, viewed as a quotient of the tensor algebra.

Let V be a finite dimensional vector space over a field $\mathbb{K}$, and let V^* denote its dual. We follow the conventions of [9, Appendix B]. The reader may also want to consult [8, Appendix A2] or [21, Chapter 1].

We let $T = \bigoplus_{d\geq 0} T^dV^*$ be the tensor algebra of V^*, where T^dV^* denotes the tensor product of V^* with itself d times. The symmetric algebra S, on V^* is defined to be the quotient of T by the ideal $\langle x\otimes y - y\otimes x \mid x, y \in V^*\rangle$. If we pick a basis $\mathbf{x} = (x_1, \ldots, x_n)$, for V^*, then we may identify S with $\mathbb{K}[x_1, \ldots, x_n]$, the homogeneous coordinate ring of $\mathbb{P}V$. A monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ of degree d represents the equivalence class of tensors which map to it under the canonical projection $T \to S$.

The *co-multiplication* or *diagonal* map $S^{d+r}V^* \to S^dV^* \otimes S^rV^*$ will be important in what follows. First, we describe it using the intrinsic point of view of [8, Appendix A2.4]. Recall that the diagonal map $\Delta\colon S \to S\otimes S$ sends $x \in V^* \mapsto x\otimes 1+1\otimes x$. We get a map $\Delta_{d,r}\colon S^{d+r}V^* \to S^dV^*\otimes S^rV^*$ by restricting the diagonal map to $S^{d+r}V^*$ and composing this with the projection to $S^dV^* \otimes S^rV^*$. For example, since

$$\begin{aligned}\Delta(x^2y) &= (x\otimes 1 + 1\otimes x)^2(y\otimes 1 + 1\otimes y)\\ &= x^2y\otimes 1 + 2xy\otimes x + y\otimes x^2 + x^2\otimes y + 2x\otimes xy + 1\otimes x^2y,\end{aligned}$$

we see that the co-multiplication map $\Delta_{2,1}$ sends x^2y to

$$2xy\otimes x + x^2\otimes y \in S^2V^*\otimes S^1V^*.$$

Following [21, p. 5] we can also describe the co-multiplication map by its action on monomials in terms of our basis $\mathbf{x}$. If $i_1 \leq \cdots \leq i_{d+r}$, then

$$x_{i_1}\cdots x_{i_{d+r}} \mapsto \sum x_{i_{\sigma(1)}}\cdots x_{i_{\sigma(d)}} \otimes x_{i_{\sigma(d+1)}}\cdots x_{i_{\sigma(d+r)}},$$

where we sum over all permutations σ of $d+r$ elements such that $\sigma(1) < \cdots < \sigma(d)$ and $\sigma(d+1) < \cdots < \sigma(d+r)$.

The reason that co-multiplication appears in connection with prolongation is that it is closely related to partial differentiation.

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

Lemma 2.1 *If $F \in S^{d+r}V^*$, then $\Delta_{d,r}(F) = \sum_{|\boldsymbol{\beta}|=r} \frac{1}{\boldsymbol{\beta}!} \frac{\partial^r F}{\partial \mathbf{x}^{\boldsymbol{\beta}}} \otimes \mathbf{x}^{\boldsymbol{\beta}}$.*

Proof By linearity it suffices to assume that F is a monomial, $F = \mathbf{x}^{\boldsymbol{\alpha}}$. The projection of $\Delta(\mathbf{x}^{\boldsymbol{\alpha}})$ to $S^dV^* \otimes S^rV^*$ is the sum of all of the terms of $\Delta(\mathbf{x}^{\boldsymbol{\alpha}})$ that can be written in the form $- \otimes \mathbf{x}^{\boldsymbol{\beta}}$ with $|\boldsymbol{\beta}| = r$. Since

$$\Delta(\mathbf{x}^{\boldsymbol{\alpha}}) = \prod_{i=1}^{n} (x_i \otimes 1 + 1 \otimes x_i)^{\alpha_i},$$

there will be $\binom{\alpha_1}{\beta_1} \cdots \binom{\alpha_n}{\beta_n}$ terms in the product of the form $- \otimes \mathbf{x}^{\boldsymbol{\beta}}$, all equal to $\mathbf{x}^{\boldsymbol{\alpha}-\boldsymbol{\beta}} \otimes \mathbf{x}^{\boldsymbol{\beta}}$. But

$$\binom{\alpha_1}{\beta_1} \cdots \binom{\alpha_n}{\beta_n} \mathbf{x}^{\boldsymbol{\alpha}-\boldsymbol{\beta}} \otimes \mathbf{x}^{\boldsymbol{\beta}} = \frac{1}{\boldsymbol{\beta}!} \frac{\partial^r \mathbf{x}^{\boldsymbol{\alpha}}}{\partial \mathbf{x}^{\boldsymbol{\beta}}} \otimes \mathbf{x}^{\boldsymbol{\beta}}. \qquad \blacksquare$$

We can use co-multiplication to see that the algebraic definition of prolongation given in [13, §2.1.3] is equivalent to Definition 1.1.

Lemma 2.2 *If $A \subset S^dV^*$, then $A^{(r)} = (A \otimes S^rV^*) \cap S^{d+r}V^*$.*

Proof Note that $\Delta_{d,r}$ maps $F \in S^{d+r}V^*$ to an element of the form

$$\sum_{|\boldsymbol{\beta}|=r} F_{\boldsymbol{\beta}} \otimes \mathbf{x}^{\beta} \in S^dV^* \otimes S^rV^*.$$

This is in $A \otimes S^rV^*$ if and only if each $F_{\boldsymbol{\beta}} \in A$, and by the previous lemma,

$$F_{\boldsymbol{\beta}} = \frac{1}{\boldsymbol{\beta}!} \frac{\partial^r F}{\partial \mathbf{x}^{\boldsymbol{\beta}}}. \qquad \blacksquare$$

2.2 Prolongations and Polarization

In this section we explain the connection between prolongation and *polarization*. Polarization, which arose in classical invariant theory [22], is the higher degree analog of associating a symmetric bilinear form to a quadratic form and is closely related to the representation of a homogeneous form as an element of the tensor algebra. The notion of polarization is also used in connection with secant varieties of curves [2, Chapter VI, §1]. What is significant for us is that thinking of prolongation in terms of polarization opens the door to connections with symbolic powers and with secant varieties.

Definition 2.3 Suppose that F is a homogeneous polynomial of degree d in $\mathbb{K}[\mathbf{x}]$ where $\mathbf{x} = (x_1, \ldots, x_n)$. For each $i = 1, \ldots, d$ we introduce a new set of n variables $\mathbf{x}_i = (x_{i1}, \ldots, x_{in})$. We also introduce an auxiliary set of variables $\mathbf{t} = (t_1, \ldots, t_d)$. The *polarization* of F, denoted $\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_d)$, is the coefficient of $\mathbf{t}^{\mathbf{1}}$ in the expansion of $F(t_1\mathbf{x}_1 + \cdots + t_d\mathbf{x}_d)$ as a polynomial in $\mathbf{t}$.

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

Example 2.4 Let $F(\mathbf{x}) = x_1^2 x_2$. We compute

$$\begin{aligned} F(t_1\mathbf{x}_1 + t_2\mathbf{x}_2 + t_3\mathbf{x}_3) &= (t_1x_{11} + t_2x_{21} + t_3x_{31})^2(t_1x_{12} + t_2x_{22} + t_3x_{32}) \\ &= t_1^3x_{11}^2x_{12} + t_2^3x_{21}^2x_{22} + \cdots \\ &\quad \cdots + 3t_1^2t_2(x_{11}^2x_{22} + x_{11}x_{21}x_{12}) + \cdots \\ &\quad \cdots + t_1t_2t_3(2x_{11}x_{21}x_{32} + 2x_{11}x_{31}x_{22} + 2x_{21}x_{31}x_{12}). \end{aligned}$$

We see that $\mathbf{F}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) = 2x_{11}x_{21}x_{32} + 2x_{11}x_{31}x_{22} + 2x_{21}x_{31}x_{12}$.

Lemma 2.5 *If $F(\mathbf{x})$ is a homogeneous form of degree d, then*

(i)
$$F(t_1\mathbf{x}_1 + \cdots + t_d\mathbf{x}_d) = \sum_{|\boldsymbol{\beta}|=d} \frac{\mathbf{t}^{\boldsymbol{\beta}}}{\boldsymbol{\beta}!}\mathbf{F}(\mathbf{x}_1^{\beta_1}, \ldots, \mathbf{x}_d^{\beta_d})$$

where $\mathbf{x}_i^{\beta_i}$ means that the set of variables $\mathbf{x}_i$ is repeated β_i times.

