Tschirnhaus Transformations, Resolvent Degree, and the Method of Obliteration

Curtis Heberle

October 27, 2022

Contents

1 Introduction

The theory of Tschirnhaus transformations dates back to 1683, when Tschirnhaus published a brief note claiming to present a general procedure for solving any polynomial equation in radicals.[19] Though flawed, the methods introduced therein have stimulated a great deal of interesting research in the following three centuries, including work of Lagrange, Hamilton, Sylvester, Hilbert, Brauer, and B. Segre, among others. Unsurprisingly, given the long time period across which this work is spread, the exact formulation of the problem (as well as the notation used to describe it) has varied considerably.

A primary goal of this document is to provide an introduction to the theory of Tschirnhaus transformations and to provide a coherent framework in which the disparate results in this area can be clearly understood. Our basic premise is that much of the work on Tschirnhaus transformations can be expressed in terms of certain elementary questions of arithmetic geometry.

Specifically, we will consider questions of the following form: let K be a field (not necessarily algebraically closed) and suppose

$$X_1, \ldots, X_k \subset \mathbb{P}^{n-1}_{\overline{K}}$$

are hypersurfaces defined over K with $d_i = \deg(X_i)$. Is there a function $N(d_1, \ldots, d_k)$ such that

$$n \geq N(d_1, \ldots, d_k)$$

is sufficient to ensure the intersection

$$X_1 \cap \ldots \cap X_k \subset \mathbb{P}^{n-1}_{\overline{K}}$$

contains an L-point, for L a field extension $K \subseteq L \subset \overline{K}$ satisfying some kind of "bounded complexity" property? For example, we might require L to be a solvable extension of K, or for the degree of L/K to be bounded, or $L = K$.

We discuss other notions of bounded complexity of a field extension in section 4. In particular, we will consider the resolvent degree of a field extension. The concept of resolvent degree has its roots in Hilbert's notion of the number of parameters necessary to represent an "algebraic function", particularly his work on Tschirnhaus transformations for the degree 9 equation.[12] The first precise field-theoretic definition of this notion was given by Brauer in 1977.[2] We review this definition and explain the relationship between resolvent degree and weight of a field extension in section 4.1.

A second major aim of this document is to strengthen our understanding of the connections between results in the classical theory of Tschirnhaus transformations and the modern theory of resolvent degree. The theory of resolvent degree was recently given new life by Farb and Wolfson, who presented an equivalent geometric definition of resolvent degree and demonstrated its connections to a number of interesting of interesting problems in enumerative geometry.[6] The connection to the theory of Tschirnhaus transformations was subsequently drawn explicitly by Wolfson, who generalized Hilbert's work on the degree 9 equation to produce bounds on resolvent degree using Tschirnhaus transformations.[21] Wolfson's bounds have subsequently been sharpened by work of Alex Sutherland.[16, 10] As of the writing of this thesis, these are the best-known results for bounds on resolvent degree.

A major portion of this document focuses on the "method of obliteration" introduced by Sylvester in his 1886 paper on Tschirnhaus transformations.[18]

This gives a method for determining points over field extensions of finite *weight*, where we say L/K is of weight at most d if it can be factored into a tower of extensions each of degree at most d. On the other hand, these results can be translated into statements about resolvent degree, as we discuss in section 4.1.

Sylvester's method turns out to be remarkably general. In sections 7 and 8 we provide an exposition of Sylvester's method and produce new explicit formulae for its most general form. Finally, we apply this method to the problem of bounding resolvent degree. We show that when correctly adapted and applied with its full power, Sylvester's obliteration method can be used to produce bounds which match or (in some cases) improve upon the best previously known results.

2 Tschirnhaus Transformations - Preliminaries and Overview

In 1683, Tschirnhaus wrote a brief note claiming to describe a method for determining the roots of any polynomial in radicals.[19] Though his proof was flawed, the technique of Tschirnhaus transformations which he introduced has proven interesting a useful for reducing generic families of polynomials into certain "canonical forms".

The basic structure of the problem is as follows. Let K be a (not necessarily algebraically closed) field with $\mathrm{char}(K) = 0$, and fix an algebraic closure $\overline{K}$ of K. Fix a monic degree n polynomial

$$p(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$$

in $K[x]$. Suppose p factors over $\overline{K}$ as

$$p(x) = \prod_{i=1}^{n}(x - \lambda_i).$$

In order to define a Tschirnhaus transformation of p we will need to introduce some additional notation. Let $s_k(z_0, \ldots, z_{n-1})$ denote the kth elementary symmetric function in n variables, and let

$$T(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_{n-1}x^{n-1}$$

with $b_0, \ldots, b_{n-1}$ indeterminates. For $1 \leq k \leq n$ we define

$$A_k(b_0, \ldots, b_{n-1}) = s_k\left(T(\lambda_1), \ldots, T(\lambda_n)\right).$$

That is,

$$\begin{aligned} A_1(b_0, \ldots, b_{n-1}) &= \sum_{i=1}^{n} T(\lambda_i) \\ A_2(b_0, \ldots, b_{n-1}) &= \sum_{i \neq j} T(\lambda_i) T(\lambda_j) \\ &\vdots \\ A_n(b_0, \ldots, b_{n-1}) &= \prod_{i=1}^{n} T(\lambda_i) \end{aligned}$$

Note that $A_k(b_0, \ldots, b_{n-1})$ is a homogeneous degree k polynomial in $K[b_0, \ldots, b_{n-1}]$; although the definition makes use of the roots $\lambda_i \in \overline{K}$, the coefficients of A_k are symmetric functions of $\lambda_1, \ldots, \lambda_n$ and hence lie in the K.

For example,

$$\begin{aligned} A_1(b_0, \ldots, b_{n-1}) &= -\sum_{i=1}^{n} T(\lambda_i) \\ &= -\sum_{i=1}^{n} (b_0 + b_1\lambda_i + \ldots + b_{n-1}\lambda_i^{n-1}) \\ &= -nb_0 - \left(\sum_{i=1}^{n} \lambda_i\right) b_1 - \left(\sum_{i=1}^{n} \lambda_i^2\right) b_2 - \ldots - \left(\sum_{i=1}^{n} \lambda_i^{n-1}\right) b_{n-1} \end{aligned}$$

is a homogeneous linear polynomial in $K[b_0, \ldots, b_{n-1}]$. The power sums $\sum_{i=1}^{n} \lambda_i^k$ can be written in terms of elementary symmetric functions $s_i(\lambda_1, \ldots, \lambda_n)$ using Newton's identities, and hence can be expressed in terms of the coefficients $a_1, \ldots, a_n$ of p.

We can now define the polynomial

$$q(y) = y^n + A_1(b_0, \ldots, b_{n-1})y^{n-1} + \ldots + A_{n-1}(b_0, \ldots, b_{n-1})y + A_n(b_0, \ldots, b_{n-1})$$

in $K[y, b_0, \ldots, b_{n-1}]$. Given a choice of values for $b_0, \ldots, b_{n-1}$ in some subextension L of $\overline{K}$ over K, $q(y)$ becomes a polynomial in $L[y]$. In this context

we say that T is a *Tschirnhaus transformation* and call $q(y)$ the *transformed polynomial* corresponding to $p(x)$.

One can verify by direct calculation that

$$q(y) = \prod_{i=1}^{n}(y - T(\lambda_i)).$$

It follows that $\mu \in \overline{K}$ is a root of q if and only if $T(\lambda_i) = \mu$ for some root λ_i of p. Thus one can think of a Tschirnhaus transformation of p as a polynomial transformation applied to the roots of p.

Now for $1 \leq k \leq n$, define the *kth Tschirnhaus hypersurface* $V(A_k)$ to be the vanishing locus of $A_k(b_0, \ldots, b_{n-1})$ in $\mathbb{P}^{n-1}_{\overline{K}}$. A point of $V(A_k)$ thus corresponds to a Tschirnhaus transformation T such that the coefficient of y^{n-k} in the transformed polynomial $q(y)$ is zero.

Tschirnhaus's original idea involved finding a point in the intersection

$$V(A_1) \cap \ldots \cap V(A_{n-1}) \subseteq \mathbb{P}^{n-1}_{\overline{K}}$$

so that $p(x)$ can be transformed via the corresponding Tschirnhaus transformation T to the solvable form

$$q(y) = y^n + A_n.$$

One potential objection to this program is that it is not immediately obvious that a Tschirnhaus transformation is invertible, so that the roots of p can be recovered from the roots of q. This turns out not to be a major obstacle: for most Tschirnhaus transformations it is possible to compute an inverse rationally over K, and (except for the trivial case of a constant Tschirnhaus transformation) it is always possible to recover the roots of p from those of q by solving an equation of lower degree than p. This is described in detail in appendix B.

A more serious problem is this: for Tschirnhaus's method to produce a solution to $p(x) = 0$ in radicals, the necessary point of $V_1 \cap \ldots \cap V_{n-1}$ must be defined over a solvable extension L of K. Such a point need not exist.

Tschirnhaus did succeed in proving that one could find a Tschirnhaus transformation defined over a quadratic extension of K such that $A_1 = A_2 = 0$ provided that $n \geq 3$.

Proposition 1 (Tschirnhaus)**.** *Given any hypersurfaces V_1 and V_2 in $\mathbb{P}^{n-1}_{\overline{K}}$ with $\deg(V_i) = i$, the intersection*

$$V_1 \cap V_2$$

contains a point defined over a quadratic extension L of K provided $n \geq 3$.

Thus given any polynomial $p(x) \in K[x]$ with $\deg(p) \geq 3$ there is a Tschirnhaus transformation $T(x) \in L[x]$ which applied to p yields a transformed polynomial of the form

$$q(y) = y^n + A_3 y^{n-3} + \ldots + A_{n-1} y + A_n.$$

It is easy to see that such a point exists: the problem reduces to determining a solution to a system of two equations: one of degree 1, and one of degree 2. This just requires the quadratic formula.

With a bit more effort, one can write down the equations

$$A_1(b_0, b_1, b_2) = A_2(b_0, b_1, b_2) = 0$$

and solve for T explicitly, so Tschirnhaus's method in the $n = 3$ case gives a (rather laborious) alternative to Cardano's method for solving cubic equations. We discuss this case in some detail in section 3.

More significantly, this shows that the roots of *any* degree n polynomial can be determined solvably from the roots of a polynomial with two fewer nonzero coefficients; informally, we have reduced the problem of solving degree n equations from an n-parameter problem to an $(n-2)$-parameter problem, provided $n \geq 3$.

More generally, we can consider the problem of putting a general degree n polynomial into an $(n-k)$-parameter form by means of a Tschirnhaus transformation satisfying

$$A_1(b_0, \ldots, b_{n-1}) = \ldots = A_k(b_0, \ldots, b_{n-1}) = 0$$

and defined over some suitably "nice" extension of K. Here Tschirnhaus's method proves fruitful provided n is sufficiently large relative to k.

The first result in this direction post-Tschirnhaus was given by Bring in 1786.[4]

Proposition 2 (Bring)**.** *Given any hypersurfaces V_1, V_2, V_3 defined over K with $\deg(V_i) = i$, the intersection*

$$V_1 \cap V_2 \cap V_3 \subseteq \mathbb{P}^{n-1}_{\overline{K}}$$

contains a point defined over a solvable extension L of K provided $n \geq 5$.

Thus given any polynomial $p(x) \in K[x]$ with $\deg(p) \geq 5$ there is a Tschirnhaus transformation $T(x) \in L[x]$ which applied to p yields a transformed polynomial of the form

$$q(y) = y^n + A_4 y^{n-4} + \ldots + A_{n-1} y + A_n.$$

Bring's result is discussed further, and a proof given, in section 3 below. The key reduction is replacing the quadric surface $V_1 \cap V_2$ by a line contained in it, which can be determined over a quadratic extension. We will also revisit this result in section 8 as an easy application of the method of obliteration.

Bring's result was later recovered independently and extended by Jerrard in the mid-19th century.[13] Curiously, Jerrard claimed (as had Tschirnhaus centuries earlier) to be able to solve any polynomial equation by means of the method. (In particular, reducing the quintic to the solvable form $y^5 + A_5$.) Jerrard's work was investigated, clarified, and expanded upon, first by Hamilton in 1836 then by Sylvester in 1887.[8, 18] This led to a collection of results which are partially summarized in the following proposition.

Proposition 3 (Hamilton, Sylvester)**.** *There is a function $N : \mathbb{N} \to \mathbb{N}$ such that the following is true whenever $n \geq N(k)$:*

For any hypersurfaces $V_1, \ldots, V_k$ in $\mathbb{P}^{n-1}_K$ with $\deg(V_i) = i$, the intersection

$$V_1 \cap \ldots \cap V_k$$

contains a point defined over an extension L of K with the property that L/K factors as a tower of finite extensions of degree at most k.

The first few values of N are $N(2) = 3$, $N(3) = 5$, $N(4) = 10$, $N(5) = 44$, $N(6) = 905$.

For example, $N(4) = 10$ says that, for any polynomial $p(x) \in K[x]$ with $\deg(p) \geq 10$ there is a weight 4 extension L/K and a Tschirnhaus transformation $T(x) \in L[x]$ which applied to p yields a transformed polynomial of the form

$$q(y) = y^n + A_4 y^{n-4} + \ldots + A_{n-1} y + A_n.$$

A proof of this proposition – and an algorithm for computing $N(k)$ –comes from the "method of obliteration" introduced by Sylvester. This method is discussed in detail in sections 7 and 8.

A significant shift in the framing of the problem was introduced by Hilbert in his analysis of Tschirnhaus transformations for the degree 9 polynomial.[12]

Hilbert sketched a geometric argument involving the existence of lines on a cubic surface to prove that it is possible to determine a point of

$$V(A_1) \cap V(A_2) \cap V(A_3) \cap V(A_4) \subseteq \mathbb{P}^{n-1}_{\overline{K}}$$

and thus remove 4 terms from a degree 9 polynomial by means of a Tschirnhaus transformation. (Compare to $N(4) = 10$.)

Although determining a line on a cubic surface requires the solution of an equation of degree 27, Hilbert argued that this equation itself can be given in a "four-parameter form". This is sufficient to show that the degree 9 equation itself depends on "algebraic functions of four-parameters".

Hilbert's result can be stated precisely using the *resolvent degree* of a field extension, first defined by Brauer in 1977. We review the basic definitions, following Brauer's treatment, in section 4. In this language, Hilbert's result says that there exists a point of

$$V(A_1) \cap V(A_2) \cap V(A_3) \cap V(A_4) \subseteq \mathbb{P}^{n-1}_{\overline{K}}$$

defined over an extension L/K of resolvent degree at most 4, provided $n \geq 9$.

Hilbert's result was subsequently refined by B. Segre and (independently) Dixmier.[15, 5]

Proposition 4 (Segre, Dixmier)**.** *For any hypersurfaces $V_1, \ldots, V_4$ in $\mathbb{P}^{n-1}_{\overline{K}}$ with $\deg(V_i) = i$, the intersection*

$$V_1 \cap V_2 \cap V_3 \cap V_4$$

contains a point defined over an extension L of K with the property that L/K factors as a tower of finite extensions of degree at most 5.

The proof of this proposition relies on a slightly different geometric idea than Hilbert's argument, and is discussed further in section 5.

Much more recently, Hilbert's ideas were generalized by by Jesse Wolfson to produce a collection of bounds on resolvent degree using Tschirnhaus transformations, significantly improving on previously known bounds.[21] Wolfson's bounds have subsequently been sharpened by work of Alex Sutherland.[17] In section 8 we show that these bounds can be reproduced and, in some cases, further improved using Sylvester's method of obliteration.

