

Geometric Aspects of Polynomial Computation Sequences

Paul Hriljac

Department of Mathematics, ERAU

Abstract: This paper investigates the geometric structure of the set of polynomial computation sequences of a given length. It then characterizes this set as a subvariety of a Grassmanian variety. It uses this characterization to yield necessary conditions for a sequence of polynomials to be a computation sequence. It further uses this characterization to define a rational correspondence between polynomial complexity classes and subvarieties of the universal bundles of Grassmannians.

Notation: Let $\mathbb{F}$ be an algebraically closed field of characteristic other than 2. For a polynomial $f = \sum f_i x^i \in \mathbb{F}[x]$ let $\mathfrak{c}(f, i) = f_i$.

Motivation: Computation sequences are one of the fundamental constructions of complexity theory. They are somewhat more tractable than complexity classes but closely related to them. They also form geometric objects that are interesting examples in algebraic geometry.

Definition: A *computation sequence* is a sequence of linearly independent polynomials $g_0, \dots, g_r \in \mathbb{F}[x]$ with $g_0 = x, g_i = (\sum_{j=0}^{i-1} a_{i,j} g_j)(\sum_{j=0}^{i-1} b_{i,j} g_j)$ here $a_{i,j}, b_{i,j} \in \mathbb{F}$. For polynomials $g = g_0, \dots, g_r \in \mathbb{F}[x]$ let $\langle g \rangle$ denote the vector space in $\mathbb{F}[x]$ generated by $g_0, \dots, g_r$. Let $\bar{g}_i$ denote the sequence $g_0, \dots, g_{i-1}$. Let $\mathcal{G}_r$ denote the set of vector spaces spanned by computation sequences of length r :

$$\mathcal{G}_r = \{ \langle g \rangle \ni g_0 = x; g_i = (a_i \cdot \bar{g}_i) * (b_i \cdot \bar{g}_i); \{g_i\} \text{ linearly independent} \}.$$

Let $G = Gr(r+1, 2^r)$ denote the Grassmannian variety of $r+1$ -planes in 2^r -space and let $U = U(r+1, 2^r)$ denote the universal bundle over G .

Theorem 1: *Suppose $r \geq 3$. Then $\mathcal{G}_r$ is a constructible, Zariski-dense subset of an irreducible closed subvariety of G of dimension $r^2 - r - 2$.*

Proof: Define a rational map $\mathbb{A}^{r(r+1)} \rightarrow G$ by $\{a_{i,j}, b_{i,j}\} \mapsto \langle g \rangle$ where $g_i = (a_i \cdot \bar{g}_i) * (b_i \cdot \bar{g}_i)$. Since $\mathbb{A}^{r(r+1)}$ is irreducible, so is the closure of its image. It is easy to see that every element of $\mathcal{G}_r$ is in the image of this map and the points where this map is defined is Zariski dense hence $\mathcal{G}_r$ is Zariski dense in the closure of the image. That it is constructible follows from Chevalley's Theorem.

Define a rational map $\mathcal{G}_r \times \mathbb{P}^r \times \mathbb{P}^r \rightarrow \mathcal{G}_{r+1}$ by

$$(\langle g_0, \dots, g_r \rangle, [a_{r,0}, \dots, a_{r,r}], [b_{r,0}, \dots, b_{r,r}]) \mapsto \langle g_0, \dots, g_r, (\Sigma a_{r,i} g_i)(\Sigma b_{r,j} g_j) \rangle$$

Claim: This map is generically a double cover.

To see this, let $\mathcal{U}_r = \{\langle g \rangle \ni a_{i,i-1}, b_{i,i-1} \neq 0 \ \forall i\}$. Then $\mathcal{U}_r$ is a Zariski open subset of $\bar{\mathcal{G}}_r$ the Zariski closure of $\mathcal{G}_r$ in G . For $\langle g \rangle \in \mathcal{U}_r$ we may assume that $a_{i,i-1}, b_{i,i-1} = 1 \ \forall i$. Suppose that $\langle g \rangle = \langle g_0, \dots, g_r \rangle \in \mathcal{U}_r$ and that $\langle g_0, \dots, g_r \rangle = \langle g_0, \dots, g_{r-1}, h \rangle$. Say $g_r = (\Sigma_{i < r} a_i g_i) * (\Sigma_{i < r} b_i g_i)$ and $h = (\Sigma_{i < r} x_i g_i) * (\Sigma_{i < r} y_i g_i)$. Since $\langle g \rangle \in \mathcal{U}_r$ we may assume that $a_{r-1} = b_{r-1} = x_{r-1} = y_{r-1} = 1$ and so

$$g_r = g_{r-1}^2 + \Sigma_{i < r-1} (a_i + b_i) g_i g_{r-1} + \Sigma_{i,j < r-1} a_i b_j g_i g_j$$

$$h = g_{r-1}^2 + \Sigma_{i < r-1} (x_i + y_i) g_i g_{r-1} + \Sigma_{i,j < r-1} x_i y_j g_i g_j.$$