(ii) $\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_d)$ *is linear in each set of variables* $\mathbf{x}_i$.

(iii) $\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_d)$ *is symmetric in the* $\mathbf{x}_i$. *(If σ is a permutation of d elements, then* $\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_d) = \mathbf{F}(\mathbf{x}_{\sigma(1)}, \ldots, \mathbf{x}_{\sigma(d)})$.*)*

(iv) $\mathbf{F}(\mathbf{x}, \ldots, \mathbf{x}) = d!F(\mathbf{x})$.

Proof Note that it is enough to prove the stated claims in the case where $F(\mathbf{x}) = \mathbf{x}^{\boldsymbol{\alpha}}$. In this case

$$F(t_1\mathbf{x}_1 + \cdots + t_d\mathbf{x}_d) = \prod_{j=1}^{n} (t_1x_{1j} + \cdots + t_dx_{dj})^{\alpha_j}. \tag{2.1}$$

For part (i), recall that $\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_d)$ is the coefficient of $\mathbf{t}^{\mathbf{1}}$ in the product consisting of d factors of the form $(t_1x_{1j} + \cdots + t_dx_{dj})$ as above. From this definition, we see that the coefficient of $\mathbf{t}^{\mathbf{1}}$ is a sum of $d!$ monomials (counted with multiplicity) which correspond to the $d!$ ways of choosing one term per factor, where each t_j is chosen exactly once.

We can construct the $d!$ monomials which are coefficients of $\mathbf{t}^{\mathbf{1}}$ as follows. Let the d factors in (2.1) be $F_1, \ldots, F_d$. Fix a subset $I \subset [d]$ of size β. A monomial coefficient of $\mathbf{t}^{\mathbf{1}}$ is obtained by choosing β terms of the form t_kx_{kj} from among the factors F_s with $s \in I$ where $k \in I$ and the k are all distinct, and $d - \beta$ terms $t_\ell x_{\ell j}$ from among the factors F_t with $t \notin I$ where $\ell \notin I$ and the ℓ are all distinct. Since there are $\binom{d}{\beta}$ ways to choose the set I, $\beta!$ ways to make our construction of a monomial from the factors F_s with $s \in I$ and $(d - \beta)!$ ways to construct a monomial from the factors F_t with $t \notin I$, we see that we get each monomial coefficient of $\mathbf{t}^{\mathbf{1}}$ in this way.

Let us consider $\mathbf{F}(\mathbf{x}_1^{\beta_1}, \ldots, \mathbf{x}_d^{\beta_d})$ where $\mathbf{x}_i$ is repeated β_i times. We can pass from $\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_d)$ to $\mathbf{F}(\mathbf{x}_1^{\beta_1}, \ldots, \mathbf{x}_d^{\beta_d})$ by computing the result of repeating the i-th set of variables β_i times successively for each i.

Assume that $I \subset [d]$ is of size β_i, and that for each $k \in I$, t_kx_{kj} is replaced by t_ix_{ij}. In $\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_d)$ there are $\beta_i!$ ways of choosing terms of the form t_kx_{kj} from the

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

factors F_s with $s \in I$ with $k \in I$ and the t_k all distinct, but if we replace each $t_k x_{kj}$ by $t_i x_{ij}$, all of these $\beta_i!$ choices look the same.

Now let us turn to the consideration of the coefficent of $\mathbf{t}^{\boldsymbol{\beta}}$ in (2.1). Note that there is only one way of choosing β_i terms of the form $t_i x_{ij}$ from among the factors F_k with $k \in I$. Considering each of the d sets of variables in turn, we see that if we substitute the i-th set of variables β_i times in $\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_d)$, we will see each monomial that appears as a coefficient of $\mathbf{t}^{\boldsymbol{\beta}}$ repeated $\boldsymbol{\beta}!$ additional times. Therefore, the coefficient of $\mathbf{t}^{\boldsymbol{\beta}}$ is $\frac{1}{\boldsymbol{\beta}!}\mathbf{F}(\mathbf{x}_1^{\beta_1}, \ldots, \mathbf{x}_d^{\beta_d})$.

Parts (ii) and (iii) follow immediately from the definition of $\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_d)$ as the coefficient of $\mathbf{t}^{\mathbf{1}}$ in (2.1). Part (iv) follows by computing $\mathbf{F}(\mathbf{x}, \ldots, \mathbf{x})$ as the coefficient of $\mathbf{t}^{\mathbf{1}}$ in

$$F(t_1\mathbf{x} + \cdots + t_d\mathbf{x}) = \prod_{i=1}^{n}((t_1 + \cdots + t_d)x_i)^{\alpha_i} = (t_1 + \cdots + t_d)^d \mathbf{x}^{\boldsymbol{\alpha}}. \qquad \blacksquare$$

Observation. Recall that we may identify the elements of S^dV^* with elements of T^dV^* that are invariant under the action of the symmetric group on d letters. This point of view is especially important in [13, 14]. Explicitly, if $v_i \in V^*$, then

$$v_1 \cdots v_d \longmapsto \sum_{\sigma \in S_d} v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(d)}.$$

Note that the image of a monomial $m \in S^dV^*$ in T^dV^* is a weighted sum over all of the monomials in the coset represented by m, and m is $1/d!$ times the projection of this element of T^dV^* into S^dV^*. Therefore, we can easily pass from the expression of an element of S^dV^* as a d-tensor that is invariant under the action of the symmetric group on d letters to its polarization; we just write the elements appearing in the i-th factor in the tensor in terms of $\mathbf{x}_i$ and erase the tensor symbols. For example,

$$\begin{aligned} x_1^2 x_2 &\longmapsto 2(x_1 \otimes x_1 \otimes x_2 + x_1 \otimes x_2 \otimes x_1 + x_2 \otimes x_1 \otimes x_1) \\ &\longmapsto 2(x_{11}x_{21}x_{32} + x_{11}x_{22}x_{31} + x_{12}x_{21}x_{31}). \end{aligned}$$

The following elementary lemma describes relationships between polarization and partial differentiation.

Lemma 2.6 *Let F be a homogeneous polynomial of degree $d + r$.*

(i) *If $F = \mathbf{x}^{\boldsymbol{\alpha}}$, then*

$$\mathbf{F}(\mathbf{x}, \ldots, \mathbf{x}, \mathbf{y}, \ldots, \mathbf{y}) = \boldsymbol{\alpha}! \sum_{\boldsymbol{\beta} \in \mathbb{N}^n, |\boldsymbol{\beta}| = r} \binom{d}{\boldsymbol{\alpha} - \boldsymbol{\beta}} \binom{r}{\boldsymbol{\beta}} \mathbf{x}^{\boldsymbol{\alpha} - \boldsymbol{\beta}} \mathbf{y}^{\boldsymbol{\beta}}.$$

(ii) *If $\boldsymbol{\beta} \in \mathbb{N}^n$ with $|\boldsymbol{\beta}| = r$, then*

$$d!r! \frac{\partial^r F}{\partial \mathbf{x}^{\boldsymbol{\beta}}} = \frac{\partial^r \mathbf{F}(\mathbf{x}, \ldots, \mathbf{x}, \mathbf{y}, \ldots, \mathbf{y})}{\partial \mathbf{y}^{\boldsymbol{\beta}}}.$$

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

In both expressions we assume there are d copies of $\mathbf{x}$ and r copies of $\mathbf{y}$.

Proof (i) When we polarize F, we get a $(d+r)$-linear symmetric form in $d+r$ sets of variables $\mathbf{x}_i$. Each of the $\binom{d+r}{\boldsymbol{\alpha}}$ distinct monomials in $\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_{d+r})$ appears with coefficient $\boldsymbol{\alpha}!$. For any choice of $\boldsymbol{\beta}$ there will be $\binom{d}{\boldsymbol{\alpha}-\boldsymbol{\beta}}\binom{r}{\boldsymbol{\beta}}$ distinct monomials which will agree (and have $\mathbf{y}^{\boldsymbol{\beta}}$ as a factor) when the first d sets of variables are all set to $\mathbf{x}$ and the last r are set to $\mathbf{y}$.