3 Tschirnhaus Transformations for $n = 3, 4, 5$

We now consider some examples of Tschirnhaus transformations in low degree. We discuss Tschirnhaus's solution to the cubic (the only case explicitly handled in Tschirnhaus's original note), Lagrange's approach to solving the quartic using Tschirnhaus transformations, and Bring's reduction of the quintic to a one-parameter form. Bring's argument is particularly important as it introduces the idea of replacing a Tschirnhaus hypersurface $V(A_i)$ by a linear subspace to control the algebraic complexity of the problem.

3.1 Tschirnhaus's Solution of the Cubic

For $n = 3$, Tschirnhaus's method gives a general solution to the cubic equation. Recall that any cubic polynomial in $K[x]$ can be put in the form

$$p(x) = x^3 + a_2 x + a_3$$

by means of a linear change of variables.

To transform $p(x)$ to the form

$$q(y) = y^3 + A_3$$

by means of a Tschirnhaus transformation $T(x) = b_0 + b_1 x + b_2 x^2$ it suffices to determine a solvable point $[b_0 : b_1 : b_2] \in \mathbb{P}^3_{\overline{K}}$ such that

$$[b_0 : b_1 : b_2] \in V(A_1(b_0, b_1, b_2)) \cap V(A_2(b_0, b_1, b_2))$$

where $V(A_1)$ and $V(A_2)$ are the first and second Tschirnhaus hypersurfaces defined in the previous section.

This is always possible. Recall A_1 is a linear homogeneous polynomial in b_0, b_1, b_2, so

$$V(A_1) \cong \mathbb{P}^2_{\overline{K}}.$$

Further, A_2 is degree 2 homogeneous, so the intersection

$$V(A_1) \cap V(A_2)$$

is a degree 2 algebraic curve in $\mathbb{P}^2_{\overline{K}}$, and it is obviously possible to determine a point on such a curve over a degree 2 extension of K.

More concretely, one can prove the following.

Proposition 5 (Tschirnhaus)**.** *Consider a depressed cubic* $p(x) = x^3 + a_2 x + a_3$ *over a field* K *and let*

$$\Delta = -27a_3^2 - 4a_2^3$$

denote the discriminant of p*. There is a Tschirnhaus transformation*

$$T(x) = b_0 + b_1 x + b_2 x^2$$

defined over the quadratic extension $L = K(\sqrt{-3\Delta})$ *such that setting*

$$y = T(x)$$

yields a transformed polynomial

$$q(y) = y^3 + A_3,$$

where

$$A_3 = (b_1^3 + b_1 b_2^2 a_2 + b_2^3 a_3)\frac{\sqrt{-3\Delta}}{9}.$$

In particular, it suffices to take

$$b_0 = 2a_2^2/3, \qquad b_1 = \frac{-9a_3 + \sqrt{-3\Delta}}{6}, \qquad b_2 = a_2.$$

The elementary but somewhat cumbersome proof of this proposition is given in Appendix C.

Example 1. *Let* $p(x) = x^3 - 6x + 6$*. This has discriminant*

$$\Delta = -108.$$

Applying proposition 5, the Tschirnhaus transformation

$$T(x) = 24 - 6x - 6x^2$$

applied to $p(x)$ *yields the transformed polynomial*

$$q(y) = y^3 - 432.$$

Now let μ *be a root of* q *and let us determine the corresponding root* λ *of* p*. Such a* λ *must be a root of both* $p(x)$ *and of* $T(x) - \mu$*, so is a root of*

$$\mathrm{GCD}(x^3 + a_2 x + a_3, b_2 x^2 + b_1 x + b_0 - \mu) = \left(\frac{b_1^2 - b_0 b_2 + b_2 \mu + b_2^2 a_2}{b_2^2}\right) x + \frac{b_0 b_1 - b_1 \mu + b_2^2 a_3}{b_2^2}.$$

It follows that

$$\lambda = \frac{-b_0 b_1 + b_1 \mu - b_2^2 a_3}{b_1^2 - b_0 b_2 + b_2 \mu + b_2^2 a_2}.$$

Plugging in the values of b_0, b_1, b_2, a_2, a_3 *for this example and simplifying yields*

$$\lambda = \frac{\mu - 12}{\mu - 6}.$$

Thus for example, taking the real root $\mu = \sqrt[3]{432} = 6\sqrt[3]{2}$ *of* q*, we find that the corresponding root of* p *is*

$$\lambda = \frac{6\sqrt[3]{2} - 12}{6\sqrt[3]{2} - 6} = \frac{\sqrt[3]{2} - 2}{\sqrt[3]{2} - 1}.$$

The complex roots can be determined similarly.

3.2 Lagrange's Solution to the Quartic

For $n = 4$, we can attempt to carry out the same procedure with a cubic Tschirnhaus transformation. That is, given

$$p(x) = x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4$$

we seek a transformation $T(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3$ such that the transformed polynomial

$$q(y) = y^4 + A_1 y^3 + A_2 y^2 + A_3 y + A_4$$

satisfies $A_1 = A_2 = A_3 = 0$. Now the intersection $V(A_1) \cap V(A_2) \cap V(A_3)$ is the intersection of a conic and a cubic curve in the plane $V(A_1)$. In general two such curves will intersect in 6 points, which are governed by an equation of degree 6, and it is not obvious whether any of these points will be defined over the solvable closure of K.

Nonetheless, in 1771 Lagrange gave two proofs that Tschirnhaus's method nonetheless could be used to put any quartic into solvable form.[14] First, he showed that for the particular equations $A_2 = 0$ and $A_3 = 0$ arising in this context, the degree 6 equation governing their intersection always factors into a pair of cubic equations, and so has solvable splitting field. Second, he observed that to put $p(x)$ in the solvable form

$$q(y) = y^4 + A_2 y^2 + A_4$$

requires only $A_1 = A_3 = 0$, a system with one linear equation and one cubic equation, and this always admits solvable solutions.

3.3 Bring's Analysis of the Quintic

For $n = 5$, the insolvability of the quintic implies that there is no transformation $T(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4$ defined over the solvable closure of K transforming a general quintic polynomial $p(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$ to

$$q(y) = y^5 + A_1y^4 + A_2y^3 + A_3y^2 + A_4y + A_5$$

with $A_1 = A_2 = A_3 = A_4 = 0$.

On the other hand, p *can* be put into a "one-parameter form" by means of a solvable Tschirnhaus transformation. To prove this, it suffices to show that there is a transformation T such that the transformed polynomial satisfies $A_1 = A_2 = A_3 = 0$, so is of the form

$$y^5 + A_4y + A_5,$$

since then substituting $z = (A_4/A_5)y$ and scaling we have

$$z^5 + Az + A,$$

where $A = A_4^5/A_5^4$. That such a T exists was first proven by Bring in 1786.[4]

Proposition 6 (Bring)**.** *Suppose V_1, V_2, V_3 are hypersurfaces in $\mathbb{P}^{n-1}_{\overline{K}}$ with $\deg(V_i) = i$. If $n \geq 5$, then there is a point of $V_1 \cap V_2 \cap V_3$ defined over a solvable extension of K.*

In particular, this implies a degree n polynomial in $K[x]$ can be put into an $n-4$-parameter form after taking a solvable extension of K.

Proof. It suffices to prove the result for $n = 5$. We can identify V_1 with $\mathbb{P}^{n-2} = \mathbb{P}^3$; let x_0, x_1, x_2, x_3 be homogeneous coordinates for this space. Then $V_1 \cap V_2$ is a quadric surface in $\mathbb{P}^{n-2}$, defined by the vanishing of some quadratic form $F(x_0, x_1, x_2, x_3)$. Since $char(K) \neq 2$, any quadratic form over K is equivalent to a diagonal form, so we may assume

$$F(x_0, x_1, x_2, x_3) = c_0x_0^2 - c_1x_1^2 + c_2x_2^2 - c_3x_3^2.$$

Now let $L = K(\sqrt{c_0}, \sqrt{c_1}, \sqrt{c_2}, \sqrt{c_3})$. This is a solvable extension of K, over which we have

$$F(x_0, x_1, x_2, x_3) = (\sqrt{c_0}x_0 + \sqrt{c_1}x_1)(\sqrt{c_0}x_0 - \sqrt{c_1}x_1) + (\sqrt{c_2}x_2 + \sqrt{c_3}x_3)(\sqrt{c_2}x_2 - \sqrt{c_3}x_3).$$

The vanishing locus of $\sqrt{c_0}x_0 + \sqrt{c_1}x_1$ and $\sqrt{c_2}x_2 + \sqrt{c_3}x_3$ is a line contained in $V_1 \cap V_2$ and defined over L. In general this line intersects the cubic surface $V_1 \cap V_3$ in 3 points, which can be determined by solving an equation of degree 3. Thus there is a point of $V_1 \cap V_2 \cap V_3$ defined over a degree 3 extension of L. Since L is a solvable extension of K, and any degree 3 extension is solvable, this implies $V_1 \cap V_2 \cap V_3$ contains a solvable point, as desired. □

The key step in Bring's proof is the determination of a line contained in $V_1 \cap V_2$, which is possible exactly when $n-1 \geq 4$. This reduces the total degree of the system sufficiently so that a solvable solution is guaranteed to exist. More generally, given hypersurfaces $V_1, \ldots, V_k$ in $\mathbb{P}^{n-1}_{\overline{K}}$ with $\deg(V_i) = i$, we can reduce the total degree of the intersection $V_1 \cap \ldots \cap V_k$ by replacing one or more of the V_i with a linear subspace that it contains. Thus an essential question is: given an extension L/K and integers $k, d > 0$, how large must n be so that any degree d hypersurface in $\mathbb{P}^n_{\overline{K}}$ contains a k-plane defined over L?

The examples we have considered thus far involved solvable extensions L of K. This is not the only possible formulation of the problem and indeed much of the historical work on Tschirnhaus transformations has not restricted itself to transformations which are defined solvably over the base field. In the next section we consider a number of different notions of the "complexity" of a field extension which can be (and have been) adopted as constraints on the field of definition of the Tschirnhaus transformation to be found. In section 5 we give a historical overview of results concerning the reduction of a degree n polynomial to $(n-5)$-parameter form by means of Tschirnhaus transformations; the relationship between the various results of Hamilton, Sylvester, Hilbert, Segre, and others, for this problem can be best understood in terms of the different notions of "bounded complexity" which they employ.

4 Tschirnhaus Transformations over Field Extensions of Bounded Complexity

A number of mathematicians have worked on the problem(s) of using Tschirnhaus transformations to put univariate polynomials into certain canonical forms. As the theory has developed, so too has the precise formulation of the problem. Informally, we can think of this in terms of what one is "allowed to do" to determine a transformation – we might insist on a "formula

in radicals", for example. These constraints have often been assumed rather than stated explicitly. In this section we will introduce some field-theoretic terminology that will allow us to describe several of the variant formulations of the problem more precisely.

The basic form of the problem is this. Let K be a field and consider a polynomial

$$p(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n.$$

We would like to determine a Tschirnhaus transformation

$$T(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}$$

such that the coefficients of the transformed polynomial

$$q(x) = x^n + A_1 x^{n-1} + \ldots + A_{n-1}x + A_n$$

satisfies some specified conditions; usually that $A_1 = \ldots = A_r = 0$ for some r. Recall that A_i is a homogeneous degree i polynomial in $b_0, \ldots, b_{n-1}$, with coefficients in K, so we are looking for a point on the intersection of several hypersurfaces in an $(n-1)$-dimensional projective space. How large must n be to ensure this is always possible? To make this question precise we need to specify conditions on the field over which the coefficients b_i of T may be taken.

The maximally permissive choice would be to allow T to be defined over the algebraic closure $\overline{K}$. In this case the problem becomes uninteresting, since the intersection

$$V(A_1) \cap \ldots \cap V(A_{r-1})$$

always contains a $\overline{K}$-point for $r \leq n$.

Intuitively – particularly from a classical perspective – we might also want the determination of the Tschirnhaus transformation T to be "simpler", in some sense, than solving the polynomial p. Indeed, over any extension of K which contains all roots of p, the theory of Tschirnhaus transformations again becomes trivial, as the following proposition shows.

Proposition 7. *Let $p(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} + a_n$ and $q(x) = x^n + c_1 x^{n-1} + \ldots + c_{n-1}x + c_n$ be polynomials in $K[x]$. If p has n distinct roots, then for any extension L/K which contains the roots of P there exists a Tschirnhaus polynomial*

$$T(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1} \in L[x]$$

such that q is the transformed polynomial obtained by applying T to p.

Proof. Let $\lambda_1, \ldots, \lambda_n$ be the roots of p and let $\mu_1, \ldots, \mu_n$ be the roots of q. Recall that the transformed polynomial obtained by applying T to p is, by definition,

$$\prod_{i=1}^{n}(x - T(\lambda_i)).$$

Thus we need to show there is a polyonomial T such that $T(\lambda_i) = \mu_i$ for all i. That is, the coefficients b_i of T must be chosen to satisfy

$$b_0 + b_1\lambda_i + \ldots + b_{n-1}\lambda_i^{n-1} = \mu_i$$

for $i = 1, \ldots, n$. This gives an $n \times n$ system of linear equations in $b_0, \ldots, b_{n-1}$, which we can write in matrix-vector form as

$$\begin{bmatrix} 1 & \lambda_1 & \lambda_1^2 & \ldots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \lambda_2^2 & \ldots & \lambda_2^{n-1} \\ & & \vdots & & \\ 1 & \lambda_n & \lambda_n^2 & \ldots & \lambda_n^{n-1} \end{bmatrix} \begin{bmatrix} b_0 \\ \vdots \\ b_{n-1} \end{bmatrix} = \begin{bmatrix} \mu_1 \\ \vdots \\ \mu_n \end{bmatrix}.$$

This matrix is the *Vandermonde matrix* associated to the polynomial p. Its determinant is given by

$$\prod_{1 \leq i < j \leq n} (\lambda_i - \lambda_j).$$

Since p has distinct roots, this product is nonzero, so the system is nonsingular and we can solve for the coefficients $b_0, \ldots, b_{n-1}$ of T in terms of the roots of p and q. □

There are a number of natural ways to constrain what sorts of field extensions L/K are permissible when determining a Tschirnhaus transformation. An approach taken by Sylvester, among others, is to bound the highest degree of any equation that must be solved in determining the transformation; in other words, to consider finite towers of finite extensions each of degree at most d. Following Sylvester's terminology, we will say such an extension has *weight* at most d. Finally, we will consider the *resolvent degree* of a field extension, with which Hilbert's idea of expressing an algebraic function in terms of algebraic functions of fewer parameters can be made precise; definitions are given in the next subsection.

4.1 Weight, Essential Dimension, and Resolvent Degree of a Field Extension

In this section we introduce the notions of weight, essential dimension, and resolvent degree of a field extension. To define the latter two concepts rigorously we must shift perspective slightly; rather than considering *any* finite extension L/K, as in previous sections, it is necessary to first fix an algebraically closed field A of characteristic zero and consider finite extensions L/K with K an extension of A. A prototypical example would be $A = \mathbb{C}$ and $K = A(a_1, \ldots, a_n)$ with $a_1, \ldots, a_n$ indeterminates, so K itself need not be algebraically closed.

For convenience we will work over a fixed algebraically closed base field A throughout the remainder of this document. On the other hand, any subsequent results that do not involve resolvent degree or essential dimension can be interpreted in the slightly more general context where K is any field of characteristic zero (including, for example, the classical perspective with $K = \mathbb{Q}$).

Now let A be a fixed algebraically closed field of characteristic zero. Let K be an extension of A, and let L be a finite extension of K. We will define the weight, essential dimension, and resolvent degree of L/K (relative to A), and discuss the relationship between these notions.

Definition 4.1. The *weight* of L/K, which we write $\mathrm{wt}(L/K)$, is the minimal d such that L/K factors as a finite tower of finite extensions

$$K = L_0 \hookrightarrow L_1 \hookrightarrow \ldots \hookrightarrow L_{r-1} \hookrightarrow L_r = L$$

with degree $[L_i : L_{i-1}] \leq d$ for all i.

