PROBABILISTIC SATURATIONS AND ALT'S PROBLEM

JONATHAN D. HAUENSTEIN AND MARTIN HELMER

Abstract. Alt's problem, formulated in 1923, is to count the number of four-bar linkages whose coupler curve interpolates nine general points in the plane. This problem can be phrased as counting the number of solutions to a system of polynomial equations which was first solved numerically using homotopy continuation by Wampler, Morgan, and Sommese in 1992. Since there is still not a proof that all solutions were obtained, we consider upper bounds for Alt's problem by counting the number of solutions outside of the base locus to a system arising as the general linear combination of polynomials. In particular, we derive effective symbolic and numeric methods for studying such systems using probabilistic saturations that can be employed using both finite fields and floating-point computations. We give bounds on the size of finite field required to achieve a desired level of certainty. These methods can also be applied to many other problems where similar systems arise such as computing the volumes of Newton-Okounkov bodies and computing intersection theoretic invariants including Euler characteristics, Chern classes, and Segre classes.

1. Introduction

In 1923, Alt [3] realized that finitely many four-bar planar linkages (see Figure 1) can be constructed whose coupler curve interpolates nine general points in the plane. Since he could not determine the exact number himself, he left this as an open problem which was solved numerically using homotopy continuation nearly 70 years later by Wampler, Morgan, and Sommese [40]. In particular, they showed that there are 1442 distinct four-bar coupler curves which pass through nine general points which, together with Roberts cognates [35], yields 4326 distinct four-bar linkages. Although this computation has been repeatedly confirmed using various homotopy continuation methods, e.g., [5, 12, 21, 22, 34, 38], these numerical computations do not preclude the existence of additional solutions. In fact, one of the distinct four-bar linkages was missed by the homotopy continuation solver in [40] but was reconstructed using the cognate formula. Since a sharp upper bound has not yet been established, we aim to derive such an upper bound by considering a generalization of Alt's problem which arises by counting the number of solutions outside of the base locus to a system of polynomials arising from a general linear combination of given polynomials.

Although formulating an upper bound on Alt's problem in this fashion is new, the idea of constructing polynomial systems from randomly generated polynomials which have finitely-many solutions is not new. For example, the volume of Newton-Okounkov bodies [26, 27, 32] (which generalize the volume of Newton polytopes [9] in the monomial case) correspond with the number of solutions to such systems. Homotopies utilizing this structure have also been proposed [28] and comparisons between homotopy continuation and modular Gröbner basis methods have been performed [6]. Moreover, aspects of this problem have also been considered in the context of computing Euler characteristics [25, 29] and Segre classes [19, 24]. In addition to formulating an upper bound on Alt's problem, the other novelty of our approach is to provide various probabilistic features of an effective algorithmic solution via modular Gröbner basis computations. We incorporate ideas used in the Gröbner trace algorithm [39] and other modular algorithms for Gröbner basis computation such as [4].

The rest of the paper is structured as follows. Section 2 formulates the problem and provides necessary background. Section 3 compares Hilbert functions computed using numerical methods and symbolic methods. Section 4 analyses the probability that randomly selected constants are general. Section 5 describes the results of some computational experiments and the paper ends with a summary of our results in the context of Alt's problem in Section 6.

2. Formulation

For a system of polynomials in $\mathbb{C}[x_1, \ldots, x_n]$, say

$$f(x) = \begin{bmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_r(x) \end{bmatrix}, \tag{1}$$

define

$$\mathcal{V}(f) = \{x \in \mathbb{C}^n \mid f(x) = 0\}.$$

For $X = \mathcal{V}(f)$ and an integer $i = 0, \ldots, n-1$, we seek to compute

$$g_i(X, \mathbb{C}^n) = \deg\left(\mathcal{V}(\Theta \cdot x - \mathbf{1}, \Lambda \cdot f) \setminus X\right) \tag{2}$$

where $\Theta \in \mathbb{C}^{i \times n}$ and $\Lambda \in \mathbb{C}^{(n-i) \times r}$ are general, and $\mathbf{1}$ is the length i vector where each entry is 1. That is, we aim to count the number of solutions to a system of i general affine linear polynomials and $n - i$ general linear combinations of $f_1, \ldots, f_r$ outside of the base locus X.

One approach for enforcing the solutions be outside of the base locus X is via the Rabinowitz trick. That is, one introduces a new variable T and, for $\mu \in \mathbb{C}^r$ general, we have

$$g_i(X, \mathbb{C}^n) = \deg(\mathcal{V}(\Theta \cdot x - 1, \Lambda \cdot f, 1 - (\mu \cdot f)T)).$$

Example 2.1. To illustrate, consider $f(x) = [x_1, x_2, x_1x_2^2, x_1^3x_2^2]^T$ consisting of $r = 4$ polynomials in $n = 2$ variables. Clearly, $\mathcal{V}(f) = \{(0, 0)\}$. Letting $\Box$ represent a general number,

$$g_1(X, \mathbb{C}^2) = \deg(\mathcal{V}(\Box x_1 + \Box x_2 - 1, \Box x_1 + \Box x_2 + \Box x_1x_2^2 + \Box x_1^3x_2^2) \setminus X) = 5$$

since there are 5 points of intersection, all of which are away from the origin, between a general affine line and an irreducible quintic curve. Additionally,

$$g_0(X, \mathbb{C}^2) = \deg(\mathcal{V}(\Box x_1 + \Box x_2 + \Box x_1x_2^2 + \Box x_1^3x_2^2, \Box x_1 + \Box x_2 + \Box x_1x_2^2 + \Box x_1^3x_2^2) \setminus X) = 6$$

since the two irreducible quintic curves intersect in 7 points, one of which is the origin. Since f consists of monomials, these values can be computed via mixed volume computations, e.g., [9].

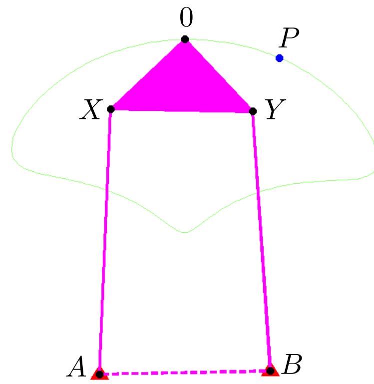

FIGURE 1. A four-bar linkage with corresponding coupler curve

2.1. **Relation to Alt's problem.** A four-bar linkage is the simplest moveable planar closed-chain linkage, one of which is shown in Figure 1 together with part of the coupler curve that it traces out. Without loss of generality, we can assign the origin 0 to be a point on the coupler curve and describe a four-bar linkage using 4 points in the plane: A, B, X, and Y. The points A and B correspond with the two fixed pivots while the segment XY is the so-called floating link. Since the 4 planar points constitute $n = 8$ design parameters, Alt realized that one can additionally specify 8 general points resulting in finitely many four-bar linkages whose coupler curve passes through all nine specified points, i.e., the origin and 8 others.

We proceed with a formulation inspired by [36, 40]. Utilizing isotropic coordinates, we write $A = (a, \bar{a})$, $B = (b, \bar{b})$, $X = (x, \bar{x})$, and $Y = (y, \bar{y})$ so that the eight design parameters are $a, \bar{a}, b, \bar{b}, x, \bar{x}, y, \bar{y}$. A point P on the coupler curve will be denoted $P = (p, \bar{p})$. Isotropic coordinates yield a natural action applied to polynomials, denoted conj(), that simply swaps z and $\bar{z}$. In particular, given design parameters $(a, \bar{a}, b, \bar{b}, x, \bar{x}, y, \bar{y})$, the coupler curve traced out by the corresponding four-bar linkage is $\mathcal{V}(G) \subset \mathbb{C}^2$ where

$$G = \sum_{j=1}^{15} c_j(p, \bar{p}) \cdot f_j(a, \bar{a}, b, \bar{b}, x, \bar{x}, y, \bar{y})$$

with

$$\begin{array}{lllll} c_1 = p^3\bar{p}^3, & c_2 = p^3\bar{p}^2, & c_3 = \mathrm{conj}(c_2), & c_4 = p^3\bar{p}, & c_5 = \mathrm{conj}(c_4), \\ c_6 = p^3, & c_7 = \mathrm{conj}(c_6), & c_8 = p^2\bar{p}^2, & c_9 = p^2\bar{p}, & c_{10} = \mathrm{conj}(c_9), \\ c_{11} = p^2, & c_{12} = \mathrm{conj}(c_{11}), & c_{13} = p\bar{p}, & c_{14} = p, & c_{15} = \mathrm{conj}(c_{14}), \end{array}$$

and

$$\begin{aligned} f_1 &= (x - y)(\bar{y} - \bar{x}), \\ f_2 &= (x - y)(\bar{a}\bar{x} - 2\bar{a}\bar{y} + 2\bar{b}\bar{x} - \bar{b}\bar{y}), \\ f_3 &= \mathrm{conj}(f_2), \\ f_4 &= (x - y)(\bar{a}^2\bar{y} - 2\bar{a}\bar{b}\bar{x} + 2\bar{a}\bar{b}\bar{y} - \bar{b}^2\bar{x}), \\ f_5 &= \mathrm{conj}(f_4), \end{aligned}$$

$$
\begin{aligned}
f_6 &= \bar{a}\bar{b}(x-y)(\bar{b}\bar{x}-\bar{a}\bar{y}),\\
f_7 &= \mathrm{conj}(f_6),\\
f_8 &= x^2\bar{y}(\bar{a}-\bar{y})+\bar{x}^2y(a-y)+x\bar{x}(2y\bar{x}+(\bar{a}-2\bar{b})y+(a-2b)\bar{y}-a\bar{a}-2a\bar{b}-2\bar{a}b-2b\bar{b})\\
&\quad+x(b\bar{y}^2+y\bar{y}(\bar{b}-2\bar{a})+\bar{y}(a\bar{a}+a\bar{b}+4\bar{a}b+b\bar{b}))-y\bar{y}(2a\bar{a}+2a\bar{b}+2\bar{a}b+b\bar{b})\\
&\quad+\bar{x}(\bar{b}y^2+y\bar{y}(b-2a)+y(a\bar{a}+\bar{a}b+4a\bar{b}+b\bar{b})),\\
f_9 &= \bar{a}x^2\bar{y}(2\bar{y}-\bar{a}-\bar{b})+2\bar{b}\bar{x}^2y(y-a)-\bar{a}x\bar{y}(a\bar{b}+2\bar{a}(b-y)+2b(\bar{b}+\bar{y}))\\
&\quad+x\bar{x}(\bar{b}(2\bar{b}y+2a\bar{a}+2\bar{a}b+a\bar{b})+\bar{y}(\bar{a}+\bar{b})(2b-a-2y))+\bar{a}y\bar{y}(2a\bar{b}+\bar{a}b+2b\bar{b})\\
&\quad+\bar{x}y((2a\bar{y}-2a\bar{b}-b\bar{y}-\bar{b}y)(\bar{a}+\bar{b})-\bar{a}b\bar{b}),\\
f_{10} &= \mathrm{conj}(f_9),\\
f_{11} &= \bar{a}^2x^2\bar{y}(\bar{b}-\bar{y})+\bar{b}^2\bar{x}^2y(a-y)-\bar{a}\bar{b}x\bar{x}(a(\bar{b}-\bar{y})+2\bar{y}(b-y)+\bar{b}y)+\bar{a}^2x\bar{y}(b\bar{b}+b\bar{y}-\bar{b}y)\\
&\quad+\bar{a}\bar{b}\bar{x}y(\bar{b}(a+y)+\bar{y}(b-2a))-\bar{a}^2b\bar{b}y\bar{y},\\
f_{12} &= \mathrm{conj}(f_{11}),\\
f_{13} &= \bar{a}x^2\bar{y}(\bar{a}(2b-y)+b(\bar{b}-3\bar{y})+\bar{b}y)+a\bar{x}^2y(a(2\bar{b}-\bar{y})+\bar{b}(b-3y)+b\bar{y})\\
&\quad+x\bar{x}(\bar{b}y^2(\bar{a}-\bar{b})+3y\bar{y}(a\bar{b}+\bar{a}b)+b\bar{y}^2(a-b)-\bar{b}y(\bar{a}b+2a\bar{b})-b\bar{y}(a\bar{b}+2\bar{a}b)-2a\bar{a}b\bar{b})\\
&\quad+\bar{a}x\bar{y}(a(b\bar{b}+b\bar{y}-\bar{b}y)+b(\bar{a}(b-2y)+2b\bar{y}))+a\bar{x}y(\bar{a}(b\bar{b}-b\bar{y}+\bar{b}y)\\
&\quad+\bar{b}(a(\bar{b}-2\bar{y})+2\bar{b}y))-2a\bar{a}b\bar{b}y\bar{y},\\
f_{14} &= (\bar{a}bx\bar{y}-a\bar{b}\bar{x}y)((\bar{a}-\bar{x})(\bar{b}y-b\bar{y})+(\bar{b}-\bar{y})(a\bar{x}-\bar{a}x)),\\
f_{15} &= \mathrm{conj}(f_{14}).
\end{aligned}
$$

In fact, the map from design parameters to coupler curves is generically a 6-to-1 map. First, there is a trivial order 2 action of relabeling, namely the design parameters

$$(a,\bar{a},b,\bar{b},x,\bar{x},y,\bar{y}) \quad \text{and} \quad (b,\bar{b},a,\bar{a},y,\bar{y},x,\bar{x})$$

yield the same coupler curve and actually describe the same mechanism. Additionally, there is an order 3 action of Roberts cognates, e.g., see [40, Eq. 17], which yield distinct mechanisms that correspond to the same coupler curve.