(ii) It is enough to prove the result for an arbitrary monomial of degree $d+r$. Assume, without loss of generality, that $F = \mathbf{x}^{\boldsymbol{\alpha}}$. Using (i) we see that the coefficient of $\mathbf{y}^{\boldsymbol{\beta}}$ in $\mathbf{F}(\mathbf{x}, \ldots, \mathbf{x}, \mathbf{y}, \ldots, \mathbf{y})$ is

$$\boldsymbol{\alpha}!\binom{d}{\boldsymbol{\alpha}-\boldsymbol{\beta}}\binom{r}{\boldsymbol{\beta}}\mathbf{x}^{\boldsymbol{\alpha}-\boldsymbol{\beta}} = \frac{d!r!\boldsymbol{\alpha}!}{(\boldsymbol{\alpha}-\boldsymbol{\beta})!\boldsymbol{\beta}!}\mathbf{x}^{\boldsymbol{\alpha}-\boldsymbol{\beta}}.$$

Therefore, we see that taking partial derivatives with respect to $\mathbf{y}^{\boldsymbol{\beta}}$ yields

$$d!r!\frac{\boldsymbol{\alpha}!}{(\boldsymbol{\alpha}-\boldsymbol{\beta})!}\mathbf{x}^{\boldsymbol{\alpha}-\boldsymbol{\beta}} = d!r!\frac{\partial^r F}{\partial \mathbf{x}^{\boldsymbol{\beta}}}.$$

■

The next lemma is a modification of an observation in [13]. (See also the discussion after [14, Corollary 3.2].)

Lemma 2.7 *Let $A \subseteq S^dV^*$, and $F \in S^{d+r}V^*$ be a homogeneous polynomial with polarization $\mathbf{F}(\mathbf{x}, \ldots, \mathbf{x}, \mathbf{y}, \ldots, \mathbf{y})$, of degree d in the $\mathbf{x}$-variables. The following are equivalent.*

(i) *F is in $A^{(r)}$.*
(ii) *Every coefficient of $\mathbf{F}$ as a polynomial in the $\mathbf{y}$-variables is in A.*
(iii) *Every coefficient of $\mathbf{F}(\mathbf{x}, \ldots, \mathbf{x}, \mathbf{y}_1, \ldots, \mathbf{y}_r)$, viewed as a polynomial in all of the $\mathbf{y}$-variables, is in A.*
(iv) *$\mathbf{F}(\mathbf{x}, \ldots, \mathbf{x}, \mathbf{v}, \ldots, \mathbf{v}) \in A$ for every choice of $\mathbf{v} \in V$.*

Proof First we show the equivalence of (i) and (ii). We know that $F \in A^{(r)}$ if and only if $\frac{\partial^r F}{\partial \mathbf{x}^{\boldsymbol{\beta}}} \in A$ for every $\boldsymbol{\beta} \in \mathbb{N}^n$ with $|\boldsymbol{\beta}| = r$. But $\frac{\partial^r F}{\partial \mathbf{x}^{\boldsymbol{\beta}}}$ is just $\boldsymbol{\beta}!$ times the coefficient of $\mathbf{y}^{\boldsymbol{\beta}}$ in $\mathbf{F}$ by part (ii) of Lemma 2.6.

The equivalence of (ii) and (iii) follows because the coefficient of the monomial $\mathbf{y}^{\boldsymbol{\beta}}$ in the polynomial $\mathbf{F}(\mathbf{x}, \ldots, \mathbf{x}, \mathbf{y}, \ldots, \mathbf{y})$, which has degree r in the $\mathbf{y}$-variables, is $\binom{r}{\boldsymbol{\beta}}$ times the coefficient of some monomial in the r sets of $\mathbf{y}$-variables in $\mathbf{F}(\mathbf{x}, \ldots, \mathbf{x}, \mathbf{y}_1, \ldots, \mathbf{y}_r)$.

For the equivalence of (ii) and (iv), note that we are working over an infinite field. If we choose $\binom{d+r+n-1}{d+r}$ sufficiently generic points $\mathbf{v}_i$, the vectors in indeterminates $F_{\boldsymbol{\alpha}}$ of the form $\sum_{|\boldsymbol{\alpha}|=r} F_{\boldsymbol{\alpha}}\mathbf{v}_i^{\boldsymbol{\alpha}}$ will be linearly independent. Hence, they are all in A if and only if every $F_{\boldsymbol{\alpha}} \in A$. ■

Lemma 2.7 allows us to prove the following result about the prolongations and ideals.

Theorem 2.8 *Let A be a subspace of S^dV^* and let $I \subset \mathbb{K}[\mathbf{x}]$ be the ideal generated by A. Then $F \in S^{d+r}V^*$ is in $A^{(r)}$ if and only if $\frac{\partial^r F}{\partial \mathbf{x}^{\boldsymbol{\beta}}} \in I$ for every $\boldsymbol{\beta} \in \mathbb{N}^n$ with $|\boldsymbol{\beta}| = k \leq r$.*

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

Proof One inclusion follows immediately from Definition 1.1. For the opposite inclusion assume that $F \in A^{(r)}$. Write $\mathbf{F}(\mathbf{x}, \ldots, \mathbf{x}, \mathbf{y}_1, \ldots, \mathbf{y}_r)$ as a polynomial in the variables $\mathbf{y}_i$:

$$\sum_{\boldsymbol{\beta} \in \mathbb{N}^{nr}, |\boldsymbol{\beta}|=k} F_{\boldsymbol{\beta}}(\mathbf{x}, \ldots, \mathbf{x}) \mathbf{y}^{\boldsymbol{\beta}}.$$

The symbol $\mathbf{y}$ above stands for the vector of vectors $\mathbf{y} = (\mathbf{y}_1, \ldots, \mathbf{y}_r)$.

Part (iii) of Lemma 2.7 tells us that each $F_{\boldsymbol{\beta}}(\mathbf{x}, \ldots, \mathbf{x})$ is in A. Now set the variables $\mathbf{y}_1, \ldots, \mathbf{y}_{r-k}$ equal to $\mathbf{x}$. Each $F_{\boldsymbol{\beta}}(\mathbf{x}, \ldots, \mathbf{x}) \mathbf{y}^{\boldsymbol{\beta}} \mapsto F_{\boldsymbol{\beta}}(\mathbf{x}, \ldots, \mathbf{x}) \mathbf{x}^{\boldsymbol{\alpha}'} \mathbf{y}^{\boldsymbol{\beta}-\boldsymbol{\alpha}}$ where $\boldsymbol{\alpha}' \in \mathbb{N}^n$ has i-th coordinate $\sum_j \alpha_{ij}$. From this, we can see that the coefficients of the monomials in the remaining $\mathbf{y}_i$-variables are all in I. Setting the remaining $\mathbf{y}_i$-variables all equal to $\mathbf{v}$, we see that the coefficients of the monomials in $\mathbf{v}$ will be in I and may be interpreted as partial derivatives of F of order k (up to a scalar) by part (ii) of Lemma 2.6. We conclude that all partial derivatives of order k are in I for all $k \leq r$. ∎

Recall that if $I \subset S$ is a radical ideal with $\mathrm{Ass}(I) = \{P_1, \ldots, P_m\}$, then the r-th *symbolic power* of I is defined to be $I^{(r)} := I^r[W^{-1}] \cap S$, where $W = S \backslash (P_1 \cup \cdots \cup P_m)$. We define the r-th *differential power* of I to be

$$I^{\langle r \rangle} = \left\{ f \in S \;\middle|\; \frac{\partial^{|\boldsymbol{\beta}|} f}{\partial \mathbf{x}^{\boldsymbol{\beta}}} \in I \text{ for all } |\boldsymbol{\beta}| \leq r-1 \right\}.$$

If $\mathbb{K}$ is algebraically closed of characteristic 0 and I is prime, then by the theorem of Zariski and Nagata, $I^{(r)} = I^{\langle r \rangle}$. See [8, Theorem 3.14] for a discussion of the proof and pointers to a more general statement in characteristic p.

The theorem of Zariski and Nagata also holds for radical ideals. While we found this statement in the literature, we could not find its proof, so we include one for completeness.