For the problem of removing r terms from the generic degree n polynomial $p(x) = x^n + a_1 x^{n-1} + \ldots + a_n$, Sylvester considers Tschirnhaus transformations defined over extensions L of K of weight at most r. Informally, this is a restriction on "elevation of degree"; recall that the coefficients of such a transformation must satisfy a system of r equations $A_1, \ldots, A_r$ with $\deg(A_i) = i$. Thus requiring $\mathrm{wt}(L/K) \leq r$ essentially amounts to requiring that any auxiliary equations introduced in the solution of the problem be of degree at most r.

We next consider the notions of essential dimension and resolvent degree. Given the classical flavor of our results, it will be most convenient to work

with Brauer's original 1977 definition.[2] Equivalent definitions – including a purely geometric version – are given by Farb and Wolfson.[6]

Definition 4.2. The *essential dimension* of L/K relative to A, written $\mathrm{ed}_A(L/K)$, is the minimal d such that $L = K(\lambda)$ for some $\lambda \in L$ satisfying

$$f_0(u_1, \ldots, u_d)\lambda^r + f_1(u_1, \ldots, u_d)\lambda^{r-1} + \ldots + f_{r-1}(u_1, \ldots, u_d)\lambda + f_r(u_1, \ldots, u_d) = 0$$

for some polynomials $f_0, \ldots, f_r \in A[x_1, \ldots, x_d]$ and elements $u_1, \ldots, u_n \in K$.

For ease of notation we will write $\mathrm{ed}(L/K)$ for $\mathrm{ed}_A(L/K)$ henceforth, omitting the explicit dependence on the fixed base field A.

Informally, the definition says we have $\mathrm{ed}(K(\lambda)/K) \leq d$ if λ is a value of an algebraic function of at most d parameters. In particular, when $K = A(a_1, \ldots, a_n)$ and λ is a root of the generic degree n polynomial, we have the following lemma.

Lemma 1. *Given $K = A(a_1, \ldots, a_n)$, let $d(n)$ denote the minimal integer m such that there exists a non-constant Tschirnhaus transformation defined over A which transforms the generic degree n polynomial $p(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ to a polynomial of the form*

$$q(x) = x^n + A_1(u_1, \ldots, u_m)x^{n-1} + \ldots + A_{n-1}(u_1, \ldots, u_m)x + A_n(u_1, \ldots, u_m)$$

where $A_1, \ldots, A_n$ are polynomials in $K[x_1, \ldots, x_m]$, and $u_1, \ldots, u_m \in K$.

Then if $L = K[x]/(p)$ we have

$$d(n) \geq \mathrm{ed}(L/K).$$

Proof. Let $\lambda = [x] \in L$. Then λ is a primitive element for L as an extension of K, so $L = K(\lambda)$, and λ satisfies

$$p(\lambda) = \lambda^n + a_1\lambda^{n-1} + \ldots + a_{n-1}\lambda + a_n = 0.$$

Suppose there is a Tschirnhaus transformation $T(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1} \in A[x]$ such that T transforms p to a polynomial q of the form

$$q(x) = x^n + A_1(u_1, \ldots, u_m)x^{n-1} + \ldots + A_{n-1}(u_1, \ldots, u_m)x + A_n(u_1, \ldots, u_m),$$

with $A_1, \ldots, A_n$ are polynomials in $K[x_1, \ldots, x_m]$, and $u_1, \ldots, u_m \in K$.

Let $\mu = T(\lambda)$. Then μ is also a primitive element of L; see Corollary 3.3 and Example 3.4 of [21].

In fact, in this context ($K = A(a_1, \ldots, a_n)$ and T defined over A) any non-constant Tschirnhaus transformation T is invertible in the sense of Appendix B, so that λ can be recovered rationally over K from $\mu = T(\lambda)$, and this implies μ is a primitive element.

The key observation is that any two roots of the generic polynomial $p(x)$ are algebraically independent over A. Thus if $\lambda' \neq \lambda$ is another root of p, one cannot have

$$T(\lambda) = T(\lambda')$$

for any non-constant Tschirnhaus transformation T with coefficients in A. It follows then that

$$\gcd(T(x) - \mu, p(x))$$

is linear, so λ is a root of a linear polynomial with coefficients in $K(\mu)$.

We thus have $K[x]/(p) = K(\mu)$ and by definition of the Tschirnhaus transformation T sends roots of p to roots of q, so

$$\mu^n + A_1(u_1, \ldots, u_m)\mu^{n-1} + \ldots + A_{n-1}(u_1, \ldots, u_m)\mu + A_n(u_1, \ldots, u_m).$$

By definition of essential dimension, this means

$$\mathrm{ed}(L/K) \leq m.$$

□

Using this relationship, Buhler and Reichstein have shown that $d(n) \geq [n/2]$ for all n.[3]

The notion of *resolvent degree* relates to essential dimension in the same way that weight relates to degree. That is, an extension is of bounded resolvent degree if it factors as a finite tower of extensions of bounded essential dimension.

Definition 4.3. The *resolvent degree* of L/K relative to A, written $\mathrm{RD}_A(L/K)$ is the minimal d such that there is a tower of finite extensions

$$K = L_0 \hookrightarrow L_1 \hookrightarrow \ldots \hookrightarrow L_{r-1} \hookrightarrow L_r$$

with $L \hookrightarrow L_r$ and $\mathrm{ed}_K(L_i/L_{i-1}) \leq d$ for $i = 1, \ldots, r$.

As with essential dimension, we will generally omit the subscript and write simply $\mathrm{RD}(L/K)$.

Definition 4.4. Let $\mathrm{RD}(n)$ denote the supremum of $\mathrm{RD}(L/K)$ over all degree n field extensions L/K over A.

For any such extension, the primitive element theorem implies $L = K(\lambda)$, where λ is a root of a monic degree n polynomial $p(x)$ over K, so $\mathrm{RD}(L/K) \leq \mathrm{ed}(L/K) \leq n$ and so $\mathrm{RD}(n) \leq n$. In subsequent sections we will produce improved bounds on $\mathrm{RD}(n)$ using Sylvester's method of obliteration

As a first example, for $n = 2$ we have $\mathrm{RD}(2) = 1$, essentially by the quadratic formula. More precisely, suppose L/K is degree 2 extension. Let λ be a primitive element and $p(x) = x^2 + a_1 x + a_2$ its minimal polynomial. By the quadratic formula,

$$\lambda = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2}}{2},$$

so $\sqrt{a_1^2 - 4a_2}$ is also a primitive element, with minimal polynomial $x^2 - (a_1^2 - 4a_2)$. It follows that $\mathrm{ed}_A(L/K) = 1$ and so $\mathrm{RD}_A(L/K) = 1$.

Slightly less trivially, Cardano's solution to the cubic implies $\mathrm{RD}(3) = 1$. Let L/K be a cubic extension with λ a primitive element. After a change of variables, we may assume the minimal polynomial for λ is of the form $x^3 + a_2 x + a_3$. Then Cardano's formula says that

$$\lambda = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

for some choice of cube roots. Thus there is a tower of extensions

$$K \hookrightarrow L_1 = K\left(\sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right) \hookrightarrow L_2 = L_1\left(\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\right)$$
$$\hookrightarrow L_3 = L_2\left(\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\right)$$

with $L \hookrightarrow L_3$. L_1/K is quadratic, so $\mathrm{ed}(L_1/K) = 1$, and L_2/L_1 and L_3/L_1 are cyclic extensions generated by elements with minimal polynomials of the form $x^3 - a$, so are also essential dimension 1. Thus $\mathrm{RD}(L/K) = 1$.

Similarly, $\mathrm{RD}(4) = 1$, and $\mathrm{RD}(L/K) = 1$ for any solvable extension L/K. On the other hand, $\mathrm{RD}(L/K) = 1$ does not imply L/K is solvable; at the end of this section we show that Bring's reduction of the quintic to a one-parameter form proves that $\mathrm{RD}(5) = 1$.

The next two lemmas will allow us to translate results for Tschirnhaus transformations over fields of bounded weight into bounds on $\mathrm{RD}(n)$.

Lemma 2. *If L is an extension of K over A with $\mathrm{wt}(L/K) \leq d$, then $\mathrm{RD}(L/K) \leq \mathrm{RD}(d)$.*

Proof. Since $\mathrm{wt}(L/K) \leq d$, there is a tower of extensions

$$K = L_0 \hookrightarrow L_1 \ldots \hookrightarrow L_r$$

with $L \hookrightarrow L_r$ and $\deg(L_i/L_{i-1}) \leq d$ and hence $\mathrm{RD}(L_i/L_{i-1}) \leq \mathrm{RD}(d)$ for $i = 1, \ldots, r$. This implies each extension L_i/L_{i-1} factors as a tower of extensions of essential dimension at most $\mathrm{RD}(d)$, so L/K factors as a tower of such extensions and so $\mathrm{RD}(L/K) \leq \mathrm{RD}(d)$. □

Lemma 3. *Let K be any extension of A. Suppose that for any degree n polynomial $p(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in K[x]$ there is a nonconstant Tschirnhaus transformation $T(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1}$ with $b_i \in L$ such that the transformed polynomial is of the form*

$$q(y) = y^n + A_r y^{n-r} + \ldots + A_{n-1}y + A_n$$

and such that $\mathrm{RD}(L/K) \leq n - r$. Then

$$RD(n) \leq \max\{n - r, \mathrm{RD}(n-1)\}.$$

Proof. Let M/K be any degree n extension with K an extension of A. We will show $\mathrm{RD}_A(M/K) \leq n - r$.

By the primitive element theorem, $M = K(\lambda)$ for some $\lambda \in M$. Let $p(x) = x^n + a_1x^{n-1} + \ldots + a_n$ be the minimal polynomial of λ. By hypothesis, there is a Tschirnhaus transformation T with coefficients in a field L such that $T(\lambda)$ is a root of $q(y) = y^n + A_{r+1}y^{n-r-1} + \ldots + A_{n-1}y + A_n$ and $\mathrm{RD}(L/K) \leq n - r$.

Now consider the field $L(T(\lambda))$. Note that λ is a solution to

$$\gcd(T(x) - T(\lambda), p(x)).$$

The degree of this polynomial is the number of roots of $p(x)$ which map to the same value $T(\lambda)$. Since p is a minimal polynomial, it is irreducible, and has all roots distinct. Since T is degree at most $n-1$, it can map at most $n-1$ distinct values to $T(\lambda)$. Hence λ is a root of a degree at most $n-1$ polynomial over $L(T(\lambda))$.

Thus there is a degree $n-1$ extension $L'/L(T(\lambda))$ which contains λ. Since L' is an extension of L (and hence of K), L' contains $M = K(\lambda)$.

We now have a tower of extensions

$$K \hookrightarrow L \hookrightarrow L(T(\lambda)) \hookrightarrow L'$$

with $M \subset L'$.

By assumption, $\mathrm{RD}(L/K) \leq n - r$.

Moreover, we can show

$$\mathrm{RD}(L(T(\lambda))/L) = n - r.$$

To see this, note that $T(\lambda)$ is a root of

$$q(y) = y^n + A_r y^{n-r} + \ldots + A_{n-1} y + A_n.$$

Making a further substitution $z = (A_{r-1}/A_r)y$ and scaling produces a monic polynomial

$$z^n + A'_r z^{n-r} + \ldots + A'_{n-1} z + A'_n$$

with $A'_r = A'_{r-1}$. It follows that

$$\mathrm{ed}(L(T(\lambda))/L) \leq n - r.$$

Finally, $\mathrm{RD}(L'/L(T(\lambda))) \leq \mathrm{RD}(n-1)$, by Lemma 2.

Thus we have

$$\begin{aligned} \mathrm{RD}(M/K) &\leq \max\{\mathrm{RD}(L/K), \mathrm{RD}(L(T(\lambda)/L), \mathrm{RD}(L'/L(T(\lambda)))\} \\ &= \max\{n - r, \mathrm{RD}(n-1)\} \end{aligned}$$

as claimed. □

4.2 Deriving Bounds on $\mathrm{RD}(n)$

The lemmas of the previous section, particularly lemma 3, can be used to translate results from the theory of Tschirnhaus transformations into bounds on resolvent degree. In this section we carry out this translation for the low degree examples previously considered, including Bring's result for $n \geq 5$.

It is well known that any polynomial $p(x)$ over K can be put into the form

$$y^n + A_2 y^{n-2} + \ldots + A_n$$

by means of a linear change of variables $y = b_0 + b_1 x$. Viewing this as a linear Tschirnhaus transformation defined over K, we can apply lemma 3 to conclude

$$\mathrm{RD}(n) \leq \max\{n-2, \mathrm{RD}(n-1)\} = n-2.$$

Next, Tschirnhaus proved that any polynomial p of degree $n \geq 3$ over K can be put into the form

$$q(y) = y^n + A_3 y^{n-3} + \ldots + A_n$$

by means of a Tschirnhaus transformation T defined over an extension L/K of weight 2 (in fact of degree 2). Hence by lemma 3, for $n \geq 3$,

$$\mathrm{RD}(n) \leq \max\{n-3, \mathrm{RD}(n-1)\}.$$

But $\mathrm{RD}(n-1) \leq n-1-2 = n-3$ by the result of the previous paragraph, so we have $\mathrm{RD}(n) \leq n-3$.

Finally, let us consider Bring's result for $n \geq 5$. This says that given any field K (over A) and any degree $n \geq 5$ polynomial p over K, we can produce a Tschirnhaus transfomation T over a field L with $\mathrm{wt}(L/K) \leq 3$ and such that T transforms p into the form $q(y) = y^n + A_4 y^{n-4} + \ldots + A_n$. By lemma 2, $\mathrm{RD}(L/K) \leq \mathrm{RD}(3) = 1$, and so by lemma 3,

$$\mathrm{RD}(n) \leq \max\{n-4, \mathrm{RD}(n-1)\}.$$

Since $n-1 > 3$, we have $\mathrm{RD}(n-1) \leq n-1-3 = n-4$ by the previous paragraph, so

$$\mathrm{RD}(n) \leq n-4$$

for $n \geq 5$.

5 Removal of Four Terms by Means of a Tschirnhaus Transformation

Bring's result, discussed in section 3.3, allows any degree n polynomial with $n \geq 5$ to be transformed to a polynomial of the form

$$q(y) = y^n + A_1 y^{n-1} + \ldots + A_{n-1}^y + A_n$$

with $A_1 = A_2 = A_3 = 0$ and $A_4 = A_5$, by means of a solvable Tschirnhaus transformation. Informally, any such polynomial can be put in an "$(n-4)$-parameter form". At the end of the preceding section, we saw that this impliles $\mathrm{RD}(n) \leq n - 4$ for $n \geq 5$

The natural next case to consider is what bound on n guarantees a polynomial of degree n can be put into an $(n-5)$-form by means of a Tschirnhaus transformation defined over an algebraic extension L/K satisfying some notion of bounded complexity? Specifically we will consider results where either the weight or the resolvent degree of L/K is subject to some given bound. In particular, this allows for the determination of n such that $\mathrm{RD}(n) \leq n - 5$.

To make this more precise we first briefly review the notion of a Tschirnhaus transformation. Let

$$p(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n \in K[x].$$

Recall that a *Tschirnhaus transformation* is a polynomial transformation of the roots of p. More precisely, we consider Tschirnhaus transformations of the form

$$T(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}.$$

The coefficients b_i of T are to taken to lie in an extension L/K satisfying some bound on either $\mathrm{wt}(L/K)$ or $\mathrm{RD}_A(L/K)$.