Since $\langle g_0, \dots, g_r \rangle = \langle g_0, \dots, g_{r-1}, h \rangle$ there exists c_i such that $g_r + \Sigma c_i g_i = h$.

Let $d = 2^{r-1} + 2^i$. Then $\mathfrak{c}(g_r, d) = \mathfrak{c}(h, d)$ and so $a_j + b_j = x_j + y_j \ \forall j$. Hence if g_r is given

$$y_j = a_j + b_j - x_j.$$

Next set $d = 2^{r-1}$. Comparing $\mathfrak{c}(g_r + \Sigma c_i g_i, d)$ with $\mathfrak{c}(h, d)$ we obtain $c_{r-1} = x_{r-2} y_{r-2} - a_{r-2} b_{r-2}$.

Set $d = 2^{r-2} + 2^{r-k}$. Since $\mathfrak{c}(g_r + \Sigma c_i g_i, d) = \mathfrak{c}(h, d)$ one can cancel terms and obtain

$$x_{r-2} y_{r-k} + x_{r-k} y_{r-2} = a_{r-2} b_{r-k} + a_{r-k} b_{r-2}, \forall k \geq 3.$$

This, along with the previous equation shows that, assuming $a_{i,j}, b_{i,j}$ is given, x_{r-k} is a linear function of x_{r-2} for all $k \geq 3$.

Set $d = 2^{r-2}$ and compare $\mathfrak{c}(g_r + \Sigma c_i g_i, d)$ with $\mathfrak{c}(h, d)$. Using the relations above and canceling results in the relation $c_{r-2} = x_{r-3} y_{r-3} - a_{r-3} b_{r-3}$. Setting $d = 2^{r-3} + 2^{r-4}$ and comparing results in the relation

$$x_{r-3} y_{r-4} + x_{r-4} y_{r-3} = a_{r-3} b_{r-4} + a_{r-4} b_{r-3}.$$

Substituting the previous equation into this results in a quadratic equation for x_{r-2} . Therefore there can be at most two solutions to $\{(x, y) \ni \langle g_0, \dots, g_r \rangle = \langle g_0, \dots, g_{r-1}, h \rangle\}$. Since $x = a, y = b$ and $x = b, y = a$ provide two such solutions the claim is proved. Therefore

$$\dim(\mathcal{G}_{r+1}) = 2r + \dim(\mathcal{G}_r).$$

It is easy to see that $\mathcal{U}_3$ consists of vector spaces generated by systems of polynomials of the form

$$\begin{aligned} g_0 &= x & g_1 &= x^2 & g_2 &= x^4 + a_{2,0} x^3 \\ g_3 &= x^8 + 2a_{2,0} x^7 + (a_{3,1} + b_{3,1} + a_{2,0}^2) x^6 + (a_{3,0} + a_{2,0}(a_{3,1} + b_{3,1})) x^5 \\ &\quad + (a_{2,0} a_{3,0} + a_{3,1} b_{3,1}) x^4 + a_{3,0} b_{3,1} x^3. \end{aligned}$$

The last statement of the theorem follows.

Remark: It is easy to see that $\mathcal{G}_1$ is a point and $\mathcal{G}_2$ is isomorphic to $\mathbb{P}^1$.

This characterization of computation sequences have some immediate consequences: For instance one can easily find necessary conditions for a sequence of polynomials to be a computation sequence.

Definition: Let $\alpha = (\alpha_0, \dots, \alpha_r)$ be a sequence of integers satisfying $1 \leq \alpha_0 < \dots < \alpha_r \leq 2^r$. The *Plucker coordinate* of $\langle g \rangle$ with respect to α is $p_\alpha(\langle g \rangle) = \det([c(g_i, \alpha_j)]_{i,j})$.

Theorem 2: If $\langle g \rangle \in Gr(r+1, 2^r)$ is an element of $\bar{\mathcal{G}}_r$ and if $\alpha = (1, 2, \dots, \alpha_r)$ with $\alpha_i > 2^i$ for some i , then $p_\alpha(\langle g \rangle) = 0$.