Corollary 2.9 *If I is a radical ideal over an algebraically closed field of characteristic zero, then $I^{(r)} = I^{\langle r \rangle}$.*

Proof Suppose that $\mathrm{Ass}(I) = \{P_1, \ldots, P_m\}$. It is easy to see that $I^{\langle r \rangle} = \bigcap P_i^{\langle r \rangle}$, so by the theorem of Zariski and Nagata it suffices to show that $I^{(r)} = \bigcap P_i^{(r)}$. Since I is radical, by prime avoidance, $\mathrm{Ass}(I^{(r)}) = \mathrm{Ass}(I)$, and the P_i-primary component of $I^{(r)}$ is $(I^{(r)})_{P_i} \cap S$. But, as localization commutes with products and intersections, we have

$$(I^{(r)})_{P_i} = (I^r[W^{-1}] \cap S)_{P_i} = (I^r)_{P_i} \cap S_{P_i} = (I_{P_i})^r = ((P_i)_{P_i}))^r = (P_i^r)_{P_i}.$$

We see that $(I^{(r)})_{P_i} \cap S = (P_i^r)_{P_i} \cap S = P_i^{(r)}$, which completes the proof. ∎

Thus, we have the following corollary to Theorem 2.8.

Corollary 2.10 *Let $\mathbb{K}$ be an algebraically closed field of characteristic 0. Let I be a radical ideal with $I \subset \langle x_1, \ldots, x_n \rangle^d$ and let $A = I_d$. Then the $(d+r)$-th graded piece of $I^{(r+1)}$ is $A^{(r)}$.*

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

3 Computing Prolongations

In this section we describe algorithms for computing prolongations that use linear algebra and can be implemented in a computer algebra system. We also discuss how combinatorial tools can be used to speed up the computations by reducing the dimensions of the intermediate vector spaces that need to be computed. These combinatorial approaches can also be used to determine explicit descriptions of prolongations.

3.1 Algorithms

We will describe some algorithms for computing prolongations that depend on various implementations of the equivalent definitions from Section 2. In practice, we will have a basis for A consisting of a set of homogeneous polynomials of degree d and will want to compute $A^{(r)}$. The crucial step in each of the algorithms for computing prolongations that we describe may be performed by Gaussian elimination. However, what is easiest to implement depends on the way polynomials are stored, since converting polynomials to vectors that may be operated on by the user may be nontrivial in practice in any given computer algebra package.

Algorithm 3.1

INPUT: A basis for A.

OUTPUT: A basis for $A^{(r)} \subseteq S^{d+r}V^*$.

STEP 1: Map a basis for $S^{d+r}V^*$ into $S^dV^* \otimes S^rV^*$ via the co-multiplication map.

STEP 2: Compute the intersection of $A \otimes S^rV^*$ with the space constructed in STEP 1. Multiplication (just "erasing" the tensor symbol) maps a basis for this intersection into $S^{d+r}V^*$ giving a basis for $A^{(r)}$.

Unfortunately, the simplest implementation of Algorithm 3.1 introduces a new set of variables to represent the terms to the right of the tensor symbol, which slows computation. Alternatively, we can exploit the connection between co-multiplication and partial differentiation to avoid introducing a new set of variables.

Algorithm 3.2

INPUT: A basis for A.

OUTPUT: A basis for $A^{(r)}$.

STEP 1: For each $\boldsymbol{\beta} \in \mathbb{N}^r$, with $|\boldsymbol{\beta}| = r$, compute $A_{\boldsymbol{\beta}}$, the space of all forms of degree $d + r$ whose partial derivative with respect to $\mathbf{x}^{\boldsymbol{\beta}}$ is in A.

STEP 2: The intersection of the spaces $A_{\boldsymbol{\beta}}$ is equal to $A^{(r)}$.

Another alternative would require more extensive programming, but is potentially quite fast. The complexity of Algorithm 3.3 is governed by the amount of preprocessing necessary to coordinatize our basis vectors and the Gaussian elimination in STEP 3.

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

Algorithm 3.3

INPUT: A basis B for A.

OUTPUT: A basis for $A^{(r)}$.

STEP 1: Fix a term order so that monomials form an ordered basis for S. Abusing notation, let A denote the matrix whose columns are the coefficients of the elements of B with respect to this ordered basis.

STEP 2: Let F be the generic form of degree $d+r$. Let C be the matrix with a column for each $|\boldsymbol{\beta}| = r$. The column corresponding to $\boldsymbol{\beta}$ is the coordinate vector of $\frac{\partial^r F}{\partial \mathbf{x}^{\boldsymbol{\beta}}}$ with respect to our ordered basis. (After a suitable scaling of the basis elements, C is the catalecticant matrix $C(d, r; n)$.)

STEP 3: Form the augmented matrix $[A|C]$. The space $A^{(r)}$ is just the space of polynomials F for which the augmented matrix $[A|C]$ is consistent. We find this space by putting A in reduced-echelon form which will give a linear equation on the entries of C for every zero row to the left of the bar in the augmented matrix. Solving this system of equations gives the coordinate vectors of a basis for $A^{(r)}$.

3.2 Monomial Prolongations

In this section, we describe the prolongations of vector spaces spanned by monomials. The monomial case can be solved purely combinatorially and can be used as a tool for reducing the computational burden in the general case.

Proposition 3.4 *Suppose that A is spanned by monomials. A monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ is in $A^{(r)}$ if and only if $\mathbf{x}^{\boldsymbol{\alpha}-\boldsymbol{\beta}} \in A$ for all $\mathbf{x}^{\boldsymbol{\beta}}$ dividing $\mathbf{x}^{\boldsymbol{\alpha}}$ with $|\boldsymbol{\beta}| = r$.*

Proof The differential operator $\partial^r/\partial \mathbf{x}^{\boldsymbol{\beta}}$ maps monomials to monomials. If $\mathbf{x}^{\boldsymbol{\beta}}$ divides $\mathbf{x}^{\boldsymbol{\alpha}}$, then $\partial^r \mathbf{x}^{\boldsymbol{\alpha}}/\partial \mathbf{x}^{\boldsymbol{\beta}} = C\mathbf{x}^{\boldsymbol{\alpha}-\boldsymbol{\beta}}$ for a nonzero constant C, otherwise $(\frac{\partial^r}{\partial \mathbf{x}^{\boldsymbol{\beta}}})\mathbf{x}^{\boldsymbol{\alpha}} = 0$. ∎

An important special case arises when $d = 2$. In this case, the generators of A have two types: squarefree pairs $x_i x_j$ and pure powers x_i^2. Let $\sigma \subset [n]$ denote the set of i such that $x_i^2 \in A$. We define a graph $G(A, r)$ as follows.

Definition 3.5 Let A be a vector space spanned by quadratic monomials from $\mathbb{K}[\mathbf{x}]$. For each integer $r > 0$, we define a graph $G(A, r)$ with $r + 2$ vertices for each indeterminate whose square is in A, and a single vertex for all other indeterminates. Formally, the vertex set of $G(A, r)$ is the set of all pairs (i, j) with $i \in [n]$, where $j \in [r+2]$ if $i \in \sigma$ and $j = 1$ otherwise. A pair of vertices (i_1, j_1) (i_2, j_2) is connected by an edge if $x_{i_1} x_{i_2} \in A$.

The graph $G(A, r)$ can be used to read off the generators of the prolongations $A^{(r)}$.

Corollary 3.6 *The induced subgraph of $G(A, r)$ on vertices $(i_1, j_1), \ldots, (i_{r+2}, j_{r+2})$ is a complete graph if and only if $x_{i_1} \cdots x_{i_{r+2}}$ is in the prolongation $A^{(r)}$.*

Proof The set of vertices $(i_1, j_1), \ldots, (i_{r+2}, j_{r+2})$ forms a K_{r+2} if and only if $x_{i_k} x_{i_l} \in A$ for all $1 \leq k < l \leq r + 2$ if and only if each divisor of $x_{i_1} \cdots x_{i_{r+2}}$ of degree r has quotient in A. ∎

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

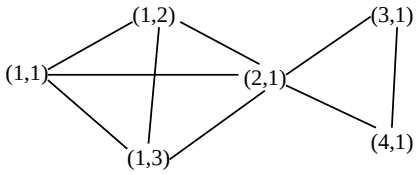

Figure 1: $G(A, 1)$

Example 3.7 Let A be the span of $x_1^2, x_1x_2, x_2x_3, x_2x_4, x_3x_4 \in \mathbb{K}[x_1, x_2, x_3, x_4]$. To compute $A^{(1)}$, we construct the graph $G(A, 1)$ (see Figure 1) containing five complete subgraphs K_3. One is the subgraph of $G(A, 1)$ on the vertices $(1, 1), (1, 2), (1, 3)$ and this corresponds to the monomial $x_1^3 \in A^{(1)}$. There are three triangles in the graph of the form $(1, i), (1, j), (2, 1)$ and these all correspond to the monomial $x_1^2x_2 \in A^{(1)}$. Finally the triangle $(2, 1), (3, 1), (4, 1)$ corresponds to the monomial $x_2x_3x_4 \in A^{(1)}$. Corollary 3.6 implies that these three monomials span $A^{(1)}$.