Given such a transformation T, if p has roots $\lambda_1, \ldots, \lambda_n$, then we form the *transformed polynomial*

$$q(x) = \prod_{i=1}^{n}(x - T(\lambda_i)) = x^n + A_1 x^{n-1} + \ldots + A_{n-1}x + A_n.$$

The A_i are homogeneous degree i polynomials in $K[b_0, \ldots, b_{n-1}]$, and $q \in L[x]$. We consider the problem of determining $b_0, \ldots, b_{n-1}$ such that $A_1 = A_2 = A_3 = A_4 = 0$.

Since A_i is a homogeneous degree i polynomial in $K[b_0, \ldots, b_n]$, the vanishing locus of A_i is a degree i hypersurface $V_i = V(A_i)$ in $\mathbb{P}^{n-1}_K$. Thus it suffices to consider the slightly more general problem: given hypersurfaces V_1, V_2, V_3, V_4 in $\mathbb{P}^{n-1}_K$ with $\deg(V_i) = i$, does there exist a point in the intersection

$$V_1 \cap V_2 \cap V_3 \cap V_4$$

defined over an extension L/K of appropriately bounded complexity?

In these terms, the results described in this section can be summarized in the following proposition.

Proposition 8. *Let V_1, V_2, V_3, V_4 be hypersurfaces in $\mathbb{P}^{n-1}_K$ with $\deg(V_i) = i$, and let*

$$X = V_1 \cap V_2 \cap V_3 \cap V_4.$$

(a) If $n \geq 10$, then X contains a point defined over a solvable extension of K. (In fact, over a weight 4 extension.)

(b) If $n \geq 9$, then X contains a point defined over an extension L/K with $\mathrm{RD}_A(L/K) \leq 4$.

(c) If $n \geq 9$ then X contains a point defined over an extension L/K with $\mathrm{wt}(L/K) \leq 5$.

These results come from several different sources. For part (a), work of Jerrard, Hamilton, and Sylvester shows that $n = 10$ is sufficient.[13, 8, 18]

Part (b) is due to an argument of Hilbert, using the existence of 27 lines on a cubic surface to show that that $n = 9$ suffices if we require only that T be defined over a field L with $\mathrm{RD}_A(L/K) \leq 4$.[12]

The statement of part (c) was first proposed by Raymond Garver as a refinement of Hilbert's result: that T could be determined over a field of weight 5 when $n = 9$.[7] Unfortunately, Garver's proof is erroneous, as we show in section 5.3. Moreover, there appears to be a potential obstruction to such a result: Hilbert's method for finding the necessary Tschirnhaus transformation requires finding a line on a cubic surfaces; the monodromy group of this problem is known and prohibits a solution of weight 5 in general.[9]

On the other hand, Hilbert's claim *can* be strengthened to exactly Garver's assertion. Correct proofs of this were given independently by Dixmier and Segre.[15, 5] In section 5.4 we describe the core geometric idea in Segre's approach and how it differs from Hilbert's; in particular, Segre's method does

not require the determination of a line on a cubic surface, and so avoids the aforementioned monodromy obstruction.

5.1 Transformations over Solvable Extensions of K

In this section we consider the following problem:

Problem 1. *What is the minimal degree n such that, for any polynomial $p(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$ in $K[x]$, we can determine a Tschirnhaus transformation $T(x) = b_0 + b_1 x + \ldots + b_n x^{n-1}$ with coefficients in some solvable extension L of K, such that in the transformed polynomial*

$$q(x) = \prod_{i=1}^{n}(x - T(\lambda_i)) = x^n + A_1 x^{n-1} + \ldots + A_{n-1}x + A_n$$

we have $A_1 = A_2 = A_3 = A_4 = 0$?

In other words, when is there a "formula in radicals" to determine a Tschirnhaus transformation which removes 4 intermediate terms from a given polynomial? As mentioned in the preceding section, A_i is a homogeneous degree i polynomial in $K[b_0, \ldots, b_n]$. Thus the vanishing locus of A_i is a degree i hypersurface in $\mathbb{P}^{n-1}_K$, and to determine a point on the intersection of these hypersurface is to determine the necessary Tschirnhaus transformation. This motivates the following reformulated question:

Problem 2. *What is the minimal n such that, given any hypersurfaces V_1, V_2, V_3, V_4 of degree $1, 2, 3, 4$ in $\mathbb{P}^{n-1}_K$, the intersection $V_1 \cap V_2 \cap V_3 \cap V_4$ is guaranteed to contain at least one point defined over a solvable extension of K?*

It should be observed that this is not *quite* equivalent to our original problem, since we have passed from the vanishing loci of $A_1, \ldots, A_4$ (which are specific polynomials in $b_0, \ldots, b_n$ determined by the set-up of the problem and the choice of polynomial p) to four *arbitrary* hypersurfaces, about which only the degree is known. However, in all that follows, we will make no use of the specific form of the polynomials $A_1, \ldots, A_4$, only keeping track of their degree and the degrees of any auxiliary equations that arise.

Now, if $n - 1 < 4$, then $V_1 \cap V_2 \cap V_3 \cap V_4$ may contain no points at all (even over the algebraic closure $\overline{K}$), so clearly we need at least $n - 1 \geq 4$.

But for $n-1=4$, by Bezout's theorem there will in general be $4!=24$ points of intersection, which are governed by an equation of degree 24 which need not be solvable. We can ensure T is defined over a solvable extension of K if T can be determined without solving any equation of degree greater than 4. (In other words, if T's field of definition can be obtained by a tower of extensions of degree at most 4, then this field is necessarily solvable.) This was first shown to be possible by Jerrard, for $n=11$.[13] Jerrard's ideas were subsequently clarified, refined, and extended first by Hamilton and then Sylvester.[8, 18] Below we sketch an informal proof of this result, hewing close to Sylvester's treatment.

This result can also be deduced from a very simple calculation once we have developed the ideas and notation of Sylvester's "method of obliteration" in section 8. Indeed, the method derives from a relatively straightforward generalization of the proof below. Here our goal is to emphasize the main geometric ideas without getting bogged down in the combinatorial bookkeeping of the more general obliteration formulae.

Proposition 9 (Jerrard, Hamilton, Sylvester)**.** *Given hypersurfaces V_1, V_2, V_3, V_4 of degree 1, 2, 3, 4 in $\mathbb{P}^{10}_K$, there exists a point in the intersection $V_1 \cap V_2 \cap V_3 \cap V_4$ over a solvable extension of K. In particular, there exists a point over an extension of weight 4.*

Proof. The key idea is to first find a line contained in the intersection $V_1 \cap V_2 \cap V_3$. Then we can intersect this line with V_4; and computing the points of intersection requires only solving an equation degree 4.

Thus our problem becomes: how to (solvably) determine such a line? The idea is as follows: find a point $Q \in V_1 \cap V_2 \cap V_3$, then look for a point $X=(x_0,\ldots,x_{10})$ such that $X+\lambda Q$ is in $V_1 \cap V_2 \cap V_3$ for any $\lambda \in K$. To find such a point we view $f_i(X+\lambda Q)$ as a polynomial in λ and require that every coefficient of λ vanishes. For example, for $f_2(X+\lambda Q)$ we have the constant coefficient, the coefficient of λ, and the coefficient of λ^2; these coefficients are, respectively, of degree 2, 1, and 0 with respect to $x_0,\ldots,x_{10}$. Assembling *all* such coefficients from $f_i(X+\lambda Q)$ we find that X must satisfy a system of equations with one equation of degree 3, two equations of degree 2, and three equations of degree 1. Actually, we must add one more equation of degree one: we must ensure X is not a multiple of Q, and we can do this by choosing a hyperplane in $\mathbb{P}^9$ disjoint from Q.

Now to solve this new system, we repeat our trick: we first determine a line lying in the intersection of two quadrics and four hyperplanes, then

intersect this line with the remaining cubic hypersurface. Repeating the strategy of the previous paragraph, we can find such a line by finding a point solution to a system with two quadrics and seven hyperplanes.

Finally, we need to find a point on the intersection of two quadrics and seven hyperplanes. But any quadric hypersurface in $\mathbb{P}^3_K$ contains a line defined over a quadratic extension of K, so we can solvably determine a line on the the intersection of a single quadric hypersurface and seven hyperplanes in $\mathbb{P}^{10}$, then intersect this line with the single remaining quadric, and we're done. □

In particular, this implies that one can solvably determine a Tschirnhaus transformation removing the first four intermediate terms from any polynomial of degree $n \geq 11$. In fact, as Hamilton recognized, this bound can be improved slightly to $n \geq 10$ with only a minor modification to the above proof. After reducing the problem to finding a point on the intersection of two quadrics and seven hyperplanes, instead of looking for a line, we can find a plane contained in the seven hyperplanes. Then intersecting the two quadrics with this plane, the problem is reduced to finding a point on the intersection of two plane conics; this requires at worst the solution of a degree 4 equation. The ambient dimension necessary for this procedure to succeed is just the number of equations in the system, $n = 2 + 7 = 9$. Hence we obtain:

Proposition 10 (Hamilton, Sylvester)**.** *Given hypersurfaces V_1, V_2, V_3, V_4 of degree 1, 2, 3, 4 in $\mathbb{P}^9_K$, there exists a point in the intersection $V_1 \cap V_2 \cap V_3 \cap V_4$ over a solvable extension of K. In particular, such a point can be determined over an extension of weight 4.*

Thus for $n \geq 10$, given a polynomial $p \in K[x]$ of degree n there exists a Tschirnhaus transformation T defined over a solvable extension of K such that the transformed polynomial q is of the form

$$q(x) = x^n + A_5 x^{n-5} + \ldots + A_{n-1} x + A_n.$$

This remains the lowest known bound for this particular formulation of the problem. In the next section, we will discuss Hilbert's bound of $n \geq 9$ for a variant of the problem in which a weaker constraint is placed on the field of definition of T.

5.2 Transformations over Fields of Bounded Resolvent Degree: Hilbert's Argument

In the previous section we saw that for any field K extending the fixed algebraically closed base field A, and any degree n polynomial $p(x) \in K[x]$ with $n \geq 10$, p can be put into the $n-4$ parameter form

$$q(x) = x^n + A_5 x^{n-5} + \ldots + A_{n-1}x + A_n$$

by means of a Tschirnhaus transformation T defined over a solvable extension L of K. In particular, this implies $\mathrm{RD}(L/K) = 1$. By lemma 3, then, we have

$$\mathrm{RD}(n) \leq \max\{n-5, \mathrm{RD}(n-1)\}.$$

for $n \geq 10$. Moreover, Bring's result tells us that $\mathrm{RD}(n-1) \leq n-1-4 = n-5$ since $n-1 \geq 5$, so we have

$$\mathrm{RD}(n) \leq n-5$$

for $n \geq 10$.

To obtain this result it would have sufficed to show that T could be determined over an extension L of K with $\mathrm{RD}(L/K) \leq n-5$; the condition that L/K be solvable (so that $\mathrm{RD}(L/K) \leq 1$) is far stronger than what is needed.

In a short 1927 paper Hilbert sketched a proof of the following proposition.[12]

Proposition 11 (Hilbert)**.** *Let $n \geq 9$ and let K be any extension of A. Given hypersurfaces V_1, V_2, V_3, V_4 in $\mathbb{P}^{n-1}_K$ with $\deg(V_i) = i$, the intersection $V_1 \cap V_2 \cap V_3 \cap V_4$ contains a point defined over an extension L/K with $\mathrm{RD}(L/K) \leq 4$.*

An immediate corollary is that any degree $n \geq 9$ polynomial $p(x) \in K[x]$ can be put into the form

$$q(x) = x^n + A_5 x^{n-5} + \ldots + A_{n-1} + A_n$$

by means of a Tschirnhaus transformation defined over an extension L/K with $\mathrm{RD}(L/K) \leq 4 \leq n-5$. Thus

$$\mathrm{RD}(n) \leq n-5 \quad \text{for } n \geq 9.$$

We now briefly summarize Hilbert's argument. As in the work of Sylvester and Hamilton, the strategy is to find a line contained in the intersection

of $V_1 \cap V_2 \cap V_3$, then intersect this line with V_4 to determine a point. The intersection $V_1 \cap V_2$ determines a quadric surface in $\mathbb{P}^{n-2}$, and when $n-2 \geq 7$ this quadric surface contains a 3-plane defined over a solvable extension L_0 of K. Intersecting this 3-plane with V_3, the problem is reduced to finding a line on a cubic surface in $\mathbb{P}^3_{\overline{L_0}}$ defined over some suitable extension of L_0. Since L_0 is solvable, $\mathrm{RD}(L_0/K) = 1$.

There are 27 such lines, determined by the roots of an equation of degree 27. In general these will be defined over a solvable extension of L_0. On the other hand, the equation of a general cubic surface can be put in the "pentahedral form"

$$x_0^3 + x_1^3 + x_2^3 + x_3^3 + (v_0x_0 + v_1x_1 + v_2x_2 + v_3x_3)^3 = 0$$

over a degree 5 extension L_1/L_0. Since $\mathrm{RD}(5) = 1$, by lemma 2 we have $\mathrm{RD}(L_1/L_0) = 1$. Now, the coefficients of the degree 27 equation governing the lines on a cubic surface defined by an equation in pentahedral form can be taken to be polynomial functions of the four parameters v_0, v_1, v_2, v_3. It follows that there exists a line defined over an extension L_2/L_1 with $\mathrm{RD}(L_2/L_1) \leq 4$. Finally, the points of intersection of this line with V_4 are defined over a degree 4 extension L_3/L_2, with $\mathrm{RD}(L_3/L_2) \leq \mathrm{RD}(4) = 1$. Thus there is a point of $V_1 \cap V_2 \cap V_3 \cap V_4$ defined over L_3, and we have $\mathrm{RD}(L_3/K) \leq 4$ since L_3/K factors over a tower of extensions each of resolvent degree at most 4.

5.3 An Analysis of Garver's Proof

A general cubic surface in $\mathbb{P}^3_{\overline{K}}$ contains 27 lines, corresponding to the roots of an equation of degree 27. Given a homogenous degree 3 polyomial $f \in K[X, Y, Z, W]$, how hard is it to determine one of the lines lying on $V(f)$? On the one hand, as Hilbert observed, since a general cubic surface can be put into the "pentahedral form"

$$X^3 + Y^3 + Z^3 + W^3 + (v_1X^3 + v_2Y^3 + v_3Z^3 + v_4W^3),$$

the degree 27 equation governing the lines depends only on the four parameters v_1, v_2, v_3, v_4; it follows that the lines are defined over a field extension L/K with $\mathrm{RD}(L/K) \leq 4$. On the other hand, it was shown by Harris that the monodromy group of the 27 lines is $W(E_6)$, and that this is an obstruction to determining a line over any solvable extension of K.[9] The same

monodromy obstruction implies a line cannot be determined over any weight 5 extension.

This last statement is in contradiction with Garver's work on Tschirnhaus transformations for degree $n \geq 9$ polynomials: following Hilbert's sketch, Garver claimed one could reduce a general degree 9 polynomial to a 4-parameter form *without solving any equation of degree greater than 5.* To resolve the conflict, we turn now to a careful analysis of Garver's proof, and show that his argument, while clever, contains a fatal error.

Beginning with a homogeneous degree three polynomial in the pentahedral form

$$f(X,Y,Z,W) = X^3 + Y^3 + Z^3 + W^3 + (v_1X^3 + v_2Y^3 + v_3Z^3 + v_4W^3)$$

Garver makes the substitutions

$$\begin{aligned} X &= s + 1 \\ Y &= a_2 s + b_2 \\ Z &= (-v_1 - v_2 a_2)s/v_3 + b_3 \\ W &= b_4. \end{aligned}$$

then shows one can solve for a_2, b_2, b_3, b_4 in terms of v_1, v_2, v_3, v_4 so that the polynomial $f(X(s), Y(s), Z(s), W(s))$ vanishes identically in s. This is sufficient to determine a line contained in $V(f)$ provided that the resulting expressions $X(s), Y(s), Z(s), W(s)$ are not all scalar multiples of one another; in this case we would determine only a point in projective space. We will show that this is indeed what happens.