Proof: First assume that $\langle g \rangle \in \mathcal{U}_r$ so $g_0 = x, g_1 = x^2, \deg(g_i) = 2^i$. Next assume that when performing Gaussian elimination on $[c(g_i, \alpha_j)]_{i,j}$ the resulting matrix is of the form $[I_{r+1}, M]$ where M is $(r+1) \times (2^r - r - 1)$. This condition is generic for elements of $\mathcal{G}_r$. Prior to the last step of the process one obtains a matrix of the form

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ & & & & \ddots & & & \\ 0 & 0 & \cdots & 1 & 0 & * & \cdots & * \\ 0 & 0 & \cdots & 0 & 1 & * & \cdots & * \\ 0 & 0 & \cdots & 0 & * & * & \cdots & * \end{bmatrix}.$$

Row j is 0 for the first $j+1$ entries and is 0 for entries $> 2^j$. The condition $\alpha_i > 2^i$ implies that row i is all zeros hence the determinant used in the Plucker coordinate is 0. These conditions remain true for the matrix of coefficients of any system of polynomials equivalent to a system obtained by a computation sequence since the relevant functions respect matrix equivalence.

Since these equations are true in a Zariski dense subset of $\bar{\mathcal{G}}_r$, which is irreducible, they must be true in all of $\bar{\mathcal{G}}_r$.

Example: Suppose $g_0 = x + 2x^7, g_1 = x + 3x^4 + x^6, g_2 = x^5 + x^6 + x^7, g_3 = x^3 + x^8$;

Is $\langle g \rangle \in \bar{\mathcal{G}}_3$? Let $\alpha = (1, 2, 7, 8)$. Then $p_\alpha(\langle g \rangle) = 2$ so $\langle g \rangle \notin \bar{\mathcal{G}}_3$

One can use the structure of $\mathcal{G}_r$ to gain some insight in the structure of classical complexity classes.

Definition: For a polynomial $f \in \mathbb{F}[x]$ let $L[f]$ the *multiplicative complexity* of f be the length of the shortest computation sequence $\langle g \rangle$ with $f(x) - f(0) \in \langle g \rangle$.

Let $\mathcal{C}_r$ denote the set of univariate polynomials of multiplicative complexity $\leq r$.

Let $\mathcal{C}_r^*$ denote the set of univariate polynomials of multiplicative complexity $\leq r$ with no constant term.

Let $\mathcal{C}_{r,d}$ denote the set of univariate polynomials of multiplicative complexity $\leq r$ and degree $\leq d$.

Let $\mathcal{B}_r$ denote the set of univariate polynomials of multiplicative complexity r , no constant term and degree 2^r .

Proposition:

$$1. \mathcal{C}_r = \bigcup_{d \leq 2^r} \mathcal{C}_{r,d};$$

$$2. \mathcal{C}_r = \mathcal{C}_r^* \times \mathbb{A}^1.$$

Theorem 3: *There is a finite rational correspondence $\mathcal{C}_r^* \rightarrow \mathcal{G}_r$ resulting in a commutative diagram of rational correspondences:*

$$\begin{array}{ccc} \mathcal{C}_r^* & \rightarrow & U \\ \downarrow & & \downarrow \\ \mathcal{G}_r & \rightarrow & G \end{array}$$

To prove this we need several technical results.

Definition: For $i \leq r, j \leq i - 2$ let $N(i, j) = 2^{i-1} - 2^j$.

Lemma 1: Suppose $\langle g \rangle \in \mathcal{U}_r$.

- (i) If $n < N(i, j)$ then $\mathfrak{C}(g_r, 2^r - n)$ is a polynomial in $\{a_{\mathfrak{i}, \mathfrak{j}}, b_{\mathfrak{i}, \mathfrak{j}} \ni N(\mathfrak{i}, \mathfrak{j}) < N(i, j)\}$.
- (ii) If $n = N(i, j)$. Then $\mathfrak{C}(g_r, 2^r - n) = 2^{r-i}(a_{i,j} + b_{i,j}) + \epsilon_{r,n}$ where $\epsilon_{r,n}$ is a polynomial in $\{a_{\mathfrak{i}, \mathfrak{j}}, b_{\mathfrak{i}, \mathfrak{j}} \ni N(\mathfrak{i}, \mathfrak{j}) < N(i, j)\}$