Corollary 3.8 *Computing prolongations is NP-hard.*

Proof Focusing on the case where M is generated by squarefree quadratic monomials, we see that the prolongations are determined by the complete subgraphs in a fixed graph $G(M)$. In particular, $A^{(r)} = 0$ if and only if the largest clique of $G(M)$ has cardinality less than $r + 2$. However, determining the cardinality of the largest clique is NP-hard. ■

Besides the connections to graph theory, the monomial case can be used as a tool for reducing the dimensionality of the computations described in Section 2.

Proposition 3.9 *Let $A \subset S^dV^*$ be any vector space of forms of degree d, and let $M(A)$ denote the span of the monomials that appear as a term with nonzero coefficient in some polynomial in A. Then $A^{(r)} \subseteq M(A)^{(r)}$.*

Proof A monomial differential operator is injective on the set of monomials it does not kill. Thus, for every monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ of every polynomial in $A^{(r)}$, and every divisor $\mathbf{x}^{\boldsymbol{\beta}}$ of $\mathbf{x}^{\boldsymbol{\alpha}}$ there exists a polynomial $f \in A$ such that $\mathbf{x}^{\boldsymbol{\alpha}-\boldsymbol{\beta}}$ appears with a nonzero coefficient in f. ■

Proposition 3.9 can be useful for computations because the monomial case can be precomputed combinatorially. Then, when applying the algorithms from the previous sections, one can immediately eliminate any polynomials that arise in a partial computation that do not belong to $M(A)^{(r)}$. Furthermore, the monomial case can be used as a theoretical tool to prove that certain prolongations are, in fact, empty.

Example 3.10 **(No 3-way Interaction)** Recall that the toric ideal of the no 3-way interaction model is the kernel of the ring homomorphism

$$\phi_{lmn}\colon \mathbb{K}\left[x_{ijk} \;\middle|\; i \in [l], j \in [m], k \in [n]\right] \longrightarrow \mathbb{K}[a_{ij}, b_{ik}, c_{jk}], \quad x_{ijk} \longmapsto a_{ij}b_{ik}c_{jk}.$$

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

The no 3-way interaction model is an example of a log-linear model in statistics. Giving a complete descriptions of the toric ideals $I_{lmn} = \ker \phi_{lmn}$ is a challenging open problem in algebraic statistics that has been studied by many authors [1, 7]. It is known that the lowest degree of a minimal generator is 4 and that $A = (I_{lmn})_4$ is spanned by the $\binom{l}{2}\binom{m}{2}\binom{n}{2}$ binomials that are equivalent to

$$x_{111}x_{122}x_{212}x_{221} - x_{112}x_{121}x_{211}x_{222}$$

under the natural action of the product of symmetric groups $S_4 \times S_4 \times S_4$ on indices.

Let $M(A)$ be the space of quartics spanned by the monomials appearing in these binomials. We will show that $M(A)^{(k)} = 0$ for all k. Proposition 3.9 then implies that $A^{(k)} = 0$ for all k. Since the prolongation of a prolongation is a prolongation, it suffices to show that $M(A)^{(1)} = 0$. This, in turn, is equivalent to showing that there is no monomial of degree five in $\mathbb{K}[\mathbf{x}]$ which is divisible by five distinct monomials from $M(A)$. However, if we are given any three variables that are part of a monomial in $M(A)$, there is a unique way to complete it to a monomial in $M(A)$, which guarantees that no degree five monomials of the desired type could exist.

Applying Theorem 1.2, we have shown that $A^{(3(r-1))} = 0$, and hence that the degree $3r + 1$ piece of $I_{lmn}^{\{r\}}$ is zero for all r, l, m and n. This implies that these secant ideals cannot be generated in their lowest possible degree.

Another useful property of the monomial point of view is that generation by circuits is preserved when taking prolongations.

Definition 3.11 Let $A \subset S^dV^*$ be a vector space of polynomials and $f \in A$. The *support* of f is the set of monomials that appear with nonzero coefficient. The polynomial f is a *circuit* of A if there is no polynomial $g \in A$ such that $\text{supp}(g) \subset \text{supp}(f)$, in other words, f has minimal monomial support. We say that A is *minimally generated* by its circuits if the set of all of its circuits is a basis for A.

Remark. Circuits are basic objects in matroid theory that generalize linearly dependent sets. Note that for polynomials there are two natural definitions of circuits. One is the definition that we have used, where we consider the set of polynomials as a vector space, and the connection to linear algebra is clear. Another definition of circuit for an ideal I is that a circuit of f is a polynomial such that the set of variables appearing in f is minimal with respect to inclusion among all nonzero polynomials in I. If I is a prime ideal, this leads to the notion of an algebraic matroid. This is the definition of circuit which appears, for instance, in [16, Chapter 4], but this is *not* the notion of circuit that we mean.

Note that $A \subset S^dV^*$ is minimally generated by its circuits if and only if the monomial support of any two circuits with distinct support are disjoint. Indeed, suppose that f and g are two circuits that contain the monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ with coefficient one. Then the polynomial $f - g \in A$ does not contain $\mathbf{x}^{\boldsymbol{\alpha}}$. The new polynomial can be written as a linear combination of circuits with support in $\text{supp}(f - g)$. But this implies that either f or g is not needed as a minimal generator. We show below that the property of being minimally generated by circuits is preserved under prolongation.

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

Proposition 3.12 *If A is minimally generated by its circuits, then so are the prolongations $A^{(r)}$.*

Proof It suffices to show that if $\mathbf{x}^{\boldsymbol{\alpha}}$ is a monomial that is in the support of some circuit of $A^{(r)}$, there is no other circuit of $A^{(r)}$ containing $\mathbf{x}^{\boldsymbol{\alpha}}$ in its support. Suppose to the contrary that there are two circuits f and g that contain a monomial in common. Let S be the set of monomials appearing in both f and g. Let $\mathbf{x}^{\boldsymbol{\alpha}}$ be any monomial in S, and let $\mathbf{x}^{\boldsymbol{\beta}}$ be any divisor of $\mathbf{x}^{\boldsymbol{\alpha}}$ of degree r. The derivatives $\frac{\partial^r f}{\partial \mathbf{x}^{\boldsymbol{\beta}}}$ and $\frac{\partial^r g}{\partial \mathbf{x}^{\boldsymbol{\beta}}}$ are thus nonzero and in A. Moreover, they must both contain a multiple of the same circuit h that contains $\mathbf{x}^{\boldsymbol{\alpha}-\boldsymbol{\beta}}$, because A is minimally generated by its circuits. This means that if $\mathbf{x}^{\boldsymbol{\gamma}}$ appears in h, then $\mathbf{x}^{\boldsymbol{\beta}+\boldsymbol{\gamma}}$ appears in both f and g, and will belong to S.

Now let f_S and g_S be the polynomials obtained from f and g by taking only those terms corresponding to elements of S. We will argue that if $\mathbf{x}^{\boldsymbol{\beta}}$ has degree r, then $\frac{\partial^r f_S}{\partial \mathbf{x}^{\boldsymbol{\beta}}}$ is in A. Indeed, by the argument in the preceding paragraph, if $\mathbf{x}^{\boldsymbol{\beta}}$ divides an element of S, we get an element of A, and otherwise $\frac{\partial^r f_S}{\partial \mathbf{x}^{\boldsymbol{\beta}}} = 0$. However, since f and g were circuits, this implies that $f_S = f$ and $g_S = g$. Since f and g are circuits with the same support, they must be nonzero multiples of each other. ∎

Proposition 3.12 is useful in special cases for proving that we have determined a complete generating set for a particular prolongation.

Example 3.13 Let I be the ideal of the Segre embedding of $\mathbb{P}^{n_1-1} \times \mathbb{P}^{n_2-1}$ into $\mathbb{P}^{n_1 n_2-1}$. The ideal I is generated by the 2×2 minors of the generic matrix $X = (x_{ij})$. Let A be the space of quadrics spanned by these 2×2 minors. Note that each 2×2 minor is a circuit, and these circuits have disjoint monomial support. By Proposition 3.12 $A^{(r)}$ is generated by circuits which have disjoint monomial support.