First, to make the s^2 term of $f(X(s), Y(s), Z(s), W(s))$ vanish, we must solve

$$1 + a_2^3 - \left(\frac{v_1 + v_2 a_2}{v_3}\right)^3 = 0$$

for a_2, then set $a_3 = -(v_1 + v_2 a_2)/v_3$. Observe that $a_2 \neq 0$ and

$$1 + a_2^3 + a_3^3 = 0.$$

Next, to make the coefficients of s^2 and s vanish, we must solve the system

$$1 + a_2^2 b_2 + a_3^2 b_3 = 0.$$

$$1 + a_2 b_2^2 + a_3 b_3^2 = 0.$$

Since $1 + a_2^3 + a_3^3 = 0$, we can obtain a solution by taking $b_2 = a_2$, $b_3 = a_3$. In fact, this is the *only* solution: we can solve for b_2 in terms of b_3 to reduce this system to the single quadratic equation

$$\left(a_3 + \frac{a_3^4}{a_2^3}\right) b_3^2 - \frac{2a_3^2}{a_2^3} b_3 + \frac{1 + a_2^3}{a_2^3} = 0.$$

This has discriminant

$$\begin{aligned}\left(-\frac{2a_3^2}{a_2^3}\right)^2 - 4\left(a_3 + \frac{a_3^4}{a_2^3}\right)\left(\frac{1 + a_2^3}{a_2^3}\right) &= -\frac{a_3(a_2^3 + a_3^3 + 1)}{a_2^3} \\ &= 0,\end{aligned}$$

since $1 + a_2^3 + a_3^3 = 0$, so has a unique solution.

Finally, the term free of s is

$$1 + b_2^3 + b_3^3 + b_4^3 + (v_1 + v_2 b_2 + v_3 b_3 + v_4 b_4)^3,$$

but

$$1 + b_2^3 + b_3^3 = 1 + a_2^3 + a_3^3 = 0$$

and

$$v_1 + v_2 b_2 + v_3 b_3 = v_1 + v_2 a_2 + v_3 a_3 = v_1 + v_2 a_2 + v_3(-v_1 - v_2 a_2)/v_3 = 0,$$

so the equation to solve for b_4 simplifies to

$$(1 + v_4^3) b_4^3 = 0$$

and $b_4 = 0$ is the only solution.

Thus Garver's substitution becomes

$$\begin{aligned} X &= s + 1 \\ Y &= a_2(s + 1) \\ Z &= a_3(s + 1) \\ W &= 0, \end{aligned}$$

so every value of s yields the same point in projective space.

This shows that a substitution of Garver's proposed form cannot determine a line on a cubic surface, so his proof cannot succeed. On the other hand, the *result* claimed by Garver is actually true, as we discuss in the next section.

5.4 Segre's Result

Hilbert's 1927 paper on Tschirnhaus transformations in the degree $n \geq 9$ case appears to have been the first to frame the problem in terms of the *resolvent degree* (though he did not use this term) of the field over which the transformation is defined, rather than its *weight*.[12] This was a powerful shift in perspective which paved the way for much of the recent progress on Tschirnhaus transformations in [21, 16, 10].

Nonetheless, there continued to be interest post-Hilbert in determining more precisely the degrees of the equations which must be solved to determine Tschirnhaus transformations of certain kinds – that is, in bounding the weight of the field of definition of the transformation. For example, Garver's work raises the question: is it possible to find a Tschirnhaus transformation reducing a general degree 9 polynomial to an $n-5$ parameter form without solving any equation of degree greater than 5?

In section 5.3, we showed that Garver's attempt to provide a proof using this method was not successful. Perhaps surprisingly, then, this was proven to be possible by Segre in 1945.[15] Segre's argument does *not* require the determination of a line lying on a cubic surface, and so avoids any monodromy obstruction.

Proposition 12 (Segre)**.** *Suppose $n \geq 9$. For any hypersurfaces V_1, V_2, V_3, V_4 in $\mathbb{P}^{n-1}_K$ with $\deg(V_i) = i$, there is an extension L/K of weight at most 5 such that the intersection*

$$V_1 \cap V_2 \cap V_3 \cap V_4$$

contains an L-point.

In particular, any polynomial of degree $n \geq 9$ can be put into an $n-5$ parameter form by means of a Tschirnhaus transformation which can be determined without solving any equation of degree greater than 5.

Proof. It is sufficient to find a line contained in $V_1 \cap V_2 \cap V_3$ defined over an extension of weight at most 5. As in the proof of Proposition 9 to determine the necessary line we first find a point $Q \in V_1 \cap V_2 \cap V_3$, then look for a point P such that $P + \lambda Q$ is in $V_1 \cap V_2 \cap V_3$ for any λ; then P must satisfy a system S with 1 cubic, 2 quadrics, and 3 linear equations.

To complete the proof we must show that S admits a solution over an extension L'/L with $\mathrm{wt}(L'/L) \leq 5$. It suffices here to find a line satisfying the 2 quadrics and 3 linear equations. They key fact which Segre makes use of is that the intersection of two quadrics in $\mathbb{P}^4_L$ contains 16 lines, which are

defined over an extension of weight 5. Intersecting one of these lines with the remaining cubic equation gives the desired solution to S. $\square$

6 General Bounds for Removing r Terms

As before let A be an algebraically closed field of characteristic zero and let K be an extension of A. Thus far we have considered the problem of removing r terms from a degree n polynomial $p \in K[x]$ by means of a Tschirnhaus transformation in detail only for small values of r. To recap, the $r = 1$ case is the standard reduction of a polynomial to its depressed form, which requires only an A-linear change of variables. To remove $r = 2$ terms it is sufficient to solve a system of two polynomials – one linear and one quadratic – so this can always be done over a quadratic extension of K; in particular, for $n = 3$ this gives an alternative to Cardano's method for the solution of the cubic in radicals, as discussed in section 3. The $r = 3$ case is handled by Bring's analysis of the quintic (and its generalization to any $n \geq 5$ polynomial), which shows that the removal of 3 terms can always be accomplished solvably.

Finally, in the previous section we considered several distinct approaches to the problem of removing $r = 4$ terms from a degree n polynomial by means of a Tschirnhaus transformation. In this case we saw that the bound obtained for n depends on what restrictions are placed on the field extension L/K over which the necessary Tschirnhaus transformation is defined.

In this section, we consider the problem of removing an arbitrary number of terms r from a degree n polynomial in $K[x]$ by means of a Tschirnhaus transformation defined over L/K, subject to some restriction on L/K. More precisely, for some fixed restriction (or class of restrictions) on L/K, does there exist a function $F(r)$ such that for all $n \geq F(r)$, it is posible to reduce an arbitrary degree n polynomial $p \in K[x]$ to an $(n-r)$-parameter form by means of a Tschirnhaus transformation defined over L?

As in previous sections, we can recast this problem in geometric terms. Let

$$p(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n \in K[x].$$

Recall that to put p into an $(n-r)$-parameter form it suffices to determine values of $b_0, \ldots, b_{n-1} \in B$ such that applying the Tschirnhaus transformation

$$T(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}$$

to p yields a transformed polynomial

$$q(y) = y^n + A_1 y^{n-1} + \ldots + A_n$$

with $A_1 = \ldots = A_r = 0$. Each A_i is a homogeneous degree i polynomial in $K[b_0, \ldots, b_{n-1}]$, so determines a degree i hypersurface in $\mathbb{P}^{n-1}_{\overline{A}}$. We can then ask about special points on the intersection of these hypersurfaces.

For example, given hypersurfaces $V_1, \cdots, V_r$ in $\mathbb{P}^{n-1}_{\overline{K}}$ with $\deg(V_i) = i$, is there a function $F(r)$ such that if $n \geq F(r)$ the intersection

$$X = V_1 \cap \ldots V_r$$

is always guaranteed to contain a solvable point? A point of weight at most r? A point of resolvent degree at most $n - r$?

More generally, given a collection of hypersurfaces in $\mathbb{P}^{n-1}_{\overline{K}}$, are there lower bounds for n which depend only on the degrees of the hypersurfaces, such that their intersection is guaranteed to contain (respectively) a solvable point, a point of weight at most r, and a point of resolvent degree at most $n - r$? Each of these questions has been answered in the affirmative.

The first result of this kind is due to Hamilton, who showed that it was always possible to determine a point on the intersection of

$$V_1 \cap \ldots \cap V_r$$

by successively solving polynomial equations of degree at most r, provided the ambient dimension is sufficiently large; a point obtained via this method is necessarily defined over an extension of weight at most r. [8]

Hamilton's work was built upon and refined by Sylvester, who improved Hamilton's bounds and introduced a relatively straighforward computational method for determining the necessary dimension $n - 1$ in terms of r, known as the "method of obliteration".[18] Moreover, the method of obliteration can be applied to *any* system of homogeneous polynomials (of degree at most r) to produce a point of weight r in the solution set of that system.

In 1945, Brauer showed that it was possible to produce a *solvable* point in the solution set of any system of homogeneous polynomials, provided the ambient dimension was larger than some bound which depends only on the degrees of the polynomials.[1] In particular, for any r, it is possible to determine solvably a Tschirnhaus transformation reducing an arbitrary degree n polynomial to $(n - r)$-parameter form, provided n is sufficiently large relative to r. Brauer's work does not compute these bounds explicitly, only

proves that they exist. Recent work of Wooley sharpens Brauer's result to the following theorem.[22]

Theorem 1 (Wooley)**.** *Let $X \subseteq \mathbb{P}^n$ be a complete intersection of hypersurfaces defined over a field K of characteristic zero. Then X possesses a point defined over a solvable extension L of K with, moreover,* $\mathrm{wt}(L/K) \leq \deg(X)$*, provided only that*

$$\dim(X) \geq 2^{2^{\deg(X)}}.$$

Thus, a Tschirnhaus transformation reducing a degree n polynomial to an $(n-r)$-parameter form can always be found solvably provided that $n \geq 2^{2^{r!}} + r + 1$.

In a subsequent paper, Brauer showed that the intersection

$$V_1 \cap \ldots V_r \in \mathbb{P}^{n-1}_{\overline{K}}$$

contains a point defined over an extension L of K with $\mathrm{RD}(L/K) \leq n - r$ provided that $n \geq r!$.[2] This implies that

$$\mathrm{RD}(n) \leq n - r$$

for $n \geq r!$.

These remained the best general bound on $\mathrm{RD}(n)$ until the problem was revisited in work of Farb and Wolfson, who recast the theory of resolvent degree in geometric terms.[6] Brauer's bounds were improved upon significantly by work of Wolfson, with further refinements given by Sutherland.[21, 16]

In fact, the early work of Hamilton and Sylvester – while most naturally applicable to the context of bounded weight extensions – can be applied to the problem of bounding $\mathrm{RD}(n)$ using Tschirnhaus transformations. In section 8.2, we show that for several values of n this produces sharper bounds on $\mathrm{RD}(n)$ than any previously published. In the next few sections, we explore the method of obliteration and its applications in significant detail.

7 Points of Bounded Weight on Intersections of Quadrics

Let A be a field of characteristic zero, and let K be an extension of A. As we have seen, a number of problems in the theory of Tschirnhaus transformations can be reduced to finding special points (or special linear subspaces) on

intersections of certain projective hypersurfaces. In this section we consider the problem of finding points of bounded weight (that is, points defined of a tower of bounded-degree extensions of K) on the intersection of several quadric hypersurfaces in $\mathbb{P}^N_{\overline{K}}$ when N is large relative to the number of hypersurfaces. This leads to the introduction of a special case of Sylvester's method of obliteration. In the following section, the method of obliteration is developed for an arbitrary collection of hypersurfaces.

Let $Q_1, \ldots, Q_r$ be quadric hypersurfaces in $\mathbb{P}^N_K$, with $r \leq N$. The intersection $V = Q_1 \cap \ldots \cap Q_r$ may contain no K-points but contains points in some finite extension of K. For example, if $r = N$, there are in general 2^r points of intersection (over $\overline{K}$) which are governed by an equation of degree 2^r, so V contains points defined over a degree 2^r extension of K.

When N is large relative to r, there will in general be infinitely many points of intersection, and it becomes possible to determine such a point by solving equations of lower degree. For example, we shall see that for sufficiently large N, it is possible to determine a point of intersection of r quadrics by solving only equations of degree 2; the resulting point is defined over a field L which can be obtained from a finite tower of quadratic extensions of K. Note that the total *degree* of the extension L/K is not necessarily less than 2^r in this case, but nonetheless in some sense the complexity of the extension has been reduced. This is captured by the notion of weight of a field extension. For convenience, we recall the definition here:

Definition 7.1. A finite extension L/K is of *weight* d if d is the minimal value such that L/K factors as a tower of extensions each of degree at most d.

We will say a point is of weight d if it is defined over a weight d extension of K. We now considering the following problem.

Problem 3. *Determine a function $F(r, d)$ such that, for any $N \geq F(r, d)$, and any quadric hypersurfaces $Q_1, \ldots, Q_r$ in $\mathbb{P}^N_{\overline{K}}$ defined over K, the intersection $V = Q_1 \cap \ldots \cap Q_r$ contains a point of weight d.*

In investigating this question the following classical lemma will be useful.

Lemma 4 (Linear Subspaces of Quadric Hypersurfaces)**.** *For any $k \in \mathbb{N}$, a quadric hypersurface $Q \subset \mathbb{P}^N_{\overline{K}}$ defined over K contains a k-plane defined over a weight 2 extension of K provided that $N \geq 2k + 1$.*

Proof. We may assume Q is the vanishing locus of a diagonal quadratic form

$$F(x_0, \ldots, x_n) = \sum_{i=0}^{n} (-1)^i c_i x_i^2$$

Over a suitable solvable extension L of K, we can factor each pair of terms $c_i x_i^2 - c_{i+1} x_{i+1}^2$ as $(\sqrt{c_i} x_i + \sqrt{c_{i+1}} x_{i+1})(\sqrt{c_i} x_i - \sqrt{c_{i+1}} x_{i+1})$.

If n is even, the system

$$\begin{aligned} c_0 &= 0 \\ \sqrt{c_1} x_1 + \sqrt{c_2} x_2 &= 0 \\ \sqrt{c_3} x_3 + \sqrt{c_4} x_4 &= 0 \\ &\vdots \\ \sqrt{c_{n-1}} x_{n-1} + \sqrt{c_n} x_n &= 0 \end{aligned}$$

defines a hyperplane over L and contained in Q, of dimension $n - n/2 - 1 = n/2 - 1$.

Otherwise, if n is odd, then

$$\begin{aligned} \sqrt{c_0} x_1 + \sqrt{c_1} x_1 &= 0 \\ \sqrt{c_2} x_2 + \sqrt{c_3} x_3 &= 0 \\ &\vdots \\ \sqrt{c_{n-1}} x_{n-1} + \sqrt{c_n} x_n &= 0 \end{aligned}$$

defines a hyperplane over B and contained in Q of dimension $n - n/2 = n/2$. □

We now consider the special case of $d = 2$ in more detail. Returning to our problem, for $r = 1$, it is clear $F(1, 2) = 1$; this just says any quadric hypersurface in $\mathbb{P}^1_K$ contains a point defined over a quadratic extension of K. For $r = 2$, we have $F(2, 2) \geq 3$; if $N = 1$, the expected number of points of intersection (even over $\overline{K}$) is zero, and for $N = 2$ we expect 4 points of intersection governed by an equation of degree 4. By the lemma, in fact $F(2, 2) = 3$: any quadric $Q_1 \in \mathbb{P}^3_{\overline{K}}$ contains a line defined over a quadratic extension of K, and the intersection of this line with the quadric Q_2 is governed by another degree 2 equation, so that a point of intersection can be determined after taking two successive quadratic extensions of K.