Returning to Alt's problem, suppose that $(p_i,\bar{p}_i)$ for $i=1,\dots,8$ are general. Thus, one aims to find the design parameters $(a,\bar{a},b,\bar{b},x,\bar{x},y,\bar{y})$ such that, for $i=1,\dots,8$, $(p_i,\bar{p}_i)$ lies on its coupler curve. Hence, for $i=1,\dots,8$ and

$$G_i=\sum_{j=1}^{15} c_j(p_i,\bar{p}_i)\cdot f_j(a,\bar{a},b,\bar{b},x,\bar{x},y,\bar{y}),$$

Alt's problem of counting the number of distinct mechanisms is equal to one-half of the number of isolated points in $\mathcal{V}(G_1,\dots,G_8)$ while the number of distinct coupler curves is equal to one-sixth of the number of isolated points in $\mathcal{V}(G_1,\dots,G_8)$. The homotopy continuation computation first described in [40] provides that the number of isolated points in $\mathcal{V}(G_1,\dots,G_8)$ is (at least) 8652.

We obtain an upper bound on the number of isolated points in $\mathcal{V}(G_1,\dots,G_8)$ by replacing each coefficient $c_j(p_i,\bar{p}_i)$ with an independent parameter, say c_{ij}. The number of isolated solutions to the resulting system is exactly $g_0(X,\mathbb{C}^n)$ from (2) where $X=\mathcal{V}(f_1,\dots,f_{15})$. In fact, it is easy to verify that X is the union of the following 7 linear spaces:

$$
\begin{array}{llll}
\mathcal{V}(x,y), & \mathcal{V}(x-y,x-b,a-b), & \mathcal{V}(x-y,a-b,\bar{x}-\bar{a},\bar{y}-\bar{b}), & \mathcal{V}(x-y,\bar{x}-\bar{y},a-b,\bar{a}-\bar{b}),\\
\mathcal{V}(\bar{x},\bar{y}), & \mathcal{V}(\bar{x}-\bar{y},\bar{x}-\bar{b},\bar{a}-\bar{b}), & \mathcal{V}(\bar{x}-\bar{y},\bar{a}-\bar{b},x-a,y-b). &
\end{array}
\tag{3}
$$

Note that each of these correspond to degenerate linkages that are not of interest. Therefore, $g_0(X, \mathbb{C}^8)/2$ is an upper bound on the number of distinct four-bar linkages whose coupler curve interpolates 9 general points. Similarly, $g_0(X, \mathbb{C}^8)/6$ is an upper bound on the number of distinct coupler curves which interpolate 9 general points. In addition, one naturally has a coefficient-parameter homotopy [30] for computing a superset of the isolated points of $\mathcal{V}(G_1, \ldots, G_8)$ by simply deforming the coefficients c_{ij} to $c_j(p_i, \bar{p}_i)$.

For $i = 1, \ldots, 7$, the number $g_i(X, \mathbb{C}^8)$ is an upper bound on the degree of the set of four-bar linkages whose coupler curve interpolates $9 - i$ general points, a variety that has dimension i. The degrees of these problems were first reported in [12, Table 1] and are displayed in Table 2. Similar to the results of [40] the computations in [12] do not prove that the degrees can be no larger than the values in Table 2 and we will use modular methods to provide a (probabilistic) confirmation of these values.

2.2. **Relation to projective degrees and characteristic classes.** For $X = \mathcal{V}(f)$, we may also view each $g_i(X, \mathbb{C}^n)$ as the degree of the pullbacks of general linear spaces under a certain rational map. Consider the rational map

$$\begin{aligned} \rho\colon \mathbb{C}^n &\dashrightarrow \mathbb{C}^r \\ x &\mapsto f(x) \end{aligned} \tag{4}$$

and let $\mathcal{L}_i \subset \mathbb{C}^r$ be a general linear space passing through the origin of dimension $r - (n - i)$ in $\mathbb{C}^r$, i.e., having codimension $n - i$ in $\mathbb{C}^r$. Let $B_{n-i} \in \mathbb{C}^{(n-i)\times r}$ be a matrix such that $\mathcal{L}_i = \mathrm{null}(B_{n-i})$. Then,

$$g_i(X, \mathbb{C}^n) = \deg(\rho^{-1}(\mathcal{L}_i) \setminus X) = \deg(\mathcal{V}(B_{n-i} \cdot f) \setminus X).$$

The number $g_0(X, \mathbb{C}^n)$ is also the volume of the Newton-Okounkov body [26, 27, 32] corresponding to f.

More generally, if $X = \mathcal{V}(F) \subset Y$ are subschemes inside of Z, which is a product of affine and projective spaces, and $F(x)$ is a collection of r polynomials in the coordinate ring of Z, we can consider the map

$$\begin{aligned} \rho_X\colon Y &\dashrightarrow \mathbb{C}^r \\ x &\mapsto F(x). \end{aligned} \tag{5}$$

In this case, we wish to compute the numbers

$$g_i(X, Y) = \deg(\rho_X^{-1}(\mathcal{L}_i) \setminus X) = \deg\left(Y \cap \mathcal{V}(B_{n-i} \cdot F) \setminus X\right). \tag{6}$$

If Z is a projective variety, then the polynomials making up F are homogeneous, $\mathbb{C}^r$ is replaced by $\mathbb{P}^{r-1}$, a set of polynomials defining $X = \mathcal{V}(F)$ can be taken to have the same degree (without changing $X \subset Z$), and the numbers $g_i(X, Y)$ are the *projective degrees* of X in Y (see [19] for the general case as well as [20, Example 19.4] and [24, 25] for the special case $g_i(X, \mathbb{P}^{n-1})$). Moreover, it is shown in [24] that when X is a subscheme of $\mathbb{P}^{n-1}$, the (pushforward of the) Chern-Schwartz-McPherson class in the Chow ring $A^*(\mathbb{P}^{n-1})$, namely $c_{SM}(X)$, and hence the topological Euler characteristic, namely $\chi(X)$, are completely determined by appropriate projective degrees. Note that this also gives (the pushforward of) the Chern class of the tangent bundle, $c(T_X) \cap [X] \in A^*(\mathbb{P}^{n-1})$, since this agrees with $c_{SM}(X)$ whenever X is smooth, i.e., whenever the Chern class is defined. For more details, see [2, §2.2]. Similarly, if $X \subset Y$ are subschemes of a smooth projective toric variety T, it is shown in [19] that the projective degrees $g_i(X,Y)$ completely determine the (pushforward of the) Segre class of X in Y, namely $s(X,Y)$, in the Chow ring $A^*(T)$. This Segre class in turn gives rise to many other invariants of potential interest such as Samuel's algebraic multiplicity of Y along X, namely $e_X Y$, e.g., see [15, §4.3] and [19, §5], and polar classes, e.g., see [15, Ex. 4.4.5]. These Segre classes have also been used to give a Gröbner free test of pairwise containment of projective varieties, e.g., see [19, §6].

2.3. **Plane conics.** To illustrate several possible situations, we consider the enumerative geometry problem of counting the number of plane conics in $\mathbb{C}^3$ passing through the origin and meeting 6 general lines. First, we associate a plane conic $C \subset \mathbb{C}^3$ passing through the origin with $(a,b) \in \mathbb{P}^4 \times \mathbb{P}^2$ where

$$C = \mathcal{V}(a_0x^2 + a_1xy + a_2y^2 + a_3x + a_4y, b_0z + b_1x + b_2y).$$

We parameterize the 6 lines by $v_i + tw_i$ where $v_i, w_i \in \mathbb{C}^3$ are general for $i = 1, \ldots, 6$. Then, the enumerative geometry problem is to count the number of isolated points in $\mathcal{V}(G_1, \ldots, G_6)$, which is 18, where $G_i = \sum_{j=1}^{14} c_j(v_i, w_i) \cdot f_j(a,b)$ with

$$\begin{array}{lcllcl}
c_1 & = & (v_1w_3 - v_3w_1)^2 & c_2 & = & (v_2w_3 - v_3w_2)(v_1w_3 - v_3w_1) \\
c_3 & = & (v_2w_3 - v_3w_2)^2 & c_4 & = & w_3(v_1w_3 - v_3w_1) \\
c_5 & = & w_3(v_2w_3 - v_3w_2) & c_6 & = & w_1(v_1w_3 - v_3w_1) \\
c_7 & = & 2v_1w_2w_3 - v_2w_1w_3 - v_3w_1w_2 & c_8 & = & 2v_2w_1w_3 - v_1w_2w_3 - v_3w_1w_2 \\
c_9 & = & w_2(v_2w_3 - v_3w_2) & c_{10} & = & (v_3w_1 - v_1w_3)(v_1w_2 - v_2w_1) \\
c_{11} & = & (v_2w_3 - v_3w_2)(v_1w_2 - v_2w_1) & c_{12} & = & w_1(v_2w_1 - v_1w_2) \\
c_{13} & = & w_2(v_2w_1 - v_1w_2) & c_{14} & = & (v_1w_2 - v_2w_1)^2,
\end{array}$$

and

$$\begin{array}{lcllcl}
f_1 & = & a_0b_0^2 & f_2 & = & a_1b_0^2 \\
f_3 & = & a_2b_0^2 & f_4 & = & a_3b_0^2 \\
f_5 & = & a_4b_0^2 & f_6 & = & a_3b_0b_1 \\
f_7 & = & a_3b_0b_2 & f_8 & = & a_4b_0b_1 \\
f_9 & = & a_4b_0b_2 & f_{10} & = & b_0(a_1b_1 - 2a_0b_2) \\
f_{11} & = & b_0(a_1b_2 - 2a_2b_1) & f_{12} & = & b_1(a_4b_1 - a_3b_2) \\
f_{13} & = & b_2(a_4b_1 - a_3b_2) & f_{14} & = & a_0b_2^2 + a_2b_1^2 - a_1b_1b_2.
\end{array}$$

For $F = [f_1, \ldots, f_{14}]^T$ and $Y = Z = \mathbb{P}^4 \times \mathbb{P}^2$, we have

$$X = \mathcal{V}(F) = \mathcal{V}(b_0, a_4b_1 - a_3b_2, a_2b_1^2 - a_1b_1b_2 + a_0b_2^2, a_2a_3b_1 - a_1a_3b_2 + a_0a_4b_2, a_2a_3^2 - a_1a_3a_4 + a_0a_4^2)$$

which corresponds with planes $\mathcal{V}(b_1x + b_2y)$ that are not of interest. In fact, $g_0(X,Y) = 18$ providing a sharp upper bound on the number of isolated points in $\mathcal{V}(G_1, \ldots, G_6)$.

Alternatively, we could work on the affine patch $Y = \mathbb{C}^4 \times \mathbb{C}^2 = \mathbb{C}^6$ defined by $a_0 = b_0 = 1$, i.e., plane cubics defined by

$$\mathcal{V}(x^2 + a_1xy + a_2y^2 + a_3x + a_4y, z + b_1x + b_2y).$$

Hence,

$$F = [1, a_1, a_2, a_3, a_4, a_3b_1, a_3b_2, a_4b_1, a_4b_2, a_1b_1 - 2b_2, \\ a_1b_2 - 2a_2b_1, b_1(a_4b_1 - a_3b_2), b_2(a_4b_1 - a_3b_2), a_2b_1^2 - a_1b_1b_2 + b_2^2]^T \tag{7}$$

with $X = \mathcal{V}(F) = \emptyset$ and $g_0(X, Y) = 18$, which we will verify in Section 3.3.