The monomials appearing in the 2×2 minors generating I are precisely the monomials $x_{i_1 j_1} x_{i_2 j_2}$ such that $i_1 \neq i_2$ and $j_1 \neq j_2$. The cliques in the resulting graph $G(A, r)$ are the monomials of the form $x_{i_1 j_1} \cdots x_{i_{r+2} j_{r+2}}$ such that $i_k \neq i_l$ and $j_k \neq j_l$ for all $k \neq l$. Each such monomial is a term of a unique $(r+2) \times (r+2)$ minor. Each $(r+2) \times (r+2)$ minor belongs to $A^{(r)}$ which can be verified by differentiating the Laplace expansion of the determinant. As each minor is a circuit, we deduce that these $(r+2) \times (r+2)$ minors span the prolongation. ∎

4 Prolongations and Secant Varieties

In this section we will explain the relationship between prolongation and secant varieties. The proof of Lemma 2.2 in [13] goes through in a more general setting, and our proof of Theorem 4.1 follows along these lines. Although we could also use the ideas of the proof of [13, Lemma 2.2] to prove Theorem 4.2, we give an alternate and simpler proof appealing to the computation of joins of ideals.

Theorem 4.1 *Suppose that $X \subseteq \mathbb{P}^{n-1}$ is a variety over an algebraically closed field, and $I = I(X)$. Let $A = I_d$. Then $A^{((r-1)(d-1))}$ is contained in the ideal of the r-th secant variety of X.*

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

Proof Suppose that $F \in A^{((r-1)(d-1))}$ so that

$$\deg F = (d-1)(r-1) + d = dr - r - d + 1 + d = dr - r + 1 = r(d-1) + 1.$$

A general point on the r-th secant variety of X is the span of r points of X. So let $\mathbf{v} = t_1\mathbf{v}_1 + \cdots + t_r\mathbf{v}_r$ where the t_i and $\mathbf{v}_i$ are indeterminates. We will show that for any specialization of the $\mathbf{v}_i$ to points of X, and $t_i \in \mathbb{K}$, $F(\mathbf{v}) = 0$. Since

$$F(\mathbf{x}) = \frac{1}{(r(d-1)+1)!}\mathbf{F}(\mathbf{x}, \ldots, \mathbf{x}),$$

$F(\mathbf{v}) = 0$ if and only if $\mathbf{F}(\mathbf{v}, \ldots, \mathbf{v}) = 0$.

The point now is that the polarization $\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_{r(d-1)+1})$ is linear in each set of variables $\mathbf{x}_i$. This implies that

$$\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_{i-1}, \mathbf{v}, \mathbf{x}_{i+1} \ldots, \mathbf{x}_{r(d-1)+1}) = \sum_{j=1}^{r} t_j \mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_{i-1}, \mathbf{v}_j, \mathbf{x}_{i+1}, \ldots, \mathbf{x}_{r(d-1)+1}).$$

Therefore, we see that

$$\mathbf{F}(\mathbf{v}, \ldots, \mathbf{v}) = \sum_{\substack{\boldsymbol{\beta} \in \mathbb{N}^r \\ |\boldsymbol{\beta}| = r(d-1)+1}} \binom{r(d-1)+1}{\boldsymbol{\beta}} \mathbf{t}^{\boldsymbol{\beta}} \mathbf{F}(\mathbf{v}_1^{\beta_1}, \ldots, \mathbf{v}_r^{\beta_r}),$$

where $\mathbf{v}_i$ is repeated β_i times. For each $\boldsymbol{\beta}$ in the sum, $|\boldsymbol{\beta}| = r(d-1)+1$, implies that some $\beta_i \geq d$. Therefore, $\mathbf{F}(\mathbf{v}_1^{\beta_1}, \ldots, \mathbf{v}_r^{\beta_r})$ can be written as a polynomial whose coefficients have degree d in $\mathbf{v}_i$. Since $F \in A^{((r-1)(d-1))}$, every coefficient of a monomial in the $\mathbf{y}$-variables in the polynomial $\mathbf{F}(\mathbf{x}, \ldots, \mathbf{x}, \mathbf{y}_1, \ldots, \mathbf{y}_{(r-1)(d-1)})$ is in A by part (iii) of Lemma 2.7. Therefore, each of these degree d coefficients is in A (written in the $\mathbf{v}_i$-variables). Thus, if we specialize all of the $\mathbf{v}_j$ to points of X, $\mathbf{F}(\mathbf{v}_1^{\beta_1}, \ldots, \mathbf{v}_r^{\beta_r}) = 0$. We conclude that $\mathbf{F}(\mathbf{v}, \ldots, \mathbf{v}) = 0$. ∎

We also have the partial converse if we know that the ideal of X does not contain any forms of degree $< d$.

Theorem 4.2 *Suppose that $X \subset \mathbb{P}^{n-1}$ is a variety over an algebraically closed field and that no form of degree $\leq d-1$ vanishes on X. If $m = r(d-1)+1$, then $I(X^{\{r\}})_m = A^{((r-1)(d-1))}$.*

To prove the theorem, we collect some general definitions and results about secants and joins of ideals. Given a collection of ideals $I_1, \ldots, I_r \subseteq \mathbb{K}[\mathbf{x}]$, their *join* is obtained by constructing the new ideal

$$I_1 * \cdots * I_r = \left(I_1(\mathbf{y}_1) + \cdots + I_r(\mathbf{y}_r) + \left\langle x_j - \sum_{i=1}^{r} y_{ij} \;\middle|\; j \in [n] \right\rangle \right) \cap \mathbb{K}[\mathbf{x}]$$

where $\mathbf{y}_i$ denotes the vector of variables $\mathbf{y}_i = (y_{i1}, \ldots, y_{in})$, $I_i(\mathbf{y}_i)$ denotes the ideal I_i with variable y_{ij} substituted for variable x_j, and the big ideal in parentheses is

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

contained in the ring $\mathbb{K}[\mathbf{x}, \mathbf{y}_1, \ldots, \mathbf{y}_r]$. The r-fold join of I with itself is the r-th secant ideal $I^{\{r\}} = I * \cdots * I$. If $I_1, \ldots, I_r$ are the saturated homogeneous radical ideals over an algebraically closed field, then $I_1 * \cdots * I_r$ is the homogenous ideal representing the embedded join of the projective varieties $V(I_1), \ldots, V(I_r)$. The secant ideal $I^{\{r\}}$ is the vanishing ideal of the r-th secant variety of $V(I)$. Note that the join construction is commutative and associative, and it respects containments. Proposition 4.3, due to Simis and Ulrich, puts a restriction on the degrees of forms which may appear in the secant ideal, and Proposition 4.4 describes how symbolic powers may be computed via the join operation.

Proposition 4.3 [15] *If* $I \subseteq \langle x_1, \ldots, x_n \rangle^d$, *then* $I^{\{r\}} \subseteq \langle x_1, \ldots, x_n \rangle^{r(d-1)+1}$.

Proposition 4.4 [19] *Suppose that* $\mathbb{K}$ *is algebraically closed. If* I *is a radical ideal, then* $I^{(r)} = I * \langle x_1 \ldots, x_n \rangle^r$.

These results lead us to a more general result involving containments of secant ideals in symbolic powers. Theorem 4.2 reflects information about one graded piece of this containment.

Proposition 4.5 *Suppose that* $\mathbb{K}$ *is algebraically closed,* I *is radical, and* I *is contained in* $\langle x_1, \ldots, x_n \rangle^d$. *Then* $I^{\{r\}} \subset I^{((r-1)(d-1)+1)}$.

Proof This follows by the chain of containments

$$I^{\{r\}} = I * I^{\{r-1\}} \subseteq I * \langle x_1, \ldots, x_n \rangle^{(r-1)(d-1)+1} = I^{((r-1)(d-1)+1)}.$$

The first equality is by the associativity of the join, the second containment follows because joins respect containment together with Proposition 4.3 and the third equality follows by Proposition 4.4. ∎

Proof of Theorem 4.2 This is a direct consequence of Proposition 4.5 and Corollary 2.10. ∎

Proof of Theorem 1.2 This is a direct consequence of Theorems 4.1 and 4.2. ∎

Remark. The proofs of Theorems 4.1 and 4.2 can be extended to the nonreduced case. To do this requires the replacement of the symbolic power with the differential power, and some more algebraic reasoning in the proof of Theorem 4.1. We have only included the proof of the reduced case because it is, by far, the most interesting.