For larger r, one strategy is to proceed inductively: first determine m such that for any field L, $Q_1 \cap \ldots \cap Q_{r-1} \subset \mathbb{P}^m_{\overline{K}}$ is guaranteed to contain a point defined over a weight two extension of L, then using the lemma determine N such that $Q_r \subset \mathbb{P}^N_{\overline{K}}$ contains an m-plane defined over a quadratic extension L of K. In his paper on Tschirnhaus transformations, B. Segre pursues this strategy. [15] This leads to the following lemma:

Lemma 5 (Segre)**.** *Given r quadric hypersurfaces $Q_1, \ldots, Q_r$ in $\mathbb{P}^N_{\overline{K}}$, a point of $Q_1 \cap \ldots \cap Q_r$ can be determined by solving equations of degree at most 2 provided $N \geq 2^r - 1$.*

Equivalently, $Q_1 \cap \ldots \cap Q_r$ contains a point defined over a field L with $\mathrm{wt}(L/K) \leq 2$.

Thus $F(r, 2) \leq 2^r - 1$.

This bound on $F(r, 2)$ is not sharp; in fact, the strategy described above is highly inefficient. In the next section we use methods of Sylvester to produce a bound for $F(r, 2)$ which is quadratic in r. As a historical aside: though Sylvester's work on Tschirnhaus transformations predates Segre's by several decades, Segre's bound of $n \geq 157$ for the removal of 6 terms from a degree n equation is considerably worse than Sylvester's bound of $n \geq 45$ for the same problem; this is largely due to the inefficiency of Segre's method for dealing with quadrics. (It seems that Segre was not aware of Sylvester's work on the problem.)

7.1 Weight 2 Points of Quadrics and Sylvester's Method of Obliteration

Sylvester, in his 1886 paper on Tschirnhaus transformations, considered the problem of finding solutions of bounded weight to systems of a given type (i.e., with a given number of equations of each degree). A complete description of Sylvester's method of obliteration is given in section 8; here we restrict attention to the special case of systems in which all equations are degree at most 2.

In the previous section our strategy for dealing with r quadrics was to find a hyperplane inside *one* of the quadrics of sufficiently high dimension that the remaining $r - 1$ quadrics could be dealt with inside of it. This allows the number of quadrics to be reduced by one, so that a bound on $F(r, 2)$ can be computed inductively; we have seen that the resulting bound

is exponential in r. A better strategy, due to Sylvester, is to find a line (defined over a field extension of weight 2) contained in $r-1$ of the quadrics, then intersect this line with the remaining quadric to determine a point of weight 2. This strategy leads to the following proposition, a special case of Sylvester's formula of obliteration.

Proposition 13 (Sylvester)**.** $F(r,2) \leq F(r-1,2) + r$.

Proof. By the preceding discussion, $F(r,2)$ is bounded above by the ambient dimension N necessary so that a line can be determined on the intersection of $r-1$ quadrics in $\mathbb{P}^N_K$ over a weight 2 extension of K. The idea will be to reduce this problem to finding a weight 2 point of some larger system.

To that end, let $f_1, \ldots, f_{r-1}$ be the homogeneous polynomials defining the $r-1$ quadric hypersurfaces. Provided that $N \geq F(r-1,2)$, we can find a weight 2 point Q satisfying $f_1(Q) = \ldots = f_{r-1}(Q) = 0$. We now seek a point $X = (x_1, \ldots, x_N)$ such that $X + \lambda Q$ is also a solution to $f_1, \ldots, f_{r-1}$ for all λ; this will give the desired line.

For each i, we can expand $f_i(X + \lambda Q)$ as a polynomial in λ; we require that this polynomial vanish identically. In particular, the linear and constant coefficients of the λ-polynomial must vanish, and these are (respectively) degree 1 and degree 2 homogeneous polynomials in terms of $x_1, \ldots, x_N$.

Repeating this process for all $i = 1, \ldots, r-1$ yields a system of $r-1$ quadrics and $r-1$ linear equations. Further, we need to ensure that the point X is distinct from Q; to do this, we simply choose any hyperplane $\mathbb{P}^{N-1}_K$ disjoint from $\{Q\}$, which amounts to imposing one additional linear constraint.

Thus to find a line in the intersection of $r-1$ quadrics, defined over a field extension of weight 2, it suffices to find a weight 2 point in the intersection of $r-1$ quadrics and r linear equations. It follows that $F(r,2) \leq F(r-1,2) + r$. □

Corollary 1. $F(r,2) \leq \frac{r(r+1)}{2}$.

Proof. Applying the proposition $r-1$ times, we have

$$F(r,2) \leq F(1,2) + 2 + 3 + \ldots + r.$$

But $F(1,2) = 1$, so

$$F(r,2) = 1 + 2 + \ldots + r = \frac{r(r+1)}{2}.$$

□

7.2 Points of Weight d on the Intersection of r Quadrics

In the previous section we showed that $F(r,2) \leq r(r+1)/2$. That is, given quadrics $Q_1, \ldots, Q_r$ in $\mathbb{P}^N_{\overline{K}}$, we can find a point of weight 2 in the intersection $V = Q_1 \cap \ldots \cap Q_r$ provided that that ambient dimension N is at least $r(r+1)/2$. At the other extreme, we have $F(r,d) = r$ for $d \geq 2^r$; in this case, it suffices to take a single degree 2^r extension of K to determine a weight 2^r point. We now turn our attention to the intermediate case $2 < d < 2^r$.

For $d = 2$ it was necessary to disentangle the r quadrics one at a time, producing a system of dependent but *not simultaneous* equations. For $d = 2^r$, we are free to dispatch with the entire simultaneous system in one stroke. With an intermediate bound on weight, we can deal with a subset of the quadrics simultaneously; for example, if $d = 4$, and we wish to find a weight d point on the intersection of r quadrics, we could first find a line on $r-1$ of the quadrics, and intersect this line with the remaining quadric; or we could find a plane on $r-2$ of the quadrics, and intersect the two remaining quadrics with this plane (which may require a degree 4 extension). For $d = 8$, we could look for a 3-plane on $r-3$ of the quadrics, dealing with the remaining 3 simultaneously within that 3-plane, and so on.

To help keep track of all these possibilities, we introduce some new notation.

Definition 7.2. Let $F(r,d,k)$ denote the minimal ambient dimension N such that it is always possible to find a k-plane on the intersection of r quadrics in $\mathbb{P}^N_{\overline{K}}$, defined over a weight d extension L of K.

Thus for example $F(r,d,0) = F(r,d)$ (a 0-plane is just a point), and in the proof of Sylvester's bound on $F(r,d)$ we used the rule $F(r,2,0) \leq F(r-1,2,1)$. More generally, for any s such that $2^s \leq d$, we have the rule

$$F(r,d,0) \leq F(r-s,d,s).$$

That is, to determine a weight d point on the intersection of r quadrics, it suffices to find an s-plane of weight d inside $r-s$ of the quadrics, then intersect with the remaining s quadrics.

In order to use these rules to produce bounds on $F(r,d,0)$, we need additional rules of the form $F(r,d,s) \leq F(r',d,0) + c$. That is, we need to describe how to find s-planes of weight d by solving for weight d point solutions of some related system.

Lemma 6. *To determine an s-plane of weight d in the intersection of r quadrics it suffices to determine a point solution of weight d to a system of r quadrics and $s(r+1)$ linear equations. Thus*

$$F(r,d,s) \leq F(r,d,0) + s(r+1).$$

Proof. Let $Q_1, \ldots, Q_r$ be quadric hypersurfaces in $\mathbb{P}^N_K$, with each Q_i the vanishing locus of a degree 2 homogeneous polynomial f_i. We first find an $s-1$-plane of weight d contained in the intersection of r quadrics; this requires the ambient dimension to be at least $F(r,d,s-1)$. Let $P_1, \ldots, P_s$ be points which span this plane in the sense that any point in the plane can be written as $\lambda_1 P_1 + \ldots \lambda_s P_s$ for some $\lambda_1, \ldots, \lambda_s$. Then to determine an s-plane of weight d we need to find a point $X = (x_0, \ldots, x_N)$ of weight d such that

$$f_i(X + \lambda_1 P_1 + \ldots + \lambda_s P_s) = 0$$

for all i and all $\lambda_1, \ldots, \lambda_s$. Expanding this expression as a polynomial in the λ_j's, we require the coefficient of each term to vanish. The vanishing of the coefficients $\lambda_1, \ldots, \lambda_s$ imposes s linear conditions on $x_1, \ldots, x_N$, for each quadric Q_i. Since there are a total of r quadrics this leads to $s \cdot r$ linear equations. The vanishing of the constant coefficient is just the requirement that $f_i(P) = 0$, so the system to be satisfied contains $s \cdot r$ linear equations together with the r quadratic equations with which we started. Further, for $X, P_1, \ldots, P_s$ to span an s-plane, we must ensure that X does not lie in the $(s-1)$-plane spanned by $P_1, \ldots, P_s$; we do this by imposing s additional linear conditions on X defining a complementary hyperplane.

Thus in total we require a point solution to a system with r quadrics, and $sr + s = s(r+1)$ linear equations. The minimal ambient dimension required to guarantee a weight d solution to such a system exists is $F(r,d,0) + s(r+1)$, so

$$F(r,d,s) \leq F(r,d,0) + s(r+1).$$

□

We now have two systems of rules,

$$F(r,d,0) \leq F(r-s,d,s) \quad (\text{if } d \geq 2^s)$$

and

$$F(r,d,s) \leq F(r,d,0) + s(r+1)$$

which we can apply inductively to produce bounds on $F(r, d, 0)$. However, it is not immediately clear which sequence of rule applications will produce the optimal bound. For example, if $r = 10$ and $d = 8$, we can separate up to 3 quadrics at a time. We could separate 3, then 3, then 3, then 1 quadrics at a time; or we could separate 3, then 3, then 2, then 2; or 2, 2, 2, 2, 2; and so on. What is the optimal sequence of segregations? An intuitively plausible guess is that it is always optimal to separate as many quadrics as possible (i.e., as permitted by the weight bound d) at each step. In the following section we prove that this guess is correct.

7.3 Optimal Sylvester Obliteration for Quadrics

Suppose we have a system of r quadrics in $\mathbb{P}^N_{\overline{K}}$. We wish to determine $F(r, d, 0)$ – that is, the minimal ambient dimension N such that our system is guaranteed to contain a point of weight d. We consider strategies involving successive applications of the obliteration formulae

$$F(r, d, 0) \leq F(r - s, d, s) \quad (\text{if } d \geq 2^s)$$
$$F(r, d, s) \leq F(r, d, 0) + s(r + 1)$$

to separate s quadrics at a time until we have reduced to a system of only linear equations. Such a strategy is specified by a choice of tuple

$$(s_1, \ldots, s_r)$$

with $0 \leq s_i \leq r$ and $2^s_i \leq d$ for all i and

$$r = \sum_{i=1}^{r} s_i.$$

In words, s_i is the number of quadrics to be separated in step i; if $s_i = 0$ we do nothing for that step. Requiring the s_i to sum to r ensures that we have reduced the problem to solving a purely linear system.

Example 2. *Let $r = 10$, $d = 8$. Then we can separate up to 3 quadrics in each step. We consider the strategies $(3, 3, 3, 1)$ and $(3, 3, 2, 2)$. The first*

strategy corresponds to the following sequence of rule applications

$$\begin{aligned} F(10,8,0) &\leq F(7,8,3) \leq F(7,8,0) + 3 \cdot (7+1) = F(7,8,0) + 24 \\ &\leq F(4,8,3) + 24 \leq F(4,8,0) + 24 + 3 \cdot (4+1) = F(4,8,0) + 39 \\ &\leq F(1,8,3) + 39 \leq F(1,8,0) + 39 + 3 \cdot (1+1) = F(1,8,0) + 45 \\ &\leq F(0,8,1) + 45 \\ &= 54 \end{aligned}$$

which produces the bound $F(10,8,0) \leq 54$. *The second corresponds to the sequence*

$$\begin{aligned} F(10,8,0) &\leq F(7,8,3) \leq F(7,8,0) + 3 \cdot (7+1) = F(7,8,0) + 24 \\ &\leq F(4,8,3) + 24 \leq F(4,8,0) + 24 + 3 \cdot (4+1) = F(4,8,0) + 39 \\ &\leq F(2,8,2) + 39 \leq F(2,8,0) + 39 + 2 \cdot (2+1) = F(2,8,0) + 45 \\ &\leq F(0,8,2) + 45 \\ &= 55 \end{aligned}$$

which produces the bound $F(10,8,0) \leq 55$.

Given a tuple $(s_1, \ldots, s_r)$ we can compute the number of linear equations generated by the strategy it represents, then minimize this number over all tuples subject to our given constraints.

Proposition 14. *For producing bounds on* $F(r,d,0)$ *using the obliteration formulae*

$$\begin{aligned} F(r,d,0) &\leq F(r-s,d,s) \quad \textit{(if } d \geq 2^s\textit{)} \\ F(r,d,s) &\leq F(r,d,0) + s(r+1) \end{aligned}$$

to separate s *quadrics at a time, a sequence* $(s_1, \ldots, s_n)$ *is optimal if it maximizes*

$$\sum_{i=1}^{r} s_i^2$$

subject to the constraints $s_i \in \{0, 1, \ldots, r\}$, $2^{s_i} \leq d$, *and* $\sum_{i=1}^{r} s_i = r$.

Proof. If we separate s_1 quadrics in our first application of the obliteration formulae, we obtain

$$F(r,d,0) \leq F(r-s_1,d,s_1) \leq F(r-s_1,d,0) + s_1(r-s_1+1).$$

In other words, we reduce the number of quadrics by s_1 at the expense of increasing the number of linear terms by $s_1(r - s_1 + 1)$. We can rewrite this latter expression as

$$s_1 + s_1 \cdot \left(\sum_{i>1} s_i \right).$$

Similarly, after the first $k-1$ separations, the number of remaining quadrics is $r - s_1 - \ldots - s_{k-1} = s_k + \ldots + s_r$. Then since

$$\begin{aligned} F(s_k + \ldots + s_r, d, 0) &\leq F(s_{k+1} + \ldots s_r, d, s_k) \\ &\leq F(s_{k+1} + \ldots + s_r, d, 0) + s_k + s_k(s_{k+1} + \ldots + s_r), \end{aligned}$$

the number of new linear terms introduced when we separate s_k quadrics in step k is

$$s_k + s_k \left(\sum_{i>k} s_i \right).$$

Thus, after all quadrics have been separated, the number of linear equations in the system will be

$$\begin{aligned} \sum_{k=1}^{r} s_k + \sum_{k=1}^{r} s_k \left(\sum_{i>k} s_i \right) &= N + \sum_{k<i} s_k s_i \\ &= N + \frac{\left(\sum_{i=1}^{r} s_i\right)^2 - \sum_{i=1}^{r} s_i^2}{2} \\ &= N + \frac{N^2 - \sum_{i=1}^{r} s_i^2}{2}. \end{aligned}$$

Thus, the number of linear equations in the reduced system – and hence the bound we obtain on $F(r, d, 0)$ is minimized when the quantity $\sum_{i=1}^{r} s_i^2$ is maximized. □

Equivalently, an optimal sequence $(s_1, \ldots, s_n)$ is one which maximizes distance from the origin when $(s_1, \ldots, s_n)$ is interpreted as a point of $\mathbb{R}^n$. Then $\sum_{i=1}^{r} s_i = r$ determines a simplex and we can observe that this distance is maximized at the vertices of the simplex; that is, when all but one of the s_i are zero. In general the vertex points will not satisfy $2^{s_i} \leq d$; the optimal sequence(s) will be those which are as close as possible to vertex points without violating this constraint. This leads to a simple rule for optimizing sequences of separations: *at each step, separate as many quadrics as possible*, subject to the constraint $2^{s_i} \leq d$.