Proof: First assume $i = r$. Then $N(i, j) = 2^{r-1} - 2^j$. Since $g_r = g_{r-1}^2 + \sum_{\mathfrak{i} < r-1} (a_{r,\mathfrak{i}} + b_{r,\mathfrak{i}})g_{r-1}g_{\mathfrak{i}} + \sum_{\mathfrak{i}, \mathfrak{j} < r-1} (a_{r,\mathfrak{i}}b_{r,\mathfrak{j}})g_{\mathfrak{i}}g_{\mathfrak{j}}$, $a_{r,\mathfrak{i}}$ or $b_{r,\mathfrak{i}}$ only appears in $\mathfrak{C}(g_r, 2^r - n)$ via $\mathfrak{C}((a_{r,\mathfrak{i}} + b_{r,\mathfrak{i}})g_{r-1}g_{\mathfrak{i}}, 2^r - n)$ or $\mathfrak{C}((a_{r,\mathfrak{i}}b_{r,\mathfrak{j}})g_{\mathfrak{i}}g_{\mathfrak{j}}, 2^r - n)$. If $n = N(r, j)$ then $2^r - n > \deg(g_{r-1}g_{\mathfrak{j}})$ for $\mathfrak{j} < j$ and $2^r - n > \deg(g_{\mathfrak{i}}g_{\mathfrak{j}})$ so $\mathfrak{C}(g_r, 2^r - n) = \mathfrak{C}(g_{r-1}^2, 2^r - n) + \sum_{\mathfrak{j} \geq j} (a_{r,\mathfrak{j}} + b_{r,\mathfrak{j}})\mathfrak{C}(g_{r-1}g_{\mathfrak{j}}, 2^r - n)$, which proves the lemma in this case. Next observe that for $n < 2^r$ we have $2^{r+1} - n > \deg(g_{\mathfrak{i}}g_{\mathfrak{j}})$ if $\mathfrak{i}, \mathfrak{j} < r - 1$ or $\mathfrak{i} = r - 1, \mathfrak{j} < \mathfrak{i}$. Therefore $\mathfrak{C}(g_{r+1}, 2^{r+1} - n) = \mathfrak{C}(g_r^2, 2^{r+1} - n) = \sum_{\mathfrak{i} \leq n} \mathfrak{C}(g_r, 2^r - \mathfrak{i})\mathfrak{C}(g_r, 2^r - n + \mathfrak{i})$ and the result follows in this fashion by induction.

Definition: For $i \leq r, j \leq i - 2, k \leq j$ let $M(i, j, k) = 2^i - 2^j - 2^k$.

Lemma 2: Suppose $\langle g \rangle \in \mathcal{U}_r$.

- (i) If $n < M(i, i-2, i-2)$ then every occurrence of $a_{i,j}$ or $b_{i,j}$ in $\mathbb{C}(g_r, 2^r - n)$ is as $a_{i,j} + b_{i,j}$.
- (ii) If $M(i, j, k) \leq n < M(i, j, k-1)$ then $\mathbb{C}(g_r, 2^r - n) = \zeta_{r,n}(a_{i,j}b_{i,k} + a_{i,k}b_{i,j}) + \nu_{r,n}$ where $\zeta_{r,n}$ and $\nu_{r,n}$ are polynomials in $\{a_{i,j}, b_{i,j} \text{ with } i < i \text{ or } i = i, j > j \text{ or as } a_{i,j} + b_{i,j} \text{ or } a_{i,j}b_{i,k} \text{ or } a_{i,k}b_{i,j} \text{ with } M(i, j, k) < M(i, j, k)\}$.
- (iii) If $n = M(i, i-2, k)$ with $k < i-2$ then $\zeta_{r,n} = 2^{r-i}$;

Proof: If $i = r$ then $n < M(i, i-2, i-2)$ implies $2^r - n > 2^{r-1}$ and so $\mathbb{C}(g_r, 2^r - n) = \mathbb{C}(g_{r-1}^2, 2^r - n) + \Sigma_j(a_{r,j} + b_{r,j})\mathbb{C}(g_{r-1}g_j, 2^r - n)$, which proves (i) in this case.