Finally, one could work on $Y = \mathbb{P}^6$, i.e., plane cubics defined by

$$\mathcal{V}(a_0x^2 + a_1xy + a_2y^2 + a_3x + a_4y, a_0z + b_1x + b_2y),$$

with

$$F = [a_0^3, a_0^2a_1, a_0^2a_2, a_0^2a_3, a_0^2a_4, a_0a_3b_1, a_0a_3b_2, a_0a_4b_1, a_0a_4b_2, a_0(a_1b_1 - 2a_0b_2), \\ a_0(a_1b_2 - 2a_2b_1), b_1(a_4b_1 - a_3b_2), b_2(a_4b_1 - a_3b_2), a_2b_1^2 - a_1b_1b_2 + b_2^2]^T$$

so that

$$X = \mathcal{V}(F) = \mathcal{V}(a_0, a_4b_1 - a_3b_2, a_2b_1 - a_1b_2, a_2a_3 - a_1a_4) \cup \mathcal{V}(a_0, b_1, b_2) \cup \mathcal{V}(a_0, a_3, b_1),$$

which all correspond to degenerate cases that are not of interest, and $g_0(X, Y) = 18$.

3. Verification using Hilbert functions

For homogeneous ideals, modular computations can be utilized to provide upper bounds on the Hilbert function [4, Thm. 5.3]. However, since the ideals of particular interest are parameterized ideals which are generically radical and zero-dimensional but need not be homogeneous, this section compares affine Hilbert functions computed using numerical methods (yielding lower bounds) and symbolic methods (yielding upper bounds). In particular, when the upper and lower bounds agree, one has computed the generic value of the Hilbert function.

Consider the field $\mathfrak{K} = \mathbb{Q}(p_1, \ldots, p_\ell)$ consisting of rational functions in the parameters $p = (p_1, \ldots, p_\ell)$ with rational coefficients. Let $R = \mathfrak{K}[x_1, \ldots, x_n]$ be the ring of polynomials in the variables $x_1, \ldots, x_n$ whose coefficients are in $\mathfrak{K}$. Fix $p^* = (p_1^*, \ldots, p_\ell^*) \in \mathbb{C}^\ell$. For a polynomial $h \in R$, let $h_{p^*} \in \mathbb{C}[x_1, \ldots, x_n]$ be the polynomial obtained by specializing the parameters p to p^* whenever all coefficients of h are defined at p^*. Suppose that $h_1, \ldots, h_n \in R$ generate an ideal $I = \langle h_1, \ldots, h_n \rangle \subset R$ that is generically radical and zero-dimensional. That is, for general values $p^* \in \mathbb{C}^\ell$, $I_{p^*} = \langle h_{1p^*}, \ldots, h_{np^*} \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$ with $\#\mathcal{V}(I_{p^*}) = \deg I_{p^*} < \infty$.

For $d \geq 0$, let $R_{\leq d}$ and $I_{\leq d}$ denote the vector space over $\mathfrak{K}$ of polynomials in R and I, respectively, of degree at most d. In particular, $\dim_{\mathfrak{K}}(R_{\leq d}) = \binom{n+d}{d}$. The *affine Hilbert function* of I is the function $\mathrm{HF}_I : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ defined by

$$\mathrm{HF}_I(d) := \dim_{\mathfrak{K}}(\mathfrak{K}[x_1, \ldots, x_n]_{\leq d}) - \dim_{\mathfrak{K}}(I_{\leq d}) = \binom{n+d}{d} - \dim_{\mathfrak{K}}(I_{\leq d}). \tag{8}$$

Moreover, for general $p^* \in \mathbb{C}^\ell$,

$$\mathrm{HF}_{I_{p^*}}(d) := \binom{n+d}{d} - \dim_{\mathbb{C}}((I_{p^*})_{\leq d}) = \mathrm{HF}_I(d).$$

3.1. **Numerical Hilbert functions.** With the setup described above, we develop a certified approach for computing lower bounds on the Hilbert function of I that combines [17] with a method that guarantees the existence of a solution to a polynomial system, one such approach being α-theory [10, Ch. 8]. We first introduce the exact computation followed by the certified numerical approach for computing lower bounds using a well-constrained system.

Suppose that $p^* \in \mathbb{C}^\ell$ and $V_{p^*} = \{q_1^*, \ldots, q_k^*\} \subset \mathcal{V}(h_{1p^*}, \ldots, h_{np^*}) \subset \mathbb{C}^n$ consists of nonsingular solutions. Let $I(V_{p^*}) \subset \mathbb{C}[x_1, \ldots, x_n]$ be the ideal of polynomials vanishing on V_{p^*}. By the implicit function theorem, each point $q_i^* \in V_{p^*}$ lifts locally to a solution in $\mathcal{V}(I)$, say $q_i(p)$ with $q_i^* = q_i(p^*)$.

Let $\nu_d : \mathbb{C}^n \to \mathbb{C}^{\binom{n+d}{d}}$ be the degree $\le d$ Veronese embedding, i.e.,

$$\nu_d(x) = \begin{bmatrix} 1 & x_1 & \cdots & x_n & x_1^2 & x_1x_2 & \cdots & x_n^2 & \cdots & x_1^d & x_1^{d-1}x_2 & \cdots & x_n^d \end{bmatrix}.$$

Moreover, let $M_d : (\mathbb{C}^n)^k \to \mathbb{C}^{k\times\binom{n+d}{d}}$ be

$$M_d(y_1, \ldots, y_k) = \begin{bmatrix} \nu_d(y_1) \\ \vdots \\ \nu_d(y_k) \end{bmatrix}.$$

With this setup, rank $M_d(q_1^*, \ldots, q_k^*) \le$ rank $M_d(q_1(p), \ldots, q_k(p)) \le \mathrm{HF}_I(d)$. The following theorem adds certification to produce guaranteed lower bounds on $HF_I(d)$.

Theorem 3.1. *With the setup above, let $p^* \in \mathbb{C}^\ell$, $q_1, \ldots, q_k \in \mathbb{C}^n$, and $S_d(q_1, \ldots, q_k)$ be a $k \times k$ submatrix of $M_d(q_1, \ldots, q_k)$. Then, $HF_I(d) \ge k$ provided that there exists a nonsingular solution to the well-constrained system*

$$\mathcal{G}(y_1, \ldots, y_k, \Lambda) = \begin{bmatrix} G_{p^*}(y_1) \\ \vdots \\ G_{p^*}(y_k) \\ \Lambda \cdot S_d(y_1, \ldots, y_k) - \mathbf{I} \end{bmatrix}$$

where $G_{p^*}(x) = [h_{1p^*}(x), \ldots, h_{np^*}(x)]^T$ and $\mathbf{I}$ is the $k \times k$ identity matrix.

Proof. Since $S_d(q_1, \ldots, q_k)$ is a submatrix of $M_d(q_1, \ldots, q_k)$ and both have k rows,

$$k \ge \text{rank } M_d(q_1, \ldots, q_k) \ge \text{rank } S_d(q_1, \ldots, q_k).$$

Suppose that $(q_1^*, \ldots, q_k^*, \Lambda^*)$ is a nonsingular solution of $\mathcal{G} = 0$. Note that $\mathcal{G}$ is well-constrained consisting of $kn + k^2$ polynomials in $kn + k^2$ variables. Thus, the structure of $\mathcal{G}$ yields that each q_i^* is a nonsingular solution of $G_{p^*} = 0$ and $\Lambda^* = S_d(q_1^*, \ldots, q_k^*)^{-1}$. Therefore,

$$\mathrm{HF}_I(d) \ge \text{rank } M_d(q_1^*, \ldots, q_k^*) \ge \text{rank } S_d(q_1^*, \ldots, q_k^*) = k.$$

$\square$

In practice, one uses numerical approximations of known solutions to select k and the corresponding $k \times k$ submatrix which one expects to be invertible. Therefore, starting from numerical approximations, one can use a local certification routine, e.g., α-theory [10, Ch. 8], to prove the existence of a nonsingular solution of $\mathcal{G} = 0$ thereby certifying $\mathrm{HF}_I(d) \ge k$.

For each $d \geq 0$, let $\mathrm{HF}_I^{\mathrm{num}}(d)$ be the largest value k for which one can certify $\mathrm{HF}_I(d) \geq k$ based on known numerical data. Hence, $\mathrm{HF}_I^{\mathrm{num}}(d) \leq \mathrm{HF}_I(d)$.

An upper bound on $\mathrm{HF}_I(d)$ is developed in Section 3.2 with an example in Section 3.3.

3.2. **Symbolic reduction.** One option for computing the Hilbert function and thus $\deg(I)$ is to compute a Gröbner basis for $I = \langle h_1, \ldots, h_n \rangle \subset R$. However, when this is not practical, partial information provides upper bounds on the Hilbert function. For example, for each $d \geq 0$ and $e \geq 0$, consider the linear space

$$J_d^e = \left(\mathrm{span}_{\mathfrak{K}} \left(\bigcup_{i=1}^{n} \langle h_i \rangle_{\leq d+e} \right) \right)_{\leq d}.$$

Clearly, $J_d^e \subset I_{\leq d}$ showing that

$$\mathrm{HF}_I(d) \leq \binom{n+d}{d} - \dim_{\mathfrak{K}} J_d^e.$$

Moreover, $J_d^e \subset J_d^{e+1} \subset I_{\leq d}$ and there exists $e^* \geq 0$ such that $J_d^e = I_{\leq d}$ for all $e \geq e^*$ showing that this upper bound eventually becomes sharp. In fact, one such stopping criterion is if e^* such that $\mathrm{HF}_I^{\mathrm{num}}(d) = \binom{n+d}{d} - \dim_{\mathfrak{K}} J_d^{e^*}$, then $\mathrm{HF}_I^{\mathrm{num}}(d) = \mathrm{HF}_I(d) = \binom{n+d}{d} - \dim_{\mathfrak{K}} J_d^e$ for $e \geq e^*$.

Let $p^* \in \mathbb{Q}^\ell$. Rather than taking an exhaustive approach that considers all possible polynomials, one could instead repeat similar computations on I to the modular computations performed when computing a Gröbner basis for I_{p^*} over a finite field. Thus, one uses these computations to guide the computation of the polynomials in $I_{\leq d}$ via the Gröbner trace algorithm [39]. Since one is performing exact computations on I, one maintains the upper bounds on $\mathrm{HF}_I(d)$.

3.3. **Example.** We demonstrate the lower and upper bounds via the parameterized system

$$G(a, b; P) = P \cdot F(a, b)$$

where P is a 6×14 matrix of parameters and F is as in (7). Let $I = \langle G \rangle$ and consider

$$P^* = \begin{bmatrix} 1 & -2 & 2 & -4 & -4 & -5 & -3 & 1 & -1 & -1 & -2 & -3 & 1 & -5 \\ 0 & 0 & 3 & 4 & 5 & -1 & -3 & -4 & -5 & -5 & 4 & -1 & -5 & -4 \\ -5 & -4 & -1 & 0 & -5 & -3 & -4 & 4 & -3 & 4 & -1 & -4 & -3 & 2 \\ -2 & 1 & -5 & 5 & 3 & 3 & -4 & 1 & -4 & 5 & -4 & -4 & -2 & 3 \\ -4 & -3 & -3 & -5 & 3 & -1 & 4 & -2 & -3 & 0 & 3 & 5 & 4 & 2 \\ 3 & 2 & 5 & -1 & 4 & 5 & 1 & 0 & -3 & 0 & -1 & 5 & -5 & -1 \end{bmatrix}$$

with $G_{P^*}(a, b) = P^* \cdot F(a, b)$. Using `Bertini` [7, 8], we computed numerical approximations of 18 points in $\mathcal{V}(G_{P^*})$. From this data, we applied Theorem 3.1 for $d = 1, 2$ to yield

$$\mathrm{HF}_I^{\mathrm{num}}(1) = 7 \quad \text{and} \quad \mathrm{HF}_I^{\mathrm{num}}(d) = 18 \text{ for } d \geq 2 \tag{9}$$

as follows. For $d = 1$, we selected 7 points and utilized `alphaCertified` [23] with Theorem 3.1 to certify

$$7 = \mathrm{HF}_I^{\mathrm{num}}(1) \leq \mathrm{HF}_I(1) \leq \binom{6+1}{1} = 7.$$

Therefore, we know $\mathrm{HF}_I^{\mathrm{num}}(1) = \mathrm{HF}_I(1) = 7$.

For $d = 2$, we utilized all 18 known points with the subset of columns corresponding to the following 18 monomials:

$$a_1, a_2, a_3, a_4, b_1, b_2, a_1b_1, a_1b_2, a_2a_4, a_2b_2, a_3^2, a_3a_4, a_3b_1, a_3b_2, a_4b_1, b_1^2, b_1b_2, b_2^2.$$

This certification via `alphaCertified` and Theorem 3.1 shows that $\mathrm{HF}_I^{\mathrm{num}}(2) = 18$. Since we utilized all 18 points in this computation, we have $\mathrm{HF}_I^{\mathrm{num}}(d) = 18$ for $d \geq 2$.