7.4 Limitations of Sylvester's Method of Obliteration

We have seen that Sylvester's obliteration formulae can be leveraged to produce bounds on $F(r, d, 0)$, and determined the optimal strategy for applying these formulae. A natural next question is whether these bounds are sharp. In general the answer is no, as the next example shows.

Example 3. *Let $r = 3$ and $d = 5$. What is $F(3, 5, 0)$? That is, what is the minimal ambient dimension N such that the intersection of any three quadrics Q_1, Q_2, Q_3 in $\mathbb{P}^N_K$ is guaranteed to contain at least one point of weight at most 5?*

Applying the obliteration formulae, we obtain

$$\begin{aligned} F(3, 5, 0) &\leq F(1, 5, 2) \\ &\leq F(1, 5, 0) + 2 \cdot (2) \\ &= F(1, 5, 0) + 4 = 5. \end{aligned}$$

This is optimal in the sense of Proposition 14; there is no way to obtain a sharper bound using only the rules $F(r, d, 0) \leq F(r - s, d, s)$ and $F(r, d, s) \leq F(r, d, 0) + s(r + 1)$.

On the other hand, we can obtain a sharper bound by using certain special facts about the geometry of quadrics and their intersections. It is a classical result that the intersection of any 2 quadrics in $\mathbb{P}^4_{\overline{K}}$ contains 16 lines; Segre has shown that these lines are defined over a weight 5 extension of the base field K.[15] Thus, given three quadrics, in $\mathbb{P}^4$, we can determine a line of weight 5 lying inside two of them, then intersect this line with the remaining quadric to determine a weight 5 point. Thus $F(3, 5, 0) \leq 4$.

Recall that in determining a line on the intersection $V = Q_1 \cap \ldots Q_r$ of r quadrics, the basis of Sylvester's method was to find a point P of V, then determine a point X such that $X + \lambda P$ is in V for all λ. For this to succeed, we require not only that V contain a line, but that it contain a line through the (arbitrary) point X we chose. Thus when there are only finitely many lines to be found, the method will not succeed. In particular, Segre's observation that the 16 lines in the intersection of two quadrics in $\mathbb{P}^4$ are of weight 5 cannot be derived from the obliteration formula. Analogous considerations apply to the problem of determining k-planes in intersections of quadrics (or in intersections of higher degree hypersurfaces).

8 Sylvester's Obliteration Algorithm

We now give a description of the obliteration algorithm in general. Though motivated by the problem of finding Tschirnhaus transformations, the procedure Sylvester describes in [18] is remarkably general, allowing for a solution of bounded weight to be found to any system of homogeneous polynomials, provided only that the number of variables is greater than some bound which depends only on the degrees of the polynomials.

It will be convenient to first establish some new notation.

Definition 8.1. A system S of homogeneous polynomials in $K[x_0, \ldots, x_{n-1}]$ is of *type*

$$\begin{bmatrix} n_d, & n_{d-1}, & \ldots & n_2, & n_1 \end{bmatrix}$$

if it contains exactly n_i equations of degree i for each $i = 1, \ldots, d$, and no equations of degree $d+1$ or higher.

Sylvester shows that such a system S of homogneous polynomial equations in n variables of degree at most d, there is some bound N which depends only on the type of S such that if $n > N$, then S has a solution defined over a weight k extension of K.

For determining points of weight 2 on intersections of quadrics, a useful trick was to separate (at least) one of the quadrics from S, then find a line contained in the solution set of the remaining quadrics. The determination of such a line required the solution of a system S' which, while perhaps containing more equations than S, contains one fewer equation of the highest degree. Generalizing this trick to an arbitrary system S yields the following proposition.

Proposition 15 (Sylvester's First-Order Formula of Obliteration)**.** *Given $n_1, \ldots, n_k \in \mathbb{N}$ with $n_k > 0$, let*

$$[[n_k, n_{k-1}, \ldots, n_2, n_1]]$$

denote the minimum n such that, for any system S of type $[n_k, \ldots, n_1]$, the variety $V(S) \subset \mathbb{P}^{n-1}$ contains a point defined over an extension L of K of weight at most k.

Then

$$[[n_k, n_{k-1}, \ldots, n_2, n_1]] \leq [[m_k, m_{k-1}, \ldots, m_2, m_1 + 1]]$$

where

$$m_i = \begin{cases} \left(\sum_{j=i}^{k} n_j\right) - 1 & i \neq k \\ n_k - 1 & i = k. \end{cases}$$

Proof. Let S be a system of equations with the given number of equations of the given degrees. Pick any f of maximal degree k from the system S.

We can find a solution to S by first finding a line L contained in the solution set of the subsystem $S' = S \setminus \{f\}$, then intersecting this line with the vanishing locus of f. To find L, first find a solution $P = (q_0, \ldots, q_N)$ to S'. Then to get the required line it suffices to find a point $X = (x_0, \ldots, x_N)$ such that $X + \lambda P$ is a solution to S' for all λ.

For any equation $g \in S'$, then, view $g(X + \lambda P)$ as a polynomial in λ; if $\deg(g) = d$, the coefficients of $1, \lambda, \ldots, \lambda^{d-1}, \lambda^d$ must vanish identically. In fact the coefficient of λ^d is just $g(P)$, so vanishes since we chose P to be a solution of S'. The vanishing of the remaining coefficients imposes polynomial conditions on the $x_0, \ldots, x_N$ of degrees $1, 2, \ldots, d$.

Ranging over all $g \in S'$, we have that X must be a solution to a system S'' with m_i equations of degree i, where

$$\begin{aligned} m_k &= n_k - 1 \\ m_{k-1} &= n_k + n_{k-1} - 1 \\ m_{k-2} &= n_k + n_{k-1} + n_{k-2} - 1 \\ &\vdots \\ m_1 &= n_k + n_{k-1} + \ldots + n_1 - 1. \end{aligned}$$

Finally, we require that X not be simply a multiple of P (in which case $X + \lambda P$ does not describe a line). This can be done by imposing an arbitrary linear condition which P does not satisfy, so that the number of equations of degree 1 increases by one. □

We call this reduction formula the *first-order formula of obliteration* – it is first-order in the sense that we consider here only separating one equation at a time. For determining solutions of weight at most k this appears to be optimal, but for less restrictive bounds on weight we can consider other obliteration formulae involving the determination of higher-dimensional linear subspaces.

Note that applying this formula n_k times yields a system with no equations of degree k, so all equations of the highest degree can be removed. This can be repeated until only (a large number of) linear equations remain, in which case the minimum number of variables needed is easy to determine.

For example, we can use this obliteration formula to recover Bring's result for removing three terms from a degree n polynomial for $n \geq 5$.[4] Recall that to determine a Tschirnhaus transformation which accomplishes this it suffices to determine a point on the intersection

$$V_1 \cap V_2 \cap V_3 \subset \mathbb{P}^{n-1}$$

of three hypersurfaces with $\deg(V_i) = i$. Thus, in Sylvester's notation, one requires $n \geq [1, 1, 1]$. Using the formula of obliteration, we have

$$\begin{aligned} [1, 1, 1] &\leq [0, 1, 3] \\ &\leq [0, 0, 4]. \end{aligned}$$

Thus to find a point of weight at most 3 on $V_1 \cap V_2 \cap V_3$ it suffices to find a point of weight at most 3 on the intersection of 4 hyperplanes in $\mathbb{P}^{n-1}$. This is always possible provided $n - 1 \geq 4$.

8.1 Higher-Order Obliteration

As Sylvester himself observed, the bounds obtained by the first-order obliteration formula can often be improved.

For example, using the obliteration calculation

$$\begin{aligned} [1, 1, 1, 1] &\leq [0, 1, 2, 4] \\ &\leq [0, 0, 2, 7] \\ &\leq [0, 0, 1, 9] \\ &\leq [0, 0, 0, 10] = 11 \end{aligned}$$

recovering the Hamilton/Jerrard bound $n \leq 11$ for the removal of 4 terms which we discussed in section 5.1. But in fact, as Hamilton himself observed, $n \geq 10$ suffices. [8]

We can prove this as follows: from $[1, 1, 1, 1] \leq [0, 0, 2, 7]$ we see that it suffices to determine a point of weight 4 on the intersection of 7 hyperplanes and 2 quadric hypersurfaces in $\mathbb{P}^{n-1}$. This is possible when $n \geq 10$. In

this case, we can always find a 2-plane contained in the 7 hyperplanes; the intersection of the 2 quadrics with this 2-plane is a pair of conics, whose intersection can be computed via an equation of degree 4.

The sharpening is possible because the obliteration formula of proposition 15 involves the separation of only *one* equation of highest degree at a time from the given system (and subsequently the determination of a one-dimensional linear subspace of the vanishing locus of the remaining subsystem). By instead separating the two quadrics simultaneously (and then finding a two-dimensional linear subspace of the remaining subsystem) the dimension required is reduced by one.

More generally, one can consider separating s equations of highest degree k from a given system, then finding an s-plane contained in the remaining subsystem. Sylvester derived obliteration formulae for this more general technique uses them to sharpen Hamilton's bounds for the removal of r terms from a degree n by means of a Tschirnhaus transformation of weight at most r.

We now turn to stating and proving the more general formulae of obliteration which we will need. The ideas are due to Sylvester, though he does not produce explicit formulae for this version of the method.

Definition 8.2. Let

$$D\left(d, r, \left[n_k, \quad n_{k-1}, \quad \ldots \quad n_2, \quad n_1\right]\right)$$

denote the minimum n such that, given any system S of type

$$\left[n_k, \quad n_{k-1}, \quad \ldots \quad n_2, \quad n_1\right]$$

of homogeneous polynomials in $K[x_1, \ldots, x_n]$, there exists an r-plane (or a point, if $r = 0$) contained in $V(S) \subset \mathbb{P}^{n-1}$ defined over a field L with $\mathrm{wt}(L/K) \leq d$.

Now consider separating s equations of highest degree from a system S. If an s-plane can be found contained in the vanishing locus of the remaining subsystem, then a point of $V(S)$ can be found by intersecting the s separated equations with this s-plane; this intersection is guaranteed to contain a point of weight at most k^s. This yields the following formula.

Proposition 16. *Sylvester Obliteration Suppose $s < n_k$ and $d \geq k^s$. Then*

$$D\left(d, 0, \left[n_k, \quad n_{k-1}, \quad \ldots \quad n_2, \quad n_1\right]\right) \leq D\left(d, s, \left[n_k - s, \quad n_{k-1}, \quad \ldots \quad n_2, \quad n_1\right]\right)$$

The hypothesis $s < n_k$ is inessential; the same logic allows for the separation of s equations of any degree provided the product of the degrees of the separated subsystem is at most d. Thus, if $s > n_k$ but $s < n_k + n_{k-1}$, one can separate all n_k equations of degree k together with $s - n_k$ equations of degree $k-1$. If $n_k + n_{k-1} + n_{k-2} < s < n_k + n_{k-1}$, one can separate all equations of degree k and $k-1$ together with some equations of degree $k-2$, and so on. It is easy to make the necessary adjustments to the formula in these cases.

To apply the obliteration process iteratively, we need an additional formula to reduce the problem of finding an s-plane in the solution set of a given system to finding a point solution to some auxiliary system (with a larger number of equations).

Proposition 17. *Sylvester Obliteration*

$$D\left(d, s, \left[n_k, \quad n_{k-1}, \quad \ldots \quad n_2, \quad n_1\right]\right) \leq D\left(d, 0, \left[m_k, \quad m_{k-1}, \quad \ldots \quad m_2, \quad m_1 + s\right]\right)$$

where

$$m_i = \sum_{j \geq i} n_j \binom{s + j - i - 1}{j - i}.$$

Proof. We proceed by induction on the dimension s of the plane to be found. The base case $s = 1$ has already been dealt with in the proof of the first-order obliteration formula.

Now let Let S a system of polynomial equations in n variables of type $[n_k, n_{k-1}, \ldots, n_2, n_1]$ and suppose that the result has been established for $s - 1$. To simplify notation let $G(s)$ denote the quantity on the right-hand side of the inequality to be proven.

Our strategy to find an s-plane contained in $V(S)$ is as follows: first find find an $(s-1)$-plane of contained in $V(S)$ and defined over an extension L/K with $\mathrm{wt}(L/K) \leq d$. By the inductive hypothesis, this is possible when $n \geq G(s-1)$. Next we show that given such an $(s-1)$-plane we can determine an s-plane in $V(S)$ defined over an extension L'/L with $\mathrm{wt}(L'/L) \leq d$ (and hence $\mathrm{wt}(L'/K) \leq d$) provided that $n \geq G(s)$. Thus to determine an s-plane requires

$$n \geq \max G(s), G(s-1) = G(s).$$

The equality $\max G(s), G(s-1)$ holds because

$$\sum_{j \geq i} n_j \binom{s + j - i}{j - i} > \sum_{j \geq i} n_j \binom{s - 1 + j - i}{j - i}$$

for all i, j and s and this implies $G(s) \geq G(s-1)$.

Suppose then that $V(S)$ contains an $(s-1)$-plane spanned by points $Q_1, \ldots, Q_s \in \mathbb{P}_L^{n-1}$. To determine an s-plane given this data it suffices to find a point $X = (x_1 : \ldots : x_n)$ such that the expression

$$f(X + \lambda_1 Q_1 + \ldots + \lambda_s Q_s) = 0$$

vanishes for any polynomial $f \in S$ and any $\lambda_1, \ldots, \lambda_s \in L$.

Consider now the expansion of $f(X + \lambda_1 Q_1 + \ldots + \lambda_s Q_s)$ as a polynomial in $\lambda_1, \ldots, \lambda_{s-1}$. Suppose $\deg(f) = j$. The degree j component of this polynomial is simply $f(\lambda_1 Q_1 + \ldots + \lambda_s Q_{s-1})$, which vanishes since $\lambda_1 Q_1 + \ldots + \lambda_s Q_s$ is contained in $V(S) \subseteq V(f)$ by assumption. For the expression $(X + \lambda_1 Q_1 + \ldots + \lambda_s Q_s)$ to vanish for all $\lambda_1, \ldots, \lambda_s$, then, we require that for all $i > 0$ and all $(e_1, \ldots, e_s) \in \mathbb{N}^s$ such that $e_1 + \ldots + e_s = j - i$, the coefficient of the monomial

$$\lambda_1^{e_1} \cdots \lambda_s^{e_s}$$

must be zero. This coefficient will be a homogeneous degree i polynomial in $x_1, \ldots, x_n$.

The number of monomials in $\lambda_1, \ldots, \lambda_s$ of total degree $j - i$ is given by

$$\binom{s + j - i - 1}{j - i}$$

so the requirement $f(X + \lambda_1 Q_1 + \ldots + \lambda_s Q_s) = 0$ imposes $\binom{s+j-i}{j-i}$ homogeneous degree i polynomial conditions on $x_1, \ldots, x_n$.

There are n_j polynomials of degree j in S, so collectively these contribute

$$n_j \binom{s + j - i}{j - i}$$

degree i polynomials.

Now summing over all $j \geq i$, the number of degree i polynomials which $(x_1, \ldots, x_n)$ must satisfy is given by

$$\sum_{j \geq i} n_j \binom{s + j - i}{j - i}.$$

Finally, we must ensure X is not itself a point of the $(s-1)$-plane spanned by $Q_1, \ldots, Q_{s-1}$. We do this by choosing a complementary hyperplane $\mathbb{P}^{n-1-s}$, which amounts to imposing an additional s linear conditions on $x_1, \ldots, x_n$.