5 Application to the Binary Symmetric Model

As mentioned in the introduction, one recent motivation for the detailed study of equations vanishing on secant varieties comes from algebraic statistics, where secant varieties correspond to statistical models called mixture models. Our goal in this section is to illustrate how prolongations can be used to derive some nontrivial algebraic constraints on mixture models in situations where it seems difficult to prove directly that the same equations belong to the secant ideal. In particular, we explore this problem for some models arising in phylogenetics.

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

To give our description of equations in the prolongation, we first need to describe the space of quadrics which generate the ideal of the phylogenetic model. The bulk of this description can be found in [17]. First we describe the variables of the toric ideal. Let T be an unrooted trivalent tree (that is, each vertex of the tree that is not a leaf has degree three) with n leaves. The ideal of the phylogenetic model I_T lives in the polynomial ring in 2^{n-1} indeterminates,

$$\mathbb{K}[q] := \mathbb{K}[q_{\mathbf{i}} \mid \mathbf{i} \in (\mathbb{Z}/2\mathbb{Z})^n_{\text{even}}],$$

where $(\mathbb{Z}/2\mathbb{Z})^n_{\text{even}}$ is the group of binary strings of length n with sum zero in $\mathbb{Z}/2\mathbb{Z}$. These q indeterminates are the Fourier transform of the natural probability coordinates (see [17]).

The ideal I_T is generated by determinantal quadrics. Specifically, each internal edge e of the tree induces a *split* of the leaves into two disjoint sets, $A|B$. The indeterminates are also partitioned into two disjoint sets, namely, the sets

$$\left\{ q_{\mathbf{i}} \mid \sum_{j\in A} i_j = 0 \in \mathbb{Z}/2\mathbb{Z} \right\} \quad \text{and} \quad \left\{ q_{\mathbf{i}} \mid \sum_{j\in A} i_j = 1 \in \mathbb{Z}/2\mathbb{Z} \right\}.$$

These two sets of indeterminates fit into two $2^{|A|-1} \times 2^{|B|-1}$ matrices, M_0^e and M_1^e, whose rows are indexed by the strings $\mathbf{i}_A$ and whose columns are indexed by $\mathbf{i}_B$. The toric ideal I_T is generated by the set of all 2×2 minors of the matrices M_0^e and M_1^e as e ranges over all the internal edges of T. Let A_T denote the space of quadrics generated by the determinants described above.

Example 5.1 For instance if T is the trivalent tree with four leaves with unique internal split $12|34$, then we have

$$M_0^e = \begin{pmatrix} q_{0000} & q_{0011} \\ q_{1100} & q_{1111} \end{pmatrix} \qquad M_1^e = \begin{pmatrix} q_{0101} & q_{0110} \\ q_{1001} & q_{1010} \end{pmatrix}$$

and I_T is a complete intersection of quadrics.

While the description given thus far is rich enough to describe generators of the ideals I_T, we need a more involved combinatorial description of the indeterminates in the ring $\mathbb{K}[q]$ to provide a characterization of the polynomials in the prolongation. The crucial observation is that associated with each indeterminate $q_{\mathbf{i}}$ is a labeling of all edges in the tree T by zeros and ones. An edge gets the label $\sum_{j\in A(e)} i_j \in \mathbb{Z}/2\mathbb{Z}$ where $A(e)$ is one part of the split induced by the edge e. Note that this labeling naturally corresponds to a set of disjoint paths through the tree T such that the end points of every path are leaves of the tree. Conversely, every such set of disjoint paths is the associated labeling of some indeterminate $q_{\mathbf{i}}$. Thus, for each such labeling L we get an indeterminate q_L. In [5], these unions of paths are called sockets. We will use these path indeterminates in the remainder of the section.

Now we wish to describe generators of the prolongation of the space of quadrics we have described, which we do in terms of the path indeterminates from above.

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

A *frame* F is a partial labeling of the tree T where the labels have been assigned to a trivalent subtree $T(F)$ of T. The frame has *active edges* $a(F)$ which are the leaves of $T(F)$ that are not leaves of T. Each active edge e induces a subtree $T_e(F) \subset T$ consisting of all edges on the side of e that does not contain $T(F)$. Let L^e denote the set of all possible labelings of $T_e(F)$ that are compatible with the frame F (that is, can be completed to a variable). If F is a frame and e is an edge of F that has been assigned, let $F(e)$ be the label assigned to the edge e.

Definition 5.2 A collection of frames $F_1, \ldots, F_d$ together with a function

$$e(\,\cdot\,,\,\cdot\,)\colon \binom{[d]}{2} \longrightarrow E(T)$$

is *compatible* if $e(\,\cdot\,,\,\cdot\,)$ satisfies the following.

(i) For all $(i, j) \in \binom{[d]}{2}$, $e(i, j) \in a(F_i) \cap a(F_j)$ with $F_i(e(i, j)) = F_j(e(i, j))$;
(ii) If $e(i, j) = e(j, k)$, then $e(i, j) = e(i, k)$,
(iii) For all $j \in [d]$, $\bigcup_{i \neq j} e(i, j) = a(F_j)$.

The function $e(\,\cdot\,,\,\cdot\,)$ determines an equivalence relation on the set of pairs (F_i, e) with $e \in a(F_i)$ where (F_i, e) is defined to be equivalent to itself, and if $i \neq j$, then we define $(F_i, e_1) \sim (F_j, e_2)$ if $e(i, j) = e_1 = e_2$. Let E denote such an equivalence class and let $C(E) \subset L^e$ be a set of $|E|$ distinct labellings of $T_e(F)$ compatible with the $F_i \in E$. Given all these data (in particular, the frames and the labelling sets $C(E)$) we define a polynomial of degree d. To do this, fix a particular base ordering on each of the sets $C(E)$. Now for each E, take some permutation of $C(E)$. This set of permutations can be used to complete all the frames $F_1, \ldots, F_d$ in a unique ordered way. This is accomplished by adding the first element of each $C(E)$ to the frame F_j that appears first in the equivalence class E and so on. Thus each set of permutations yields a monomial in the q_L. Denote by $P(F_1, \ldots, F_d\,;\, C(E_1), \ldots, C(E_k))$ the signed sum of all such monomials where the sign of a monomial is the product of the signs of the permutations used to form the monomial.

Example 5.3 **(The six-leaf snowflake)** Let T be the six-leaf tree (see Figure 2) and let A be the span of the quadratic binomials which generate I_T.

Computing $A^{(1)}$ and $A^{(2)}$ with *Macaulay 2* [11], we see that $A^{(1)}$ is spanned by 32 8-term cubics and $A^{(2)}$ is spanned by a single 64-term quartic form. As we will see, in

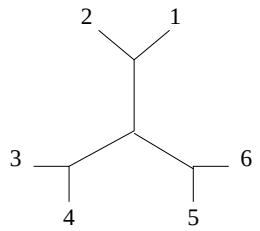

Figure 2

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

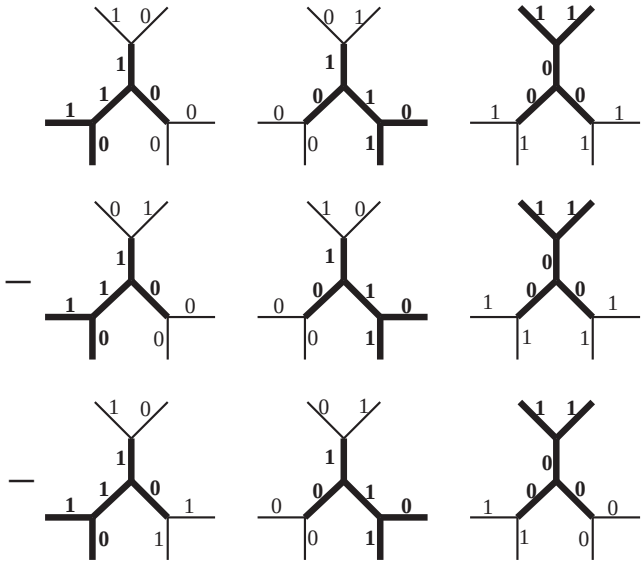

Figure 3

both cases, the construction described above yields the entire prolongation.

To construct a cubic, we need to choose three frames with compatible labelings. In Figure 3 our choice of frame is depicted in bold.