Next, we turn to upper bounds for $\mathrm{HF}_I(d)$ for $d = 2, 3$. The following tables summarize the exhaustive approach for symbolic reduction described in Section 3.2 for $d = 2, 3$ and various values of $e \geq 0$.

e	$\dim_{\mathfrak{K}} J_2^e$	$\binom{6+2}{2} - \dim_{\mathfrak{K}} J_2^e$
0	0	28
1	3	25
2	3	25
3	5	23
4	9	19
5	10	18

e	$\dim_{\mathfrak{K}} J_3^e$	$\binom{6+3}{3} - \dim_{\mathfrak{K}} J_3^e$
0	6	78
1	25	59
2	38	46
3	63	21
4	66	18

Hence, $\mathrm{HF}_I(2) \leq \mathrm{HF}_I(3) \leq 18$. Combining with (9) shows that $\mathrm{HF}_I(2) = \mathrm{HF}_I(3) = 18$ and thus $\mathrm{HF}_I(d) = 18$ for $d \geq 2$, i.e., $\mathrm{HF}_I = \mathrm{HF}_I^{\mathrm{num}}$. In particular, this shows that there are generically 18 solutions to $G = 0$, i.e., $g_0(X, \mathbb{C}^6) = 18$ where $X = \mathcal{V}(F)$ with F as in (7).

4. Probabilistic analysis

The theory in the previous sections relied upon general choices of parameters. In this section, we give explicit characterization of when constants are sufficiently general for our computations. Since Alt's problem is formulated affinely in Section 2.1, we focus on the affine case but note that the results proved here have analogs in the other settings discussed in Section 2.

Let $R = \mathbb{Q}[x_1, \ldots, x_n]$, $f = [f_1, \ldots, f_r]^T \subset R$, and $i \in \{0, \ldots, n-1\}$. Consider the ideal

$$I_i(\Theta, \Lambda, \mu) = \langle \Theta \cdot x - \mathbf{1}, \Lambda \cdot f, 1 - (\mu \cdot f)T \rangle \tag{10}$$

where $\Theta \in \mathbb{Q}^{i \times n}$, $\Lambda \in \mathbb{Q}^{(n-i)\times r}$, and $\mu \in \mathbb{Q}^r$. The following is an affine version of [24, Thm. 4.1].

Theorem 4.1. *Let $f = [f_1, \ldots, f_r]^T \subset R = \mathbb{Q}[x_1, \ldots, x_n]$, $i \in \{0, \ldots, n-1\}$, and $X = \mathcal{V}(f)$. For general choices of $\Theta \in \mathbb{Q}^{i\times n}$, $\Lambda \in \mathbb{Q}^{(n-i)\times r}$, and $\mu \in \mathbb{Q}^r$, $I_i(\Theta, \Lambda, \mu) \subset R[T]$ as in (10) is either the unit ideal or has dimension 0. In either case,*

$$g_i(X, \mathbb{C}^n) = \dim_{\mathbb{Q}} \left(R[T]/I_i(\Theta, \Lambda, \mu)\right) \tag{11}$$

is independent of Θ, Λ and μ (provided they are general).

Proof. This immediately follows from Bertini's Theorem and the Rabinowitz trick. The proof is identical to that of [24, Thm. 4.1] with $\mathbb{P}^n$ replaced by $\mathbb{C}^n$. □

In practice, when computing the numbers $g_i(X, \mathbb{C}^n)$, the constants Θ, Λ, and μ are chosen randomly from a finite set of rational numbers, e.g., all rational numbers of bounded height or a subset of floating-point numbers of a given bit size. Therefore, even working over $\mathbb{Q}$, the computation of the integers $g_i(X, \mathbb{C}^n)$ in Theorem 4.1 is probabilistic. For our random choices in the following, we will utilize a uniform distribution on the chosen finite set.

Since the results below depend on generators with integer coefficients, we will assume that, without loss of generality, $f = [f_1, \ldots, f_r]^T \subset \mathbb{Z}[x_1, \ldots, x_n]$ and that the coefficients in each f_i are relatively prime.

4.1. **Lucky primes for randomly constructed ideals.** To simplify computations, we can employ modular methods which require the notion of lucky primes as in [4, §5.1] and [33].

The following is from [33, Defn. 4.1].

Definition 4.2. For $h_1, \ldots, h_k \in \mathbb{Z}[x_1, \ldots, x_n]$, let $I = \langle h_1, \ldots, h_k \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$ and $I_{\mathbb{Z}} = \langle h_1, \ldots, h_k \rangle \subset \mathbb{Z}[x_1, \ldots, x_n]$ be ideals with Gröbner bases G and $G_{\mathbb{Z}}$, respectively. A prime p is *Pauer lucky* with respect to I if and only if p does not divide any of the leading coefficients of the polynomials in $G_{\mathbb{Z}}$. Otherwise, p is *Pauer unlucky* with respect to I.

For $h_1, \ldots, h_k \in \mathbb{Z}[x_1, \ldots, x_n]$ and $I = \langle h_1, \ldots, h_k \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$, let $LM_{\mathbb{Q}}(I)$ denote the set of leading monomials of I. For a prime p, let $LM_{\mathbb{Z}_p}(I)$ denote the leading monomials of $\langle h_1, \ldots, h_k \rangle \subset \mathbb{Z}_p[x_1, \ldots, x_n]$. The following is [33, Prop. 4.1] which states that if a prime p is Pauer lucky, then the ideal of leading terms computed over $\mathbb{Q}$ and $\mathbb{Z}_p$ agree.

Proposition 4.3 (Prop. 4.1 of [33])**.** *With the setup as above, if a prime p is Pauer lucky with respect to I, then $LM_{\mathbb{Q}}(I) = LM_{\mathbb{Z}_p}(I)$.*

The following is used to avoid dividing any coefficients.

Definition 4.4. For a finite collection of polynomials $h \subset \mathbb{Z}[x_1, \ldots, x_n]$, we say that a prime p is *large relative to the coefficients of* h if p is larger than any coefficient appearing in a polynomial contained in h.

The following shows that every prime that is large relative to the coefficients of f is Pauer lucky for $I_i(\Theta, \Lambda, \mu)$ defined in (10) on a Zariski dense set.

Theorem 4.5. *Following the notation from Theorem 4.1 such that $f \subset \mathbb{Z}[x_1, \ldots, x_n]$, suppose that U is a Zariski dense subset of $\mathbb{Q}^{i\times n} \times \mathbb{Q}^{(n-i)\times r} \times \mathbb{Q}^r$ where the statements of Theorem 4.1 hold. Also, suppose that for $(\Theta, \Lambda, \mu) \in U$, we have that $\dim(I_i(\Theta, \Lambda, \mu)) = 0$. Then, every prime p which is large relative to the coefficients of f is a Pauer lucky prime for the ideal $I_i(\Theta, \Lambda, \mu)$ on a Zariski dense set of parameters $(\Theta, \Lambda, \mu) \in \mathbb{Q}^{i\times n} \times \mathbb{Q}^{(n-i)\times r} \times \mathbb{Q}^r$.*

Proof. Since each entry of Θ, Λ, and μ is rational, we symbolically treat the numerator and denominator separately. To that end, let $\Theta^{\text{num}}, \Theta^{\text{denom}} \in \mathbb{Z}^{i\times n}, \Lambda^{\text{num}}, \Lambda^{\text{denom}} \in \mathbb{Z}^{(n-i)\times r}$ and $\mu^{\text{num}}, \mu^{\text{denom}} \in \mathbb{Z}^r$ denote the corresponding numerators and denominators of Θ, Λ and μ, respectively. Let $\mathfrak{W} = (\Theta^{\text{num}}, \Theta^{\text{denom}}, \Lambda^{\text{num}}, \Lambda^{\text{denom}}, \mu^{\text{num}}, \mu^{\text{denom}})$ denote the collection of integer parameters.

For $I_i(\Theta, \Lambda, \mu)$ as in (10), let $I_i(\mathfrak{W})$ be the ideal obtained by clearing denominators in each of the generators of $I_i(\Theta, \Lambda, \mu)$. Note that for any $(\Theta, \Lambda, \mu) \in U$, the corresponding $I_i(\Theta, \Lambda, \mu)$ and $I_i(\mathfrak{W})$ define the same ideal in $\mathbb{Q}[x_1, \ldots, x_n, T]$. Also note that since p is large relative to the coefficients of f, each coefficient in f is not divisible by p.

Given an integer vector $\mathfrak{W}$ where each entry of Θ^{denom}, Λ^{denom}, μ^{denom} is nonzero, we let $\text{rat}(\mathfrak{W})$ denote the corresponding rational values $(\Theta, \Lambda, \mu) \in \mathbb{Q}^{i\times n} \times \mathbb{Q}^{(n-i)\times r} \times \mathbb{Q}^r$.

With this setup, we will consider $I_i(\mathfrak{W})$ as an ideal in the ring $(\mathbb{Z}[\mathfrak{W}])\,[x_1, \ldots, x_n, T]$. Let $G \subset (\mathbb{Z}[\mathfrak{W}])\,[x_1, \ldots, x_n, T]$ be a Gröbner basis of $I_i(\mathfrak{W})$ consisting of, say, ν polynomials. Let $\{c_1(\mathfrak{W}), \ldots, c_\nu(\mathfrak{W})\}$ be the leading coefficients of G where each $c_j(\mathfrak{W}) \in \mathbb{Z}[\mathfrak{W}]$. Given $(\Theta, \Lambda, \mu) \in U$ and integer vector $\mathfrak{W}$ such that $\text{rat}(\mathfrak{W}) = (\Theta, \Lambda, \mu)$, the leading monomials of G evaluated at $\mathfrak{W}$ are a superset of the leading monomials obtained by computing a Gröbner basis of $I_i(\mathfrak{W})$ in the ring $\mathbb{Z}[x_1, \ldots, x_n, T]$. In particular, the evaluated values of the leading coefficients $\{c_1(\mathfrak{W}), \ldots, c_\nu(\mathfrak{W})\}$ are multiples of the leading coefficients of a Gröbner basis of $I_i(\mathfrak{W})$ in the ring $\mathbb{Z}[x_1, \ldots, x_n, T]$. Therefore, for every $(\Theta, \Lambda, \mu) \in U$ giving rise to a corresponding $\mathfrak{W}$, either p is Pauer lucky or Pauer unlucky. Hence, there must be a Zariski dense subset of U such that at least one of these properties is satisfied. It is enough to show that there is a Zariski dense subset of U such that for each (Θ, Λ, μ) in this subset with corresponding $\mathfrak{W}$, we have that p does not divide $\{c_1(\mathfrak{W}), \ldots, c_\nu(\mathfrak{W})\}$ since this shows that p does not divide the leading coefficients of a Gröbner basis of $I_i(\mathfrak{W})$ in the ring $\mathbb{Z}[x_1, \ldots, x_n, T]$.

We note that if $(\Theta, \Lambda, \mu) \in U$ with corresponding $\mathfrak{W}$, $\dim_{\mathbb{Q}}(I_i(\Theta, \Lambda, \mu)) = \dim_{\mathbb{Q}}(I_i(\mathfrak{W})) = 0$. In particular, each leading monomial of G is not constant with respect to $x_1, \ldots, x_n, T$.

For the sake of reaching a contradiction, suppose that there exists a Zariski dense subset $D \subset U$ such that for all $(\Theta, \Lambda, \mu) \in D$ with corresponding integer vector $\mathfrak{W}$, we have that p is a Pauer *unlucky* prime for the ideal $I_i(\mathfrak{W}) \subset \mathbb{Z}[x_1, \ldots, x_n, T]$. If p is Pauer *unlucky* for $I_i(\mathfrak{W})$ for all $\text{rat}(\mathfrak{W}) \in D$, then there must exist a fixed $j \in \{1, \ldots, \nu\}$ and a (possibly smaller) Zariski dense subset $\tilde{D} \subset D$ such that p divides $c_j(\mathfrak{W})$ for all $\mathfrak{W}$ corresponding to $(\Lambda, \Theta, \mu) \in \tilde{D}$.