If $M(r, j, k) \leq n < M(r, j, k-1)$ then $2^j + 2^{k-1} \leq 2^r - n < 2^j + 2^k$ and so $\mathbb{C}(g_r, 2^r - n) = \mathbb{C}(g_{r-1}^2, 2^r - n) + \Sigma_j(a_{r,j} + b_{r,j})\mathbb{C}(g_{r-1}g_j, 2^r - n) + (a_{r,j}b_{r,k} + a_{r,k}b_{r,j}) + \Sigma_{2^j+2^k < 2^j+2^k} \mathbb{C}(g_jg_k, 2^r - n)$, which shows (ii) and (iii) in this case. Now suppose the lemma is true for i and r with $i \leq r$ and consider $g_{r+1} = g_r^2 + \Sigma_{i < r}(a_{r+1,i} + b_{r+1,i})g_rg_i + \Sigma_{i,j < r}(a_{r+1,i}b_{r+1,j})g_ig_j$. Then $2^{r+1} - M(i, i-2, i-2) > \deg(g_rg_j)$ and so if $n < M(i, i-2, i-2)$ we have $\mathbb{C}(g_{r+1}, 2^{r+1} - n) = \mathbb{C}(g_r^2, 2^{r+1} - n) = \Sigma_{i \leq n} \mathbb{C}(g_r, 2^r - i)\mathbb{C}(g_r, 2^r - n + i)$ and so (i) and (iii) follows by induction.

If $M(i, j, k) \leq n < M(i, j, k-1)$ then $2^{r+1} - n > \deg(g_rg_j)$ so once again $\mathbb{C}(g_{r+1}, 2^{r+1} - n) = \Sigma_{i \leq n} \mathbb{C}(g_r, 2^r - i)\mathbb{C}(g_r, 2^r - n + i)$ and (ii) then follows by induction.

Proof of theorem: Suppose that $f \in \mathcal{B}_r$. Suppose also that initially the parameters $a_{i,j}, b_{i,j}, c_i$ are all indeterminate. By using the lemmas and the fact that if $f \in \langle g \rangle$ then $\mathbb{C}(g_r, 2^r - n) = \mathbb{C}(f, 2^r - n)$ for $n < 2^{r-1}$ we obtain constraints on the parameters $a_{i,j}, b_{i,j}$ that are sufficient to establish the theorem.

Define a series of specializations:

1. For $2 \leq r, 0 \leq j \leq i-2$ let $n = N(i, j), B_n : b_{i,j} \rightsquigarrow -a_{i,j} + 2^{i-r}(\mathbb{C}(f, 2^r - n) - \epsilon_{r,n})$. Then Lemma 1 implies $\mathbb{C}(g_r, 2^r - n) \rightsquigarrow \mathbb{C}(f, 2^r - n)$ and that $\epsilon_{r,n}$ is a rational function of $\{a_{i,j}, b_{i,j} \ni N(i, j) < N(i, j)\}$, i.e. either $i < i$ or $i = i$ and $0 \leq j < j$.

2. Define a nested loop of specializations. For $2 \leq i \leq r-1, 0 \leq j \leq i-2$ proceed as follows : let $n = M(i, i-2, j), n1 = N(i, j), n2 = N(i, i-2)$ and $B_n : a_{i,j} \rightsquigarrow$

$$-2^{i-r-1} \left(\frac{\mathbb{C}(f, 2^r - n) - \mathbb{C}(f, 2^r - n1) - \mathbb{C}(f, 2^r - n2) + \epsilon_{r,n1} + \epsilon_{r,n2} + \nu_{r,n}}{a_{i,i-2}} \right)$$

$\mathbb{C}(g_r, 2^r - n) \rightsquigarrow \mathbb{C}(f, 2^r - n)$ and Lemma 1 implies that $\epsilon_{r,N(i,j)}, \epsilon_{r,N(i,i-2)}$ are rational functions of $\{a_{i,j}, b_{i,j} \ni N(i, j) < N(i, j)\}$. Lemma 2 implies $\nu_{r,n}$ is a rational function of $\{a_{i,j}, b_{i,j} \text{ with } i < i \text{ or } i = i, j > j \text{ or } a_{i,k}, b_{i,j} \text{ with } M(i, j, k) < M(i, j, k)\}$. In all cases these are functions of $a_{i,j}, b_{i,j}$ with $i \leq i$.