We show triples of trees that correspond to the first three terms of the 8-term cubic

$$q_{011000}q_{100010}q_{111111} - q_{101000}q_{010010}q_{111111} - q_{011011}q_{100010}q_{111100} + q_{101011}q_{010010}q_{111100} - q_{011000}q_{101110}q_{110011} + q_{101000}q_{011110}q_{110011} + q_{011011}q_{101110}q_{110000} - q_{101011}q_{011110}q_{110000}.$$

We get 32 such cubics because there are 4 ways of choosing three distinct frames and there are two ways of labelling each of the pairs of cherries attached to the three inactive edges on the frames.

Our 64-term quartic is constructed by choosing the 4-tuple consisting of our 4 distinct choices of frames and completing each edge-labelling in any way allowed. There is only one way to define the function $e(\cdot\,,\cdot\,)$ and each edge on each frame is active.

***Example 5.4* (The six-leaf caterpillar)** Let T be the six-leaf caterpillar-shaped graph (see Figure 4). The corresponding toric variety has ideal I_T generated by the 2×2 minors of four 2×8 and two 4×4 matrices. Using *Macaulay 2* [11], one can see that $A^{(1)}$ is spanned by 32 6-term cubics and that $A^{(2)}$ is spanned by two 24-term

https://doi.org/10.4153/CJM-2009-047-5 Published online by Cambridge University Press

Figure 4: Six-leaf caterpillar

quartics. These forms may be constructed using the methods above although it is easy to see that they are the 3×3 and 4×4 minors of the 4×4 matrices used to define I_T.

Theorem 5.5 *For any set of compatible frames $\mathcal{F} = F_1, \ldots, F_d$, compatibility function $e(\cdot,\cdot)$, and completions $\mathcal{C} = C(E_1), \ldots, C(E_k)$, the polynomial $P(\mathcal{F};\mathcal{C})$ is in the prolongation $A_T^{(d-2)}$.*

Proof The proof is by induction on d. When $d = 2$, $P(\mathcal{F};\mathcal{C})$ yields the description of a 2×2 minor of a matrix $M^{e(1,2)}_{F(e(1,2))}$ associated to the unique common active edge in the two frames. So suppose the statement is true for $d-1$. The result will follow if we show that the derivative of the degree d polynomial $P(\mathcal{F};\mathcal{C})$ with respect to any variable is the sum of polynomials of the form $P(\mathcal{F}';\mathcal{C}')$ of degree $d-1$.

Let $\mathcal{F} = F_1, \ldots, F_d$ and q_L be any variable appearing in a monomial in $P(\mathcal{F};\mathcal{C})$. By our construction of $P(\mathcal{F};\mathcal{C})$, each occurrence of q_L is associated to a frame in $\mathcal{F}$. Without loss of generality, assume that q_L arises by completing the labelling of the frame F_d. (It may be associated with other frames as well.) In each monomial in which q_L appears by completing a labelling of F_d, the $d-1$ other factors come from the frames $F_1, \ldots F_{d-1}$. Now construct the new set $C(E_1)', \ldots, C(E_k)'$ by removing the elements from $C(E_1), \ldots, C(E_k)$ that are used to make q_L. If any of the sets $C(E_i)'$ are singletons, we can take this single element and modify the appropriate frame F_l to get a new frame, and remove the set $C(E_i)'$ from our list of completions. Carrying out this procedure yields a set of frames $\mathcal{F}' = F_1', \ldots, F_{d-1}'$ and a set of completions $\mathcal{C}' = C(E_1'), \ldots, C(E_r')$, such that upon dividing all monomials in $P(\mathcal{F};\mathcal{C})$ that have this particular realization of q_L (associated with the frame F_d) we get the polynomial $P(\mathcal{F}';\mathcal{C}')$. Applying this argument to all realizations of q_L by different frames, we deduce that the derivative of $P(\mathcal{F};\mathcal{C})$ with respect to q_L is the (signed) sum of polynomials $P(\mathcal{F}';\mathcal{C}')$. ∎

Remark. Note that the argument in the preceding proof holds even when q_L appears to a power > 1, because the coefficient of the derivative will account for the different frames that yield q_L. It is interesting to note that this exceptional case cannot occur, however, because A is generated by polynomials with all squarefree terms. Thus, $A^{(d-2)}$ is also generated by polynomials with all squarefree terms.

Acknowledgements We would like to thank Bernd Sturmfels for suggesting to us the problem of working on prolongations and encouraging our collaboration. We also thank Aldo Conca, David Cox, J. M. Landsberg, Jason Morton and Peter Vermeire for helpful conversations and Mike Stillman for help with *Macaulay 2* which played an

important role in our understanding of examples. Experimentation with Magma[3] and Maple was also vital to this work. Finally, we are grateful to the Fields Institute for providing a wonderful working atmosphere at an important stage in the project.

References

[1] S. Aoki and A. Takemura, *Minimal basis for a connected Markov chain over* $3 \times 3 \times K$ *contingency tables with fixed two-dimensional marginals.* Aust. N. Z. J. Stat. **45**(2003), no. 2, 229–249.
[2] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of Algebraic Curves.* Springer-Verlag, New York, 1985.
[3] W. Bosma, J. Cannon, and C. Playoust. *The Magma algebra system. I. The user language.* J. Symbolic Logic **24**(1997), no. 3-4, 235–265.
[4] R. L. Bryant, S. S. Chern, R. B. Gardner, H. L. Goldschmidt, and P. A. Griffiths, *Exterior differential systems.* Mathematical Systems Research Institute Publications 18. Springer-Verlag, New York, 1991.
[5] W. Buczyńska and J. Wiśniewski, *On phylogenetic trees – a geometer's view.* Preprint, 2006. arXiv:math.AG/0601357
[6] M. Catalano-Johnson, *The homogeneous ideals of higher secant varieties.* J. Pure Appl. Algebra **158**(2001), no. 2-3, 123–129.
[7] P. Diaconis and B. Sturmfels, *Algebraic algorithms for sampling from conditional distributions.* Ann. Statis. **26**(1998), no. 1, 363–397.
[8] D. Eisenbud, *Commutative Algebra: with a View Toward Algebraic Geometry.* Graduate Texts in Mathematics 150. Springer-Verlag, New York, 1995.
[9] W. Fulton and J. Harris, *Representation Theory.* Graduate Texts in Mathematics 129. Springer-Verlag, New York, 1991.
[10] P. Griffiths, *Some aspects of exterior differential systems.* Proc. Symnpos Pure Math. 53. American Mathematical Society, Providence, RI, 1991, pp. 151–173.
[11] D. Grayson and M. Stillman, *Macaulay 2, a software system for research in algebraic geometry.* Available at http://www.math.uiuc.edu/Macaulay2/.
[12] T. Ivey and J. M. Landsberg, *Cartan for Beginners: Differential Geometry Via Moving Frames and Exterior Differential Systems.* Graduate Studies in Mathematics 61. American Mathematical Society, Providence, RI, 2003.
[13] J .M. Landsberg and L. Manivel, *On the projective geometry of rational homogeneous varieties.* Comment. Math. Helv. **78**(2003), no. 1, 65–100.
[14] ———, *On the ideals of secant varieties of Segre varieties.* Found. Comput. Math. **4**(2004), no. 4, 397–422.
[15] A. Simis and B. Ulrich, *On the ideal of an embedded join.* J. Algebra **226**(2000), no. 1, 1–14.
[16] B. Sturmfels, *Gröbner Bases and Convex Polytopes*. University Lecture Series 8. American Mathematical Society, Providence, RI, 1996.
[17] B. Sturmfels and S. Sullivant, *Toric ideals of phylogenetic invariants.* J. Comput. Biology **12**(2005), no. 2, 204–228
[18] ———, *Combinatorial secant varieties.* Pure Appl. Math. Q. **2**(2006), no. 2, 285–309
[19] S. Sullivant, *Combinatorial symbolic powers.* J. Algebra **319**(2008), no. 1, 115–142.
[20] P. Vermeire, *Some results on secant varieties leading to a geometric flip construction.* Compositio Math. **125**(2001), no. 3, 263–282.
[21] J. Weyman, *Cohomology of Vector Bundles and Syzygies.* Cambridge Tracts in Mathematics 149. Cambridge University Press, Cambridge, 2003.
[22] H. Weyl, *Classical Groups. Their Invariants and Representations*. Princeton University Press, Princeton, NJ, 1939.

Department of Mathematics and Statistics, Mount Holyoke College, South Hadley, MA 01075, U.S.A.
e-mail: jsidman@mtholyoke.edu

Department of Mathematics, North Carolina State University, Raleigh, NC, USA
e-mail: smsulli2@ncsu.edu