Since $\tilde{D} \subset \mathbb{Q}^{i\times n} \times \mathbb{Q}^{(n-i)\times r} \times \mathbb{Q}^r$ is Zariski dense, it is also dense in the classical topology. This means that $c_j(\mathfrak{W})$ must be constant since a nonconstant polynomial must map dense sets to dense sets and the set of multiples of a prime is not dense in $\mathbb{Q}$ (in the classical topology). It follows that $c_j(\mathfrak{W}) = \tilde{c} \in \mathbb{Z}$ for all $\text{rat}(\mathfrak{W}) \in \mathbb{Q}^{i\times n} \times \mathbb{Q}^{(n-i)\times r} \times \mathbb{Q}^r$. This is not possible due to the construction of $I_i(\mathfrak{W})$ since every non-constant term of every polynomial in $I_i(\mathfrak{W})$ is multiplied by some parameter value, i.e., at least one parameter must appear in each leading term since the ideal $I_i(\mathfrak{W})$ is not generated by a constant. Hence, there is *no* dense subset of U such that p is Pauer *unlucky*. It follows that there must exist some dense subset of $W \subset U \subset \mathbb{Q}^{i\times n} \times \mathbb{Q}^{(n-i)\times r} \times \mathbb{Q}^r$ for which p is a Pauer *lucky* prime for the ideal $I_i(\Theta, \Lambda, \mu)$ for all $(\Theta, \Lambda, \mu) \in W$. □

We now illustrate the construction in the proof of Theorem 4.5 with an example.

Example 4.6. Reconsider $f(x) = [x_1, x_2, x_1x_2^2, x_1^3x_2^2]^T$ from Example 2.1 where $g_1(X, \mathbb{C}^2) = 5$ with $X = \mathcal{V}(f) = \{(0, 0)\}$. Note that every prime $p \geq 2$ is large relative to the coefficients of f as in Definition 4.4. Since the ideal

$$\left\langle \theta_1x_1 + \theta_2x_2 - 1, \lambda_1x_1 + \lambda_2x_2 + \lambda_3x_1x_2^2 + \lambda_4x_1^3x_2^2 \right\rangle \tag{12}$$

generically already has degree $5 = g_1(X, \mathbb{C}^2)$, we can simplify the presentation by just considering $I_1(\Theta, \Lambda)$ equal to the ideal in (12). Define

$$\mathfrak{W} = [\theta_1^{\text{num}}, \theta_1^{\text{denom}}, \theta_2^{\text{num}}, \theta_2^{\text{denom}}, \lambda_1^{\text{num}}, \lambda_1^{\text{denom}}, \lambda_2^{\text{num}}, \lambda_2^{\text{denom}}, \lambda_3^{\text{num}}, \lambda_3^{\text{denom}}, \lambda_4^{\text{num}}, \lambda_4^{\text{denom}}]$$

so that $I_i(\Theta,\Lambda)$ is equivalent to

$$\left\langle \frac{\theta_1^{\text{num}}}{\theta_1^{\text{denom}}}x_1 + \frac{\theta_2^{\text{num}}}{\theta_2^{\text{denom}}}x_2 - 1, \frac{\lambda_1^{\text{num}}}{\lambda^{\text{denom}}}x_1 + \frac{\lambda_2^{\text{num}}}{\lambda_2^{\text{denom}}}x_2 + \frac{\lambda_3^{\text{num}}}{\lambda_3^{\text{denom}}}x_1x_2^2 + \frac{\lambda_4^{\text{num}}}{\lambda_4^{\text{denom}}}x_1^3x_2^2 \right\rangle.$$

Symoblically clearing denominators, we obtain the ideal $I_i(\mathfrak{W}) \subset (\mathbb{Z}[\mathfrak{W}])[x_1,x_2]$, namely

$$\left\langle \begin{array}{l} \theta_1^{\text{num}}\theta_2^{\text{denom}}x_1 + \theta_2^{\text{num}}\theta_1^{\text{denom}}x_2 - \theta_1^{\text{denom}}\theta_2^{\text{denom}}, \\ \lambda_1^{\text{num}}\lambda_2^{\text{denom}}\lambda_3^{\text{denom}}\lambda_4^{\text{denom}}x_1 + \lambda_2^{\text{num}}\lambda_1^{\text{denom}}\lambda_3^{\text{denom}}\lambda_4^{\text{denom}}x_2 \\ \qquad + \lambda_3^{\text{num}}\lambda_1^{\text{denom}}\lambda_2^{\text{denom}}\lambda_4^{\text{denom}}x_1x_2^2 + \lambda_4^{\text{num}}\lambda_1^{\text{denom}}\lambda_2^{\text{denom}}\lambda_3^{\text{denom}}x_1^3x_2^2 \end{array} \right\rangle.$$

Using lexicographic order, the leading terms of a Gröbner basis for $I_i(\mathfrak{W})$ are

$$\left\{c_1(\mathfrak{W})x_2^5,\ c_2(\mathfrak{W})x_1,\ c_3(\mathfrak{W})x_1x_2^4,\ c_4(\mathfrak{W})x_1^2x_2^3,\ c_5(\mathfrak{W})x_1^3x_2^2\right\} \tag{13}$$

where

$$\begin{array}{rcl} c_1(\mathfrak{W}) & = & \left(\theta_1^{\text{denom}}\theta_2^{\text{num}}\right)^3 \lambda_1^{\text{denom}}\lambda_2^{\text{denom}}\lambda_3^{\text{denom}}\lambda_4^{\text{num}}, \\ c_2(\mathfrak{W}) & = & \theta_2^{\text{denom}}\theta_1^{\text{num}}, \\ c_3(\mathfrak{W}) & = & \left(\theta_1^{\text{denom}}\theta_2^{\text{num}}\right)^2 \lambda_1^{\text{denom}}\lambda_2^{\text{denom}}\lambda_3^{\text{denom}}\lambda_4^{\text{num}}, \\ c_4(\mathfrak{W}) & = & \theta_1^{\text{denom}}\theta_2^{\text{num}}\lambda_1^{\text{denom}}\lambda_2^{\text{denom}}\lambda_3^{\text{denom}}\lambda_4^{\text{num}}, \\ c_5(\mathfrak{W}) & = & \lambda_1^{\text{denom}}\lambda_2^{\text{denom}}\lambda_3^{\text{denom}}\lambda_4^{\text{num}}. \end{array}$$

Generically, (13) yields that the $5 = g_i(X,\mathbb{C}^2)$ standard monomials are $1, x_2, \ldots, x_2^4$. As expected, each leading coefficient $c_i(\mathfrak{W})$ is nonconstant.

For illustration, consider $\Theta = [3/2, 2/3]$ and $\Lambda = [7/5, 9/11, -5/13, 13/17]$ corresponding with $\mathfrak{W} = [3,2,2,3,7,5,9,11,-5,13,13,17]$. Evaluating (13) yields the following leading terms:

$$\left\{9295000x_2^5,\ 33x_1,\ 929500x_1x_2^4,\ 92950x_1^2x_2^3,\ 9295x_1^3x_2^2\right\}. \tag{14}$$

On the other hand, if we substitute $\Theta = [3/2, 2/3]$ and $\Lambda = [7/5, 9/11, -5/13, 13/17]$ into (12), clear denominators, and compute a Gröbner basis for the resulting ideal in $\mathbb{Z}[x_1,x_2]$, the leading terms are

$$\left\{845000x_2^5,\ 33x_1,\ x_1x_2^4,\ x_1^2x_2^3,\ 11x_1^3x_2^2\right\}. \tag{15}$$

As expected, each leading coefficient in (15) divides the corresponding coefficient in (14), e.g., $9295000 = 845000 \cdot 11$ and $9295 = 11 \cdot 845$. For this problem, both (14) and (15) yield that the same set of Pauer unlucky primes via Definition 4.2, namely $\{2,3,5,11,13\}$.

4.2. **Probability of a prime being unlucky for randomly constructed ideals.** Instead of considering a Zariski dense subset of $\mathbb{Q}^{i\times n} \times \mathbb{Q}^{(n-i)\times r} \times \mathbb{Q}^r$ as in Theorem 4.5, we now consider random choices from a finite subset.

Theorem 4.7. *Let $f = [f_1,\ldots,f_r]^T \subset \mathbb{Z}[x_1,\ldots,x_n]$, $i \in \{0,\ldots,n-1\}$, and p be a prime that is large relative to the coefficients of f. Suppose that $S = \{0,\ldots,p-1\}$ and each entry of $(\Theta,\Lambda,\mu) \in \mathbb{Q}^{i\times n} \times \mathbb{Q}^{(n-i)\times r} \times \mathbb{Q}^r$ is randomly selected from S. Then, a lower bound on the probability that p is a Pauer lucky prime for $I_i(\Theta,\Lambda,\mu)$ as in (10) is*

$$P(p \text{ is Pauer lucky for } I_i(\Theta,\Lambda,\mu)) \geq \left(\frac{p-1}{p}\right)^\nu, \tag{16}$$

where ν is the number of polynomials in a Gröbner basis of $I_i(\Theta,\Lambda,\mu)$ in $\mathbb{Z}[x_1,\ldots,x_n,T]$ and

$$\nu \le \binom{\deg(I_i(\Theta,\Lambda,\mu)) + (n+1)}{(n+1)}.$$

Proof. Consider $I_i(\Theta,\Lambda,\mu)$ as an ideal in the ring $(\mathbb{Z}[\Theta,\Lambda,\mu])[x_1,\ldots,x_n,T]$ and let G be a Gröbner basis of $I_i(\Theta,\Lambda,\mu)$ in this ring which consists of ν polynomials.

First, suppose the ideal $I_i(\Theta,\Lambda,\mu)$ in $(\mathbb{Z}[\Theta,\Lambda,\mu])[x_1,\ldots,x_n,T]$ is not generated by a constant. From the proof of Theorem 4.5, we have that the leading coefficients of G, say $\{c_1(\Theta,\Lambda,\mu),\ldots,c_\nu(\Theta,\Lambda,\mu)\}$, are nonconstant polynomials in $\mathbb{Z}[\Theta,\Lambda,\mu]$. Since a nonconstant polynomial must map $\mathbb{Z}_p$ to itself injectively, the probability that a given coefficient will be nonzero in $\mathbb{Z}_p$ where each entry of (Θ,Λ,μ) is chosen from S is at least $(p-1)/p$.

Since no leading monomial can have degree greater than $\deg(I_i(\Theta,\Lambda,\mu))$ and there are

$$D = \binom{\deg(I_i(\Theta,\Lambda,\mu)) + (n+1)}{(n+1)}$$

monomials having degree at most $\deg(I_i(\Theta,\Lambda,\mu))$ in $(n+1)$ variables, it follows that $\nu \le D$.

Finally, if $I_i(\Theta,\Lambda,\mu)$ is generated by a constant, i.e., an element of $\mathbb{Z}[\Theta,\Lambda,\mu]$, the same lower bound on the probability of success holds. □

Remark 4.8. Since the degree of $I_i(\Theta,\Lambda,\mu)$ is the quantity of interest, one could produce lower bounds on the probability in (16) by using any upper bound on the degree of $I_i(\Theta,\Lambda,\mu))$, e.g., the multihomogeneous Bézout bound or the mixed volume. Further, note that [14, Cor. 2.1] yields the number of polynomials in a reduced Gröbner basis of a zero dimensional ideal over a field is at most the product of the number of variables and the degree of the ideal. While the ideal in Theorem 4.7 is zero dimensional, it is not computed over a field. However, it seems likely that there is a much lower upper bound on ν than the bound in Theorem 4.7.

In Theorem 4.7, each entry of (Θ,Λ,μ) is taken from a finite set $\mathcal{S}=\{0,1,\ldots,p-1\}$ while the ideal $I_i(\Theta,\Lambda,\mu)$ as in (10) is defined over $\mathbb{Z}$. We now turn to treating $I_i(\Theta,\Lambda,\mu)$ as an ideal defined over a finite field. To that end, let $g_i(X,\mathbb{C}^n)$ denote the (correct) integer value as in (11) computed using general rational values for Θ, Λ, and μ as in Theorem 4.1. Let $g_i(X,\mathbb{C}^n)^{\mathrm{rand}}_{\mathcal{S}\subset\mathbb{Q}}$ denote $\dim_{\mathbb{Q}}\left(R[T]/I_i(\Theta,\Lambda,\mu)\right)$ computed where the entries of Θ, Λ, and μ are randomly selected from a finite set $\mathcal{S}\subset\mathbb{Q}$. Finally, let $g_i(X,\mathbb{C}^n)^{\mathrm{rand}}_{\mathbb{Z}_p}$ denote $\dim_{\mathbb{Z}_p}\left(R[T]/I_i(\Theta,\Lambda,\mu)\right)$ where each entry of Θ, Λ, and μ is selected randomly among the elements of $\mathbb{Z}_p$. The following provides a comparison of probabilities for computing the same number. In this statement, $P(A=B)$ denotes the probability that random variables A and B take on the same value.

Theorem 4.9. *Following the setup of Theorem 4.7,*

$$P(g_i(X,\mathbb{C}^n) = g_i(X,\mathbb{C}^n)^{\mathrm{rand}}_{\mathbb{Z}_p}) \ge \left(\frac{p-1}{p}\right)^{\nu} P(g_i(X,\mathbb{C}^n) = g_i(X,\mathbb{C}^n)^{\mathrm{rand}}_{\mathcal{S}\subset\mathbb{Q}})$$

where ν is as in Theorem 4.7.