Note that the specializations can never overwrite each other. After the specializations

described in part 1 $\mathbb{C}(g_r, 2^r - n)$ is a function only of the parameters $a_{i,j}$, $2 \leq i \leq r - 1$ for $n < 2^{r-1}$. After an outer loop of specializations in part 2 is completed it is clear that $\mathbb{C}(g_r, 2^r - n)$ is a function only of $a_{2,0}, a_{3,1}, \dots, a_{i,i-2}$ for $n \leq M(i, i-2, i-2)$ and that $a_{i,j}$ is a function of $a_{2,0}, a_{3,1}, \dots, a_{i,i-2}$ for $j < i - 2$. Assuming that one solves for the parameters $a_{2,0}, \dots, a_{i-1,i-3}$ in equations $\mathbb{C}(g_r, 2^r - n) = \mathbb{C}(f, 2^r - n)$, $n < M(i, i-2, i-2)$ one obtains a system of equations $\mathbb{C}(g_r, 2^r - n) = \mathbb{C}(f, 2^r - n)$, $M(i, i-2, i-2) < n < M(i+1, i-1, i-2)$ which depends solely on $a_{i,i-2}$. This shows that for $f \in \mathcal{B}_r$ there are finite many parameter sets $a_{i,j}, b_i, j \ni i \leq r-1, j \leq i-2$ with $f \in \langle g_0, \dots, g_{r-1}, g_r \rangle$ some g_r . But then the proof of Theorem 1 shows that there are at most two possible polynomials g_r that go with f and $a_{i,j}, b_i, j \ni i \leq r-1, j \leq i-2$. This establishes the theorem.

Theorem 4: $\mathcal{C}_r$ is a Zariski dense subset of an irreducible variety of dimension r^2

Proof: Define a rational map $\mathbb{A}^{1+(r+1)^2} \rightarrow \mathbb{A}^{1+2^r}$ by $\{a_{i,j}, b_{i,j}, c_i\} \mapsto (\mathbb{C}(f, n))_n$ where $g_i = (a_i \cdot \bar{g}_i) * (b_i \cdot \bar{g}_i)$, $f = f(0) + \sum_i c_i g_i$. Since $\mathbb{A}^{1+(r+1)^2}$ is irreducible, so is the closure of its image. $\mathcal{C}_r$ lies in the image of this map and is clearly Zariski dense in it. The dimension claims follows from the previous theorem.

Questions: 1. When is the correspondence $\mathcal{C}_r^* \rightarrow \mathcal{G}_r$ a rational map? In other words does a generic polynomial have an unique computation sequence associated to it? This is true for f with $L[f] = 4$ but not true if $L[f] = 3$.

2. When does this correspondence break down? For *generic* f with $L[f] = 4$, there is a unique computation sequence, but what are the conditions when this is not the case?

3. How can conditions for sets of polynomials to be computation sequences be used to construct necessary conditions for a polynomial to have low complexity? In other words how do we use defining relations for $\mathcal{G}_r$ to obtain defining relations for $\mathcal{C}_{r,d}$?

References:

1. Bürgisser, Peter; Clausen, Michael; Shokrollahi, M. Amin (1997). Algebraic complexity theory. Grundlehren der Mathematischen Wissenschaften. Vol. 315. With the collaboration of Thomas Lickteig. Berlin: Springer-Verlag. ISBN 978-3-540-60582-9. Zbl 1087.68568.
2. Paterson, Michael S.; Stockmeyer, Larry J. (1973). "On the Number of Nonscalar Multiplications Necessary to Evaluate Polynomials". SIAM Journal on Computing. 2 (1): 60–66. doi:10.1137/0202007.
3. Bruns, Winfried; Vetter, Udo (1988). Determinantal rings. Lecture Notes in Mathematics. Vol. 1327. Springer-Verlag. doi:10.1007/BFb0080378. ISBN 978-3-540-39274-3.
4. Cook, Stephen (1971). "The complexity of theorem proving procedures". Proceedings of the Third Annual ACM Symposium on Theory of Computing. pp. 151–158. doi:10.1145/800157.805047. ISBN 9781450374644. S2CID 7573663.

5. Griffiths, Phillip; Harris, Joseph (1994), Principles of algebraic geometry, Wiley Classics Library (2nd ed.), New York: John Wiley and Sons, p. 211, ISBN 0-471-05059-8, MR 1288523, Zbl 0836.14001.
6. Kleiman, S. and Laksov, D. "Schubert Calculus." Amer. Math. Monthly 79, 1061-1082, 1972.
7. Hriljac, P. "Some NP Complete Problems Based on Algebra and Algebraic Geometry", Proceedings of the Symposia on Groups, Algebras, Languages and Related Areas in Computer Science, RIMS 2024.

Acknowledgements: The author wishes to thank RIMS for hosting this symposium and providing support, Szilard Fazekas for running it, and Tsunekazu Nishinaka and Hisa Tsutsui for facilitating my attendance.