Proof. This follows immediately from Theorem 4.7. □

4.3. **Probability of choosing general coefficients.** Although Theorem 4.1 states that general values of the parameters yield the correct result, it does not provide insight into the set of parameters where (11) fails. The following provides degree bounds which are used to develop lower bounds on the probability of choosing general coefficients. We note that the results in this section are essentially an affine version of those in [25, §3.3, A.2].

As above, suppose that $f = [f_1, \ldots, f_r]^T \subset \mathbb{Z}[x_1, \ldots, x_n]$, $i \in \{0, \ldots, n-1\}$, and $X = \mathcal{V}(f)$. Define the projection of $\mathbb{C}^n$ along X as the rational map $pr_X : \mathbb{C}^n \to \mathbb{C}^r$ given by $pr_X(z) = f(z)$. Let $g_i(X, \mathbb{C}^n)$ be the value in (11) for general (Θ, Λ, μ) and let $g_i(X, \mathbb{C}^n)(\Theta, \Lambda, \mu)$ be the value obtained for a particular choice of (Θ, Λ, μ).

Consider the algebraic sets

$$\Gamma_0 = \{(x, y) \mid f_1(x) \neq 0,\ y = pr_X(x)\} \subset \mathbb{C}^n_x \times \mathbb{C}^r_y \quad \text{and} \quad \Gamma = \overline{\Gamma_0} \subset \mathbb{C}^n_x \times \mathbb{C}^r_y. \tag{17}$$

We call Γ the graph of pr_X. Define $\Gamma_{\mathrm{b}} = \Gamma \cap (\mathcal{V}(f_1) \times \mathbb{C}^r)$. In this notation, $g_i(X, \mathbb{C}^n)$ is simply the number of solutions (counted with multiplicity) to the system

$$(x, y) \in \Gamma,\quad \Theta \cdot x - \mathbf{1} = 0,\quad \Lambda \cdot y = 0$$

where $\Theta \in \mathbb{Q}^{i \times n}$ and $\Lambda \in \mathbb{Q}^{(n-i) \times r}$ are general matrices.

We now treat Θ and Λ as variables and work in $\mathbb{C}^n_x \times \mathbb{C}^r_y \times \mathbb{C}^{i \times n}_\Theta \times \mathbb{C}^{(n-i) \times r}_\Lambda$. We construct the corresponding discriminant variety as follows. Let

$$\Phi_{\mathrm{b}} = \{(x, y, \Theta, \Lambda) \mid (x, y) \in \Gamma_{\mathrm{b}},\ \Theta \cdot x - \mathbf{1} = 0,\ \Lambda \cdot y = 0\} \tag{18}$$

and $\pi_2 : \mathbb{C}^n_x \times \mathbb{C}^r_y \times \mathbb{C}^{(n-i) \times r}_\Lambda \times \mathbb{C}^{i \times n}_\Theta \to \mathbb{C}^{(n-i) \times r}_\Lambda \times \mathbb{C}^{i \times n}_\Theta$ be the projection onto the Θ and Λ coordinates. Also, define

$$\Phi_\Gamma = \{(x, y, \Theta, \Lambda) \mid (x, y) \in \Gamma,\ \Theta \cdot x - \mathbf{1} = 0,\ \Lambda \cdot y = 0\}, \tag{19}$$

and set

$$\mathfrak{D} = \det \begin{bmatrix} \multicolumn{2}{c}{\mathrm{Jac}_{x,y}(y_1 - f_1(x), \ldots, y_r - f_r(x))} \\ \Lambda & 0 \\ 0 & \Theta \end{bmatrix} \in \mathbb{C}[x, y, \Theta, \Lambda].$$

The discriminant (as shown below in Proposition 4.11) is given by

$$\Delta_{pr_X} = \begin{cases} \pi_2(\Phi_{\mathrm{b}}) \cup \pi_2(\mathcal{V}(\mathfrak{D}) \cap \Phi_\Gamma) & \text{if } \pi_2|_{\Phi_\Gamma} \text{ is surjective,} \\ \pi_2(\Phi_\Gamma) & \text{if } \pi_2|_{\Phi_\Gamma} \text{ is not surjective,} \end{cases} \tag{20}$$

that is, we show that for $(\Theta, \Lambda) \notin \Delta_{pr_X}$, we have that $g_i(X, \mathbb{C}^n) = g_i(X, \mathbb{C}^n)(\Theta, \Lambda)$. The following helps to show this.

Lemma 4.10. *Let $(\Theta, \Lambda) \in (\mathbb{C}^{(n-i) \times r}_\Lambda \times \mathbb{C}^{i \times n}_\Theta) \backslash \pi_2(\Phi_{\mathrm{b}})$. Suppose that*

$$B = \pi_2^{-1}(\Theta, \Lambda) \cap \Phi_\Gamma \subset \mathbb{C}^n_x \times \mathbb{C}^r_y \times \mathbb{C}^{(n-i) \times r}_\Lambda \times \mathbb{C}^{i \times n}_\Theta$$

and let $\widetilde{B} = \mathcal{V}(\Theta \cdot x - \mathbf{1}, \Lambda \cdot f) \backslash X \subset \mathbb{C}^n_x$. Then, all points in B are such that $f_1(x) \neq 0$ and the map $(x, y) \mapsto x$ gives a bijection $B \to \widetilde{B}$ with inverse map $x \mapsto (x, pr_X(x))$.

Proof. Note that Γ may be defined as the Zariski closure of the image of the restriction of pr_X to either $\mathbb{C}^n\backslash\mathcal{V}(f_1)$ or $\mathbb{C}^n\backslash X$ since these are the same. Let $b \in \widetilde{B}$. Since $b \notin X$, we can set $y = pr_X(b)$ and hence $(b, y) \in \Gamma$. It follows that $(b, y, \Theta, \Lambda) \in \Phi_\Gamma$ and is thus contained in B.

By assumption, $(\Theta,\Lambda) \in (\mathbb{C}_\Lambda^{(n-i)\times r} \times \mathbb{C}_\Theta^{i\times n})\backslash\pi_2(\Phi_\mathrm{b})$ so take $(x, y, \Theta, \Lambda) \in B \subset \Phi_\Gamma$ to be a point lying over (Θ, Λ). Since $(\Theta, \Lambda) \notin \pi_2(\Phi_\mathrm{b})$, this implies that $(x, y) \in \Gamma_0$ (since Γ_0 and Γ_b must be disjoint and $\Gamma = \Gamma_\mathrm{b} \cup \Gamma_0$). Hence, $y = pr_X(x)$ which implies that $x \in \widetilde{B}$. ☐

Proposition 4.11. *Using the notation above, $g_i(X, \mathbb{C}^n) = g_i(X, \mathbb{C}^n)(\Theta, \Lambda)$ for $(\Theta, \Lambda) \notin \Delta_{pr_X}$.*

Proof. The proof is split into two cases: either the restriction of π_2 to Φ_Γ is surjective or not.

Suppose that π_2 restricted to Φ_Γ is not surjective. Note that since the map π_2 is closed, then we must have that Δ_{pr_X} has codimension at least one. If $(\Theta, \Lambda) \notin \Delta_{pr_X}$, then we have that there is no (x, y) such that $(x, y, \Theta, \Lambda) \in \Phi_\Gamma$. Note that $\pi_2(\Phi_\mathrm{b}) \subset \pi_2(\Phi_\Gamma)$ by definition. By Lemma 4.10, it follows that $\mathcal{V}(\Theta \cdot x - \mathbf{1}, \Lambda \cdot f)\backslash X \subset \mathbb{C}_x^n$ is empty. Hence, $g_i(X, \mathbb{C}^n) = g_i(X, \mathbb{C}^n)(\Theta, \Lambda) = 0$.

Suppose that π_2 restricted to Φ_Γ is surjective. Let $(\Theta, \Lambda) \in (\mathbb{C}_\Lambda^{(n-i)\times r} \times \mathbb{C}_\Theta^{i\times n})\backslash\pi_2(\Phi_\mathrm{b})$. By [25, Lemma A.11], we have that (Θ, Λ) is a regular value of the restriction of π_2 to Γ if and only if for any (x, y, Θ, Λ) in the fiber $\pi_2^{-1}(x, y, \Theta, \Lambda) \cap \Phi_\Gamma$, we have that $\mathfrak{D}(x, y, \Theta, \Lambda) \neq 0$. Hence, for $(\Theta, \Lambda) \in \left(\mathbb{C}_\Lambda^{(n-i)\times r} \times \mathbb{C}_\Theta^{i\times n}\right)\backslash\Delta_{pr_X}$ we have that (Θ, Λ) is a regular value of the restriction of π_2 to Γ. Then, since π_2 restricted to Φ_Γ is surjective, it follows that $\pi_2|_{\Phi_\Gamma}$ is a dominant map, and hence the fibers of its regular values have the same cardinality (e.g., see [18, Prop. 12.19, Cor. 12.20, (12.6.2)]). The conclusion follows by Lemma 4.10. ☐

The following provides a degree bound.

Proposition 4.12. *Let $V = \mathcal{V}(y_1 - f_1(x), \ldots, y_r - f_r(x)) \subset \mathbb{C}_x^n \times \mathbb{C}_y^r$, $D_{\min} = \min_j \deg(f_j)$, and $D_{\max} = \max_j \deg(f_j)$. Then, there exists a polynomial $Q \in \mathbb{C}[\Theta, \Lambda]$ of degree at most*

$$2^n \cdot (D_{\min} + (r + n) \cdot D_{\max}) \cdot \deg(V)$$

such that if $Q(\Theta, \Lambda) \neq 0$, then $g_i(X, \mathbb{C}^n) = g_i(X, \mathbb{C}^n)(\Theta, \Lambda)$.

Proof. We first consider the case where π_2 restricted to Φ_Γ is surjective. Note that we may choose the polynomial of minimal degree to be f_1 when defining Γ_0, i.e., assume $D_{\min} = \deg(f_1)$. We must bound the degree of the discriminant $\Delta_{pr_X} = \pi_2(\Phi_\mathrm{b})$. By Bézout's Theorem,

$$\deg(\Phi_b) \leq \deg(\Gamma_\mathrm{b}) \cdot \deg(\Theta \cdot x - \mathbf{1}) \cdot \deg(\Lambda \cdot y) = 2^n \cdot \deg(\Gamma_\mathrm{b}).$$

We next bound $\deg(\Gamma_\mathrm{b})$. Let $\Omega = (\mathbb{C}^n \setminus \mathcal{V}(f_i)) \times \mathbb{C}^r$. For $G(x, y) = y - f(x)$, we have $\Omega \cap \Gamma = \Omega \cap \mathcal{V}(G)$. It follows that Γ is one of the irreducible components of $V = \mathcal{V}(G)$. Hence, $\deg(\Gamma) \leq \deg(V)$. Moreover,

$$\Gamma_\mathrm{b} = \Gamma \cap (\mathcal{V}(f_1) \times \mathbb{C}^r),$$

showing that $\deg(\Gamma_\mathrm{b}) \leq D_{\min} \cdot \deg(V)$. Therefore, $\deg(\Phi_\mathrm{b}) \leq 2^n \cdot D_{\min} \cdot \deg(V)$. Since degrees cannot increase under projection, it follows that $\deg(\Delta_{pr_X}) \leq \deg(\pi_2(\Phi)) \leq 2^n \cdot D_{\min} \cdot \deg(V)$.

Next, we need to bound $\deg(\pi_2(\mathcal{V}(\mathfrak{D}) \cap \Phi_\Gamma)) \leq \deg(\mathcal{V}(\mathfrak{D}) \cap \Phi_\Gamma)$. The polynomial $\mathfrak{D}$ has degree at most $(r + n) \cdot D_{\max}$ and $\deg(\Phi_\Gamma) \leq 2^n \cdot \deg(V)$. The result now follows from (20).

The nonsurjective case follows similarly with $\deg(\Delta_{pr_X}) \leq 2^n \cdot \deg(V)$. ☐

With this upper bound on degree, we can derive probabilistic bounds.

Proposition 4.13. *With the setup from Proposition 4.12, if the values for Λ, Θ, and μ are chosen randomly from a finite set of $S \subset \mathbb{Q}$, then*

$$P(g_i(X, \mathbb{C}^n) = \dim_{\mathbb{C}}(R/I_i(\Theta, \Lambda, \mu)) \geq 1 - \frac{g_i(X, \mathbb{C}^n) + 2^n \cdot (D_{\min} + (r+n) \cdot D_{\max}) \cdot \deg(V)}{|S|}.$$

Proof. Consider the ideal

$$J_i(\Theta, \Lambda) = \langle \Theta \cdot x - \mathbf{1}, \Lambda \cdot f \rangle : \langle f \rangle^\infty. \tag{21}$$

Let $Q \in \mathbb{C}[\Theta, \Lambda]$ be as in Proposition 4.12 and suppose Θ and Λ are selected such that $Q(\Theta, \Lambda) \neq 0$. Then, we know $\dim(J_i(\Theta, \Lambda)) = 0$ and $s := g_i(X, \mathbb{C}^n) = \deg(J_i(\Theta, \Lambda))$. Suppose that $\mathcal{V}(J_i(\Theta, \Lambda)) = \{q_1, \ldots, q_s\}$ and consider the following polynomial of degree $s = g_i(X, \mathbb{C}^n)$:

$$U(\mu) = (\mu_1 f_1(q_1) + \cdots + \mu_r f_r(q_1)) \cdots (\mu_1 f_1(q_s) + \cdots + \mu_r f_r(q_s)) \in \mathbb{C}[\mu_1, \ldots, \mu_r].$$

Note that if $U(\mu) \neq 0$, then $\deg(J_i(\Theta, \Lambda)) = \deg(I_i(\Theta, \Lambda, \mu))$. The probability bound follows from applying the Schwartz-Zippel Lemma [37, 41] using the polynomial $U \cdot Q \in \mathbb{C}[\Theta, \Lambda, \mu]$. ☐

The following considers the computation over finite fields.

Corollary 4.14. *Let $f = [f_1, \ldots, f_r]^T \subset \mathbb{Z}[x_1, \ldots, x_n]$, $i \in \{0, \ldots, n-1\}$, and p be a prime that is large relative to the coefficients of f. Set $D_{\max} = \max_j \deg(f_j)$, $D_{\min} = \min_j \deg(f_j)$, and*

$$V = \mathcal{V}(y_1 - f_1(x), \ldots, y_r - f_r(x)) \subset \mathbb{C}^n_x \times \mathbb{C}^r_y.$$

Suppose that

$$g_i(X, \mathbb{C}^n)^{\text{rand}}_{\mathbb{Z}_p} = \dim_{\mathbb{Z}_p}(R/I_i(\Theta, \Lambda, \mu))$$

is computed over $\mathbb{Z}_p$ where each entry of Θ, Λ, and μ are selected randomly from $\mathbb{Z}_p$. Then,

$$P(g_i(X, \mathbb{C}^n)^{\text{rand}}_{\mathbb{Z}_p} = g_i(X, \mathbb{C}^n)) \geq \left(\frac{p-1}{p}\right)^\nu \left(1 - \frac{g_i(X, \mathbb{C}^n) + 2^n \cdot (D_{\min} + (r+n) \cdot D_{\max}) \cdot \deg(V)}{p}\right)$$

where ν is as in Theorem 4.7 with the upper bound

$$\nu \leq \binom{\deg(I_i(\Theta, \Lambda, \mu)) + (n+1)}{(n+1)}.$$

Proof. This follows immediately from Theorem 4.9 and Proposition 4.13. ☐

5. Computations

The following considers problems associated with Alt's problem introduced in Section 2.1. We let $f = [f_1, \ldots, f_{15}]^T$ as in Section 2.1 which depend upon variables $\mathbf{x} = [a, \bar{a}, b, \bar{b}, x, \bar{x}, y, \bar{y}]^T$ with $X = \mathcal{V}(f) \subset \mathbb{C}^8$ as in (3). Throughout this section, we will suppose that all primes p being considered are such that $p \geq 5$ so that p is large relative to the coefficients of f as in Definition 4.4. The following finds primes that are large enough to provide a high probability that $g_i(X, \mathbb{C}^8)^{\text{rand}}_{\mathbb{Z}_p} = g_i(X, \mathbb{C}^8)$. The modular computations described below utilized `Magma` [11].

5.1. **Probabilistic considerations.** The following specialize results from Section 4 to the setup related to Alt's problem for computing the numbers $g_i(X, \mathbb{C}^8)$. In particular, we provide theoretical bounds on the size of the prime p required to obtain a desired level of certainty in computing $g_i(X, \mathbb{C}^8)$ using random choices with computations over $\mathbb{Z}_p$.

Corollary 5.1. *With the setup described above,*

$$P(g_i(X, \mathbb{C}^8)^{\text{rand}}_{\mathbb{Z}_p} = g_i(X, \mathbb{C}^8)) \geq \left(\frac{p-1}{p}\right)^{\nu} \left(1 - \frac{g_i(X, \mathbb{C}^8) + 317{,}987{,}389{,}440{,}000}{p}\right)$$

where ν as in Theorem 4.7 which is bounded above by $\binom{g_i(X,\mathbb{C}^8)+9}{9}$.

Proof. Using the notation of Corollary 4.14, we have $n = 8$, $r = 15$, $D_{\min} = 2$, and $D_{\max} = 7$. Using Bezóut's theorem, we obtain the bound $\deg(V) \leq 7{,}620{,}480{,}000$. ☐

For example, when $i = 0$, $I_0(\Theta, \Lambda, \mu)$ is generated by eight general linear combinations of f along with the polynomial $1 - (\mu \cdot f) \cdot T$. The results of [31] can be extended to this situation to yield $g_0(X, \mathbb{C}^8) \leq 18{,}700$. For $\omega = \binom{18709}{9}$, this gives

$$P(g_i(X, \mathbb{C}^8)^{\text{rand}}_{\mathbb{Z}_p} = g_i(X, \mathbb{C}^8)) \geq \left(\frac{p-1}{p}\right)^{\omega} \left(1 - \frac{317{,}987{,}389{,}458{,}700}{p}\right).$$

For example, if we take $p > 2^{116}$, we have $P(g_i(X, \mathbb{C}^8)^{\text{rand}}_{\mathbb{Z}_p} = g_i(X, \mathbb{C}^8)) \geq 0.99$ Although this bound is pessimistic, it provides an *a priori* lower bound on the probability. The following compares the probabilistic bound for $g_6(X, \mathbb{C}^8)$ with what is actually achieved in experiments.

5.2. **Practical success rate for $g_6(X, \mathbb{C}^8)$.** To compare the theoretical lower bounds with the practical success rate, we consider the simplest nontrivial case, namely computing $g_6(X, \mathbb{C}^8)$. Bézout's Theorem together with X described in (3) provides $g_6(X, \mathbb{C}^8) \leq 49 - 2 = 47$ while the actual value of 43 can be verified using methods described in Section 3. Using $g_6(X, \mathbb{C}^8) \leq 47$ with Corollary 5.1, we have

$$P(g_i(X, \mathbb{C}^8)^{\text{rand}}_{\mathbb{Z}_p} = g_i(X, \mathbb{C}^8)) \geq \left(\frac{p-1}{p}\right)^{7{,}575{,}968{,}400} \left(1 - \frac{317{,}987{,}389{,}440{,}047}{p}\right).$$

Therefore, the theoretical results show that $p > 2^{55}$ will yield a probability of success over 0.99. For this problem, note that the size of p is dominated by the second term of the product since

$$\log_2(100 \cdot 317{,}987{,}389{,}440{,}047) \geq 54.8 \quad \text{while} \quad \left(\frac{2^{55}-1}{2^{55}}\right)^{7{,}575{,}968{,}400} \geq 0.9999997897.$$

To check the practical success rate for various smaller primes p, we performed 10,000 random trials for selected primes p. Table 1 lists the number of successes, i.e., when $g_6(X, \mathbb{C}^8)^{\text{rand}}_{\mathbb{Z}_p} = 43$. In particular, this experiment, as expected, shows that the *a priori* theoretical bounds are quite pessimistic. For example, for all the selected primes $p \geq 2^{11} - 9 = 2039$, we already obtained a success rate over 99% in 10,000 random trials.

Prime p	Successes in 10,000 Trials
$2^6 - 5$	8,202
$2^7 - 15$	9,057
$2^8 - 5$	9,592
$2^{11} - 9$	9,941
$2^{13} - 1$	9,986
$2^{14} - 3$	9,994
$2^{15} - 19$	9,998
$2^{16} - 17$	9,999
$2^{17} - 1$	10,000
$2^{18} - 5$	10,000
$2^{19} - 1$	10,000

TABLE 1. Number of successes, i.e., when $g_6(X, \mathbb{C}^8)^{\mathrm{rand}}_{\mathbb{Z}_p} = 43$, for 10,000 trials using various primes p.

5.3. **Larger computations.** As mentioned in Section 2.1, $g_i(X, \mathbb{C}^8)$ is an upper bound on the degree of the set of four-bar linkages whose coupler curve interpolates $9 - i$ general points. The actual degree of these sets were first reported in [12, Table 1] which were computed using homotopy continuation. For convenience, we lists these degrees in Table 2.

i	7	6	5	4	3	2	1	0
degree	7	43	234	1108	3832	8716	10858	8652

TABLE 2. Degree of the set of four-bar linkages whose coupler curve interpolates $9 - i$ general points for $i = 0, \ldots, 7$.

Trivially, $g_7(X, \mathbb{C}^8) = 7$. For $i = 6$, the results of Section 5.2 show that $g_6(X, \mathbb{C}^8) = 43$ is also a sharp upper bound. Hence, we consider the sharpness for $i = 0, \ldots, 5$ by computing $g_i(X, \mathbb{C}^8)^{\mathrm{rand}}_{\mathbb{Z}_p}$ for various primes p where the parameters are selected uniformly at random in $\mathbb{Z}_p$. The results of these computations, which were performed using a 2.5 GHz Intel Xeon E5-2680 v3 processor with 256 GB of memory, are summarized in Table 3. The ones marked with "$-$" failed to finish in 10 days, while the ones in **bold** agree with the degrees reported in Table 2. In particular, these results suggest that $g_i(X, \mathbb{C}^8)$ is indeed a sharp upper bound for all $i = 0, \ldots, 7$. We note that Table 3 shows a considerable increase in the computational time needed for the two largest primes in our experiment compared with the other selected primes.

To provide additional validation of $g_0(X, \mathbb{C}^8) = 8652$, we performed 10 additional trails of $g_i(X, \mathbb{C}^8)^{\mathrm{rand}}_{\mathbb{Z}_p}$ for $p = 2^{23} + 9$ as well as using randomly selected floating-point parameters via homotopy continuation in `Bertini`. All of these experiments also yielded 8652.

Table 4 lists the purported Hilbert functions in $\mathbb{C}[\mathbf{x}, T]$. These are in agreement with numerical computations based on using solutions computed by homotopy continuation in `Bertini`.

$p \setminus i$	5	4	3	2	1	0
2^1+1	176 0.16s	849 4.66s	3352 2.50m	6192 0.52h	8756 4.69h	8492 0.84d
2^2+1	189 0.23s	975 6.99s	3594 3.36m	6803 0.79h	10693 7.01h	8586 1.20d
2^3+3	233 0.27s	1003 6.26s	3566 3.94m	7673 1.24h	10651 7.44h	8644 3.45d
2^4+1	**234** 0.23s	1059 7.94s	3766 4.46m	8635 1.20h	10739 7.99h	8646 1.82d
2^7+3	**234** 0.29s	1100 8.49s	3812 4.38m	**8716** 1.42h	**10858** 8.55h	**8652** 2.69d
$2^{11}+5$	**234** 0.34s	1107 7.53s	**3832** 4.64m	**8716** 1.41h	**10858** 9.68h	**8652** 3.11d
$2^{15}+3$	**234** 0.23s	**1108** 8.45s	**3832** 4.67m	**8716** 1.41h	**10858** 8.52h	**8652** 2.54d
$2^{19}+21$	**234** 0.24s	**1108** 7.85s	**3832** 4.83m	**8716** 1.47h	**10858** 9.36h	**8652** 3.03d
$2^{23}+9$	**234** 0.24s	**1108** 7.96s	**3832** 4.83m	**8716** 1.56h	**10858** 9.11h	**8652** 2.91d
$2^{27}+29$	**234** 0.81s	**1108** 87.63s	**3832** 95.23m	**8716** 36.76h	**10858** 250.31h	–
$2^{31}+11$	**234** 3.08s	**1108** 395.85s	**3832** 1385.45m	–	–	–

TABLE 3. Values of $g_i(X,\mathbb{C}^8)^{\mathrm{rand}}_{\mathbb{Z}_p}$ for $i = 0,\ldots,5$ and various primes p for randomly selected values of the parameters along with timings listed in either seconds (s), minutes (m), hours (h), or days (d).

$i \setminus d$	0	1	2	3	4	5	6	7	8	9	10
7	1	3	6	7	7	7	7	7	7	7	7
6	1	4	10	20	35	43	43	43	43	43	43
5	1	5	15	35	70	126	209	234	234	234	234
4	1	6	21	56	126	252	460	777	1108	1108	1108
3	1	7	28	84	210	462	920	1686	2876	3832	3832
2	1	8	36	120	330	791	1704	3362	6154	8716	8716
1	1	9	45	165	495	1285	2981	6307	10858	10858	10858
0	1	10	55	220	715	1999	4971	8652	8652	8652	8652

TABLE 4. Comparison of Hilbert function values for $i = 0,\ldots,7$

6. Conclusion

For a polynomial system f with $X = \mathcal{V}(f) \subset \mathbb{C}^n$ and a variety $Y \subset \mathbb{C}^n$ containing X, we considered the computational problem of computing $g_i(X, Y)$ for $i = 0, \dots, \dim(Y) - 1$ as defined in (6). This question was primarily motivated by its application to providing a sharp upper bound to Alt's problem, namely $g_0(X, \mathbb{C}^8)$ where $X = \mathcal{V}(f_1, \dots, f_{15})$ as formulated in Section 2.1. More generally, the values $g_i(X, Y)$ also arise in the computation of the volumes of Newton-Okounkov bodies and for the computation of characteristic classes such as Chern and Segre classes as described in Section 2.2. In particular, Section 4 provides an analysis of a probabilistic saturation technique for computing $g_i(X, Y)$ using Gröbner basis computations over finite fields.

In the context of Alt's problem, the numbers $g_i(X, \mathbb{C}^8)$ for $i = 0, \dots, 7$ provide an upper bound on the degree of the set of four-bar linkages whose coupler curve interpolates $9 - i$ general points, which is a variety of dimension i. In fact, the solution to Alt's original problem from 1923 on the number of distinct four-bar linkages that interpolate 9 general points is bounded above by $g_0(X, \mathbb{C}^8)/2$ and the number of distinct coupler curves that interpolate 9 general points is bounded above by $g_0(X, \mathbb{C}^8)/6$. In 1992, homotopy continuation was used in [40] to show the actual numbers were 4326 and 1442, respectively. However, due to the nature of the computation, they could not be sure that no additional solutions could exist. In fact, it is reported in [40] that one of the solutions was missed by their homotopy continuation solver, but was reconstructed using Roberts' cognate formula. Therefore, we posit that verifying $g_0(X, \mathbb{C}^8) = 8652$ theoretically completes Alt's problem by showing that there could be no additional solutions. To that end, we analyzed a probabilistic saturation technique (see Theorem 4.1 and Corollary 4.14) using Gröbner basis computations over various finite fields to show $g_0(X, \mathbb{C}^8)^{\text{rand}}_{\mathbb{Z}_p} = 8652$ for various primes p, a result that is also confirmed numerically using homotopy continuation.

As shown in Section 5.1, we were able to derive *a priori* theoretical bounds from Corollary 4.14 for the probabilistic computation of $g_0(X, \mathbb{C}^8) = 8652$. This bound requires the prime characteristic of our finite field to be $p > 2^{116}$ in order to guarantee a probability of success greater than 0.99. Unfortunately, our computational resources together with `Magma` do not currently permit computing $g_0(X, \mathbb{C}^8)^{\text{rand}}_{\mathbb{Z}_p}$ for $p > 2^{116}$. In fact, Table 3 shows a drastic increase in computational time between $p \leq 2^{23} + 9$ and $p \geq 2^{27} + 29$.

On the other hand, Section 5.2 shows the pessimism of the *a priori* theoretical bounds in that much higher success rates can be obtained in practice when computing over finite fields with much smaller characteristic. In particular, for the probabilistic computation of $g_6(X, \mathbb{C}^8) = 43$, the bound of Corollary 4.14 suggests one would need to take a finite field with prime characteristic larger than 2^{55} to obtain a success rate greater than 99%. Experimentally, we found that we achieved this success rate on 10,000 random trials with all selected primes $p \geq 2^{11} - 9 = 2039$. Further, even with the prime $p = 2^7 - 15 = 113$, we achieved a success rate of over 90% in our experiment. Naturally, this leads us to conclude that the bound of Corollary 4.14 of 2^{116} for computing $g_0(X, \mathbb{C}^8)$ with a success rate greater than 99% is also overly pessimistic. Coupled with numerical homotopy continuation computations, we have confidence that the probabilistic computational results indeed correctly yield $g_0(X, \mathbb{C}^8) = 8652$.

Finally, we remark that the probabilistic saturation technique has permitted computations related to Alt's problem to terminate using symbolic methods. For example, our probabilistic saturation computations related to $i = 6$ completed on average in under 0.1 seconds for our experiments using both `Magma` and `Macaulay2` [16] for the primes listed in Table 1. A similar problem was attempted in [6, §5.4] using primary decomposition over finite fields via `Singular` [13], a computation which failed to terminate in 24 hours. In fact, to generate the data for Table 1, the 10,000 random trials for each prime were completed in under 10 minutes. This drastic increase in speed allowed us to successful complete random trials for computing $g_i(X, \mathbb{C}^8)$ associated with Alt's problem for $i = 0, \ldots, 6$ for various primes as reported in Section 5. In particular, since the values of $g_i(X, \mathbb{C}^8)$ match the results in Table 2, we have utilized symbolic methods to confirm numerical homotopy continuation computations in [12, 40].

Acknowledgments

The authors would like to thank the Fall 2018 semester program on *Nonlinear Algebra* at the Institute for Computational and Experimental Research in Mathematics (ICERM) where this project was started. JDH was supported in part by NSF CCF 1812746.

References

[1] J. Abbott, M. Kreuzer, L. Robbiano. Computing zero-dimensional schemes. *J. Symb. Comput.*, 39(1), 31–49, 2005.

[2] P. Aluffi. Computing characteristic classes of projective schemes. *J. Symb. Comput.*, 35(1), 3–19, 2003.

[3] H. Alt. Über die Erzeugung gegebener ebener Kurven mit Hilfe des Gelenkvierecks. *ZAMM*, 3(1), 13–19, 1923.

[4] E.A. Arnold. Modular algorithms for computing Gröbner bases. *J. Symb. Comput.*, 35(4), 403–419, 2003.

[5] A. Baskar, S. Bandyopadhyay. An algorithm to compute the finite roots of large systems of polynomial equations arising in kinematic synthesis. *Mech. Mach. Theory*, 133, 493–513, 2019.

[6] D.J. Bates, W. Decker, J.D. Hauenstein, C. Peterson, G. Pfister, F.-O. Schreyer, A.J. Sommese, C.W. Wampler. Comparison of probabilistic algorithms for analyzing the components of an affine algebraic variety. *Appl. Math. Comput.*, 231, 619–633, 2014.

[7] D.J. Bates, J.D. Hauenstein, A.J. Sommese, C.W. Wampler. Bertini: Software for Numerical Algebraic Geometry. Available at `bertini.nd.edu`.

[8] D.J. Bates, J.D. Hauenstein, A.J. Sommese, C.W. Wampler. *Numerically solving polynomial systems with Bertini*, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2013.

[9] D.N. Bernstein, A.G Kušnirenko, A.G. Hovanskiĭ. Newton polyhedra, *Uspehi Mat. Nauk*, 31, 201–202, 1976.

[10] L. Blum, F. Cucker, M. Shub, S. Smale. *Complexity and real computation*, Springer-Verlag, New York, 1998.

[11] W. Bosma, J. Cannon, C. Playoust. The Magma algebra system. I. The user language. *J. Symb. Comput.*, 24, 235–265, 1997.

[12] D.A. Brake, J.D. Hauenstein, A.P. Murray, D.H. Myszka, C.W. Wampler. The complete solution of Alt-Burmester synthesis problems for four-bar linkages. *J. Mech. Robotics*, 8(4), 041018, 2016.

[13] W. Decker, G.-M. Greuel, G. Pfister, M. Schönemann. SINGULAR 4-1-2 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2019).

[14] J. Faugére, P. Gianni, D. Lazard, T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symb. Comput.*, 16(4), 329-344, 1993.

[15] W. Fulton. *Intersection theory*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, vol. 2, Springer-Verlag, Berlin, 1998.

[16] D. Grayson, M. Stillman. *Macaulay2, a software system for research in algebraic geometry*, available at `www.math.uiuc.edu/Macaulay2/`.
[17] Z.A. Griffin, J.D. Hauenstein, C. Peterson, A.J. Sommese. Numerical computation of the Hilbert function of a zero-scheme. *Springer Proceedings in Mathematics & Statistics*, 76, 235–250, 2014.
[18] U. Görtz, T. Wedhorn. *Algebraic Geometry: Part I: Schemes*. Springer Science & Business Media, 2010.
[19] C. Harris, M. Helmer. Segre class computation and practical applications. To appear in *Math. Comput.*
[20] J. Harris. *Algebraic geometry: a first course*. Springer Science & Business Media, 2013.
[21] J.D. Hauenstein, J.I. Rodriguez. Multiprojective witness sets and a trace test. To appear in *Adv. Geom.*
[22] J.D. Hauenstein, A.J. Sommese, C.W. Wampler. Regeneration homotopies for solving systems of polynomials. *Math. Comp.*, 80, 345–377, 2011.
[23] J.D. Hauenstein, F. Sottile. Algorithm 921: alphaCertified: Certifying solutions to polynomial systems. *ACM Trans. Math. Softw.*, 38(4), 28, 2012.
[24] M. Helmer. Algorithms to compute the topological Euler characteristic, Chern-Schwartz-MacPherson class and Segre class of projective varieties. *J. Symb. Comput.*, 73, 120–138, 2016.
[25] M. Helmer. A direct algorithm to compute the topological Euler characteristic and Chern-Schwartz-MacPherson class of projective complete intersection varieties. *Theor. Comput. Sci.*, 681, 54–74, 2017.
[26] K. Kaveh, A.G. Khovanskii. Newton-Okounkov bodies, semigroups of integral points, graded algebras and intersection theory. *Ann. of Math. (2)*, 176(2), 925–978, 2012.
[27] R. Lazarsfeld, M. Mustaţă. Convex bodies associated to linear series. *Ann. Sci. Éc. Norm. Supér. (4)*, 42(5), 783–865, 2009.
[28] A. Leykin, J. Yu. Beyond polyhedral homotopies. *J. Symb. Comput.*, 91, 173–190, 2019.
[29] M.A. Marco-Buzunáriz. A polynomial generalization of the Euler characteristic for algebraic sets. *Journal of Singularities*, 4, 114–130, 2012.
[30] A.P. Morgan, A.J. Sommese. Coefficient-parameter polynomial continuation. *Appl. Math. Comput.*, 29(2), 123–160, 1989.
[31] A.P. Morgan, A.J. Sommese, C.W. Wampler. A product-decomposition bound for Bezout numbers. *SIAM J. Num. Anal.*, 32(4), 1308–1325, 1995.
[32] A. Okounkov. Brunn-Minkowski inequality for multiplicities. *Invent. Math.*, 125(3), 405–411, 1996.
[33] F. Pauer. On lucky ideals for Gröbner basis computations. *J. Symb. Comput.*, 14, 471–482, 1992.
[34] M.M. Plecnik, R.S. Fearing. Finding only finite roots to large kinematic synthesis systems. *J. Mech. Robot.*, 9(2), 021005, 2017.
[35] S. Roberts. On three-bar motion in plane space. *Proc. London Mathematical Society, III*, 286–319, 1875.
[36] B. Roth, F. Freudenstein. Synthesis of path-generating mechanisms by numerical methods. *ASME Journal of Engineering for Industry, Series B*. 85(3):298–306, 1963.
[37] J.T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4), 701–717, 1980.
[38] H. Tari, H.-J. Su, T.-Y. Li. A constrained homotopy technique for excluding unwanted solutions from polynomial equations arising in kinematics problems. *Mech. Mach. Theory*, 45(6), 898–910, 2010.
[39] C. Traverso. Gröbner trace algorithms. In *International Symposium on Symbolic and Algebraic Computation*. Springer, Berlin, 1988.
[40] C.W. Wampler, A.P. Morgan, A.J. Sommese. Complete solution of the nine-point path synthesis problem for four-bar linkages. *ASME J. Mech. Des.*. 114(1), 153–161, 1992.
[41] R. Zippel. Probabilistic algorithms for sparse polynomials. *LNCS*, 72, 216–226, 1979.

Jonathan D. Hauenstein. Department of Applied and Computational Mathematics and Statistics, University of Notre Dame, Notre Dame, IN, USA. (hauenstein@nd.edu, `www.nd.edu/~jhauenst`).

Martin Helmer. Mathematical Sciences Institute, The Australian National University, Canberra, ACT, Australia. (martin.helmer@anu.edu.au, `www.maths.anu.edu.au/people/academics/martin-helmer`).