Thus given an $(s-1)$-plane of weight d contained in $V(S)$, to determine an s-plane of weight d contained in $V(S)$ it suffices to determine a point solution X to a system S' of type

$$[m_k \quad m_{k-1} \quad \dots \quad m_2 \quad m_1 + s]$$

where

$$m_i = \sum_{j \geq i} n_j \binom{s+j-i-1}{j-i}.$$

The ambient dimension required to do this is therefore given by

$$G(s) = D\left(d, 0, \left[m_k \quad m_{k-1} \quad \dots \quad m_2 \quad m_1 + s\right]\right).$$

This completes the proof. □

Applying these obliteration formulae iteratively, one can reduce the type of the given system until only equations of degree 1 remain, in which case the value of the function D can be computed easily.

8.2 Bounds on Resolvent Degree from Sylvester's Method

Sylvester's obliteration formulae are most naturally understood in terms of finding solutions of bounded weight to a given system, but can also be used to prove statements about resolvent degree.

For example, Sylvester uses the obliteration formulae to prove that on the intersection of

$$V_1 \dots \cap \dots V_5 \subset \mathbb{P}^{n-1}_K$$

with $\deg(V_i) = i$, there is always a point defined over an extension L of K with $\mathrm{wt}(L/K) \leq 5$ provided that $n \geq 41$. Thus there is a Tschirnhaus transformation defined over L removing the first 5 intermediate terms from any degree n polynomial in $K[x]$. By lemma 2, we have $\mathrm{RD}(L/K) \leq \mathrm{RD}(5) = 1$. By lemma 3, this implies

$$\mathrm{RD}(n) \leq \max\{n-6, \mathrm{RD}(n-1)\}$$

for $n \geq 41$. Since Hilbert's argument establishes $\mathrm{RD}(n-1) \leq n-1-5 = n-6$ for $n-1 \geq 9$, this implies

$$\mathrm{RD}(n) \leq n-6 \quad \text{for } n \geq 41.$$

Observe, however, that $\mathrm{wt}(L/K) \leq 5$ is much stricter than required for this argument; all that we require is that $\mathrm{RD}(L/K) \leq n-6$, and this will hold provided $\mathrm{wt}(L/K) \leq d$ and $\mathrm{RD}(d) \leq n-6$.

Raising the allowable weight allows for more terms to be separated in each step of Sylvester's obliteration algorithm, and this makes the algorithm potentially more efficient. Thus, for example, $\mathrm{RD}(n) \leq n-6$ for $n \geq 21$ can be proven using Sylvester's obliteration algorithm with an appropriate choice of maximum weight. This resolvent degree bound was first conjectured by Wiman and Chebotarev and rigorously proved independently by Sutherland in 2021.[16, 20, 16] The application of the obliteration algorithm to derive this specific bound is described in [11].

The following proposition gives the relationship between the obliteration formulae and bounds on resolvent degree more precisely.

Proposition 18 (Obtaining Bounds on Resolvent Degree)**.** *Suppose that*

$$D\left(d, 0, \underbrace{\begin{bmatrix}1 & 1 \dots & 1 & 1\end{bmatrix}}_{k-1 \text{ times}}\right) \leq n$$

and $\mathrm{RD}(d) < n-k$*. Then*

$$\mathrm{RD}(n) \leq \max\{n-k, \mathrm{RD}(n-1)\}.$$

Proof. By lemma 3, it suffices to show that for any degree n polynomial

$$p(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n \in K[x]$$

there is a Tschirnhaus transformation

$$T(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}$$

defined over an extension L/K such that that transformed polynomial has the form

$$q(y) = y^n + A_k y^{n-k} + \ldots + A_{n-1}y + A_n$$

and such that $\mathrm{RD}(L/K) \leq n-k$.

Such a transformation is given by an L-point on the intersection of the Tschirnhaus hypersurfaces

$$V(A_1) \cap \ldots \cap V(A_{k-1}) \subset \mathbb{P}^{n-1}_{\overline{K}}.$$

The system $\{A_1, \ldots, A_{k-1}\}$ has type

$$\underbrace{[1, \quad 1, \quad \ldots \quad 1, \quad 1]}_{k-1 \text{ times}},$$

so since

$$D\left(d, 0, \underbrace{[1, \quad 1, \ldots \quad 1, \quad 1]}_{k-1 \text{ times}}\right) \leq n$$

there is an L-point of $V(A_1) \cap \ldots \cap V(A_{k-1})$ with $\mathrm{wt}(L/K) \leq d$.

Now by lemma 2, $\mathrm{RD}(L/K) \leq \mathrm{RD}(d)$, and so $\mathrm{RD}(L/K) \leq n - k$, by hypothesis. □

In Appendix A, Python code is given which uses this proposition to compute, for $r = 6, \ldots, 17$, upper bounds $B(r)$ on the degree n such that $\mathrm{RD}(n) \leq n - r$. Results are shown in the table below. This method improves on the previous best-known bounds $B'(r)$ for $r = 7, 8, 11, 12$, and 13, and matches the best-known bounds for other $r \geq 6$. For $6 \leq r \leq 12$ the previous bounds $B'(r)$ are from [17]. For $13 \leq r \leq 17$ they are from [10].

Table 1: Bounds on Resolvent Degree

r	B(r)	Best Previous Bound B'(r)
6	21	21
7	76	109
8	211	325
9	1,681	1,681
10	15,121	15,121
11	59,050	151,201
12	332,641	1,663,201
13	3,991,681	5,250,199
14	51,891,841	51,891,841
15	726,485,761	726,485,761
16	10,897,286,401	10,897,286,401
17	174,356,582,401	174,356,582,401

A Python Code for Optimizing Resolvent Degree Bounds using Obliteration

```
import math

def multichoose(N, k):
    return math.comb(N+k-1,k)

"""Helper function to determine the maximum allowable separation
    based
on a given degree constraint."""
def bestSeparation(maxDegree, systemType):
    totalDegree = 1
    maxSeparation = {}
    key = max((key for key in systemType))
    while True:
        if systemType[key] == 0:
            del systemType[key]
            key -= 1
        currDegree = key
        if currDegree == 1:
            return(totalDegree, maxSeparation, systemType)
        if totalDegree*currDegree <= maxDegree:
            totalDegree *= currDegree
            systemType[key] -= 1
            if key in maxSeparation.keys():
                maxSeparation[key] += 1
            else:
                maxSeparation[key] = 1
        else:
            return(totalDegree, maxSeparation, systemType)

"""Applies the obliteration algorithm to a system of type
    systemType, only
allowing solutions of weight at most maxDegree. Returns the
dimension bound computed and modifies the list stepDegrees
to record the necessary degree elevation at each step."""
def optimizer(maxDegree, systemType, stepDegrees, RD):
    for key in systemType:
```

```
            if systemType[key] == 0:
                del systemType[key]

        if len(systemType.keys()) == 1:
            return systemType[1]+1

        if sum(systemType[key] for key in systemType) > RD:
            return float('inf')
        (totalDegree, outerSeg, systemType) = bestSeparation(maxDegree,
            systemType)
        stepDegrees += [totalDegree]
        k = sum(outerSeg[key] for key in outerSeg)
        newSystemType = {key: systemType[key] for key in systemType}
        for key in systemType:
            i = 1
            while key-i >= 1:
                #print(key, key-i, multichoose(k,i))
                newSystemType[key-i] += systemType[key]*multichoose(k, i)
                i += 1
        newSystemType[1] += k
        return optimizer(maxDegree, newSystemType, stepDegrees, RD)

    def obliterationOptimizer(systemType):
        m = max(systemType.keys())
        maxDegree = math.prod(key**systemType[key] for key in
            systemType)
        RD = float('inf')
        N = float('inf')
        while True:
            degreesNeeded = []
            #print(maxDegree, systemType)
            N = optimizer(maxDegree, dict(systemType), degreesNeeded,
                RD)
            curr = max(N, maxDegree)     #print(systemType)
            if curr <= RD:
                RD = curr
            else:
                return RD
            maxDegree = min(max(N, max(degreesNeeded)), maxDegree-1)
```

```
"""Given a positive integer r, returns an upper bound on n such
    that RD(n) <= n-r."""
def bound(r):
    sys = {(r-i):1 for i in range(r)}
    return obliterationOptimizer(sys)+1
```

B Recovering Roots after a Tschirnhaus Transformation

One natural question is whether (or under what circumstances) a Tschirnhaus transformation can be inverted. We can consider this question from two distinct points of view. First, the classical perspective, which we adopted in the previous section, in which a concrete degree n polynomial $p(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \in K[x]$ is fixed and a transformed polynomial is obtained by applying a degree $n-1$ polynomial transformation $T(x)$ (called a Tschirnhaus transformation) to the roots of $p(x)$. We can then consider the problem of recovering the roots of the original polynomial p from the roots of the transformed polynomial q. In particular, if q is solvable and T is defined over a solvable extension of K, does it follow that p is solvable? In general the answer is no – as a trivial example, suppose $T(x) = 0$. Then the transformed polynomial is $q(y) = y^n$ regardless of the original polynomial p, so the roots of q obviously convey no information about the roots of p. On the other hand, for most transformations T the roots of p can be computed rationally from the roots of q. More precisely, this can be done for any T outside of a closed subset of "bad" Tschirnhaus transformations which send two or more distinct roots of p to the same value. We will show that the bad transformations form the zero locus of a homogeneous polynomial in the coefficients of $T(x)$. We describe how to compute this polynomial and compute it explicilty in the $n = 3$ case.

Second, a more modern perspective is to work over the transcendental field extension $K(a_1, \ldots, a_n)$, view $p(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ as the generic polynomial, and define a Tschirnhaus transformation to be a $\overline{K(a_1, \ldots, a_n)}$-linear field automorphism of $\overline{K(a_1, \ldots, a_n)}[x]/(p(x))$. This is the definition of Tschirnhaus transformation adopted by Wolfson in [21]

Wolfson shows every such isomorphism can be described by the assignment $x \mapsto T(x)$, where T is a degree $n-1$ polynomial, providing the connection to the classical point-of-view. Conversely, an assignment $x \mapsto T(x)$ defines an $\overline{K(a_1, \ldots, a_n)}$-linear endomorphism which is an automorphism if and only if its determinant (a polynomial in $a_1, \ldots, a_n$ and the coefficients of T) is nonzero. The classical problem of recovering the roots of the original polynomial then corresponds to computing the inverse of such an automorphism, which requires only linear algebra. This provides a method for recovering the original roots which works generically; on the other hand, after specializing

to particular values of $a_1, \ldots, a_n$ in K the determinant may become zero, so this does not work for every choice of polynomial p and Tschirnhaus transformation T. For $n = 3$ we compute the determinant polynomial explicitly and show that it is zero for exactly those choices of $a_1, \ldots, a_n$ and T such that T is a "bad" Tschirnhaus transformation for $p(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$ in the sense of the previous paragraph.

B.1 Recovering Roots from a Classical Perspective

Let $p \in K[x]$ be a degree n polynomial, let $T(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}$ be a Tschirnhaus transformation defined over some extension L of K, and let q be the transformed polynomial obtained by applying T to the roots of p. In this section, we will describe how to compute the roots of p if T and the roots of q are known.

Let y_i be a root of q and suppose x_i is some root of p such that $y_i = T(x_i)$. Then x_i is a root of both $p(x)$ and $T(x) - y_i$, so it is a root of

$$\mathrm{GCD}(p(x), T(x) - y_i).$$

This is a polynomial $L[x]$ which can be computed (rationally over L) using the Euclidean algorithm. The degree of this polynomial is equal to the number of roots of $p(x)$ which satisfy $T(x_i) = y_i$. In particular, if $T(x_1), \ldots, T(x_n)$ are all distinct, then this will be a linear polynomial for each i and so we can recover the roots x_i rationally in terms of the y_i. On the other hand, if $q(y)$ has a root of multiplicity d, we may need to solve an equation of degree up to d to recover the roots of $p(x)$. In the extreme case where $T(x) = b_0$ is a constant transformation, so $q(y) = (y - b_0)^n$, knowing the roots of $q(y)$ conveys no information about the roots of $p(x)$. On the other hand, if $p(x)$ has n distinct roots and $T(x)$ is a nonconstant polynomial, then at most $n - 1$ of $T(x_1), \ldots, T(x_n)$ can be equal (since T has degree at most $n - 1$), then the roots of $p(x)$ can be recovered from the roots of $q(y)$ after solving an auxiliary polynomial of degree at most $n - 1$.

Now suppose the roots $x_1, \ldots, x_n$ of $p(x)$ are all distinct. In light of the discussion in the previous paragraph, we will say a Tschirnhaus transformation $T(x) = b_0 + \ldots + b_{n-1}x^{n-1}$ is "bad" if $T(x_i) = T(x_j)$ for $i \neq j$, so that T maps two distinct roots of $p(x)$ to the same root of $q(y)$, so that irrationalities potentially arise in recovering the original roots from the transformed roots. (Though note that even for bad transformations, recovering the roots of p

from those of q may be easier than determining roots of p directly.) Then T is bad if and only if

$$\begin{aligned}
0 &= \prod_{i<j}(T(x_i) - T(x_j)) \\
&= \prod_{i<j}\left[\left(b_0 + b_1x_i + \ldots + b_{n-1}x_i^{n-1}\right) - \left(b_0 + b_1x_j + \ldots + b_{n-1}x_j^{n-1}\right)\right] \\
&= \prod_{i<j}\left(\sum_{k=1}^{n-1} b_k(x_i^k - x_j^k)\right) \\
&= \prod_{i<j}\left((x_i - x_j)\sum_{k=1}^{n-1} b_k(x_i^{k-1} + x_j^{k-1}\right) \\
&= \left(\prod_{i<j}(x_i - x_j)\right)\prod_{i<j}\left(\sum_{k=1}^{n-1} b_k(x_i^{k-1} + x_j^{k-1})\right)
\end{aligned}$$

By assumption, $x_i \neq x_j$ for $i \neq j$, so $\prod_{i<j}(x_i - x_j) \neq 0$. Thus we must have

$$\prod_{i<j}\left(\sum_{k=1}^{n-1} b_k(x_i^{k-1} + x_j^{k-1})\right) = 0.$$

Each term in the product is homogeneous linear in $b_1, \ldots, b_{n-1}$, and there are $\binom{n}{2}$ terms, so the set of bad Tschirnhaus transformations is the zero locus of a homogeneous degree $\binom{n}{2}$ polynomial condition in the b_i's (with no dependence on b_0). Furthermore, this expression is symmetric in $x_1, \ldots, x_n$, so the coefficients of this polynomial can themselves be written as polynomial functions in $a_1, \ldots, a_n$, since these generate the algebra of symmetric functions in the x_i's.

Example 4. *$n = 3$ Let $n = 3$ and let $p(x) = x^3 + a_1x^2 + a_2x + a_3$ be a cubic polynomial with three distinct roots x_1, x_2, x_3. Then a Tschirnhaus transformation $T(x) = b_0 + b_1x + b_2x^2$ is bad (in the sense that $T(x_i) = T(x_j)$ for some $i \neq j$) if and only if*

$$(b_1 + b_2(x_1 + x_2))(b_1 + b_2(x_1 + x_3))(b_1 + b_2(x_2 + x_3)) = 0.$$

Expanding the left-hand side, we have

$$\begin{aligned}
&b_1^3+\\
&b_1^2b_2(2(x_1+x_2+x_3))+\\
&b_1b_2^2((x_1+x_2)(x_1+x_3)+(x_1+x_2)(x_2+x_3)+(x_1+x_3)(x_2+x_3))+\\
&b_2^3(x_1+x_2)(x_1+x_3)(x_2+x_3)=0.
\end{aligned}$$

Given that $a_1=-(x_1+x_2+x_3)$, $a_2=x_1x_2+x_1x_3+x_2x_3$, $a_3=-x_1x_2x_3$, *one can verify by direct computation that*

$$\begin{aligned}
2(x_1+x_2+x_3)&=-2a_1\\
(x_1+x_2)(x_1+x_3)+(x_1+x_2)(x_2+x_3)+(x_1+x_3)(x_2+x_3)&=a_1^2+a_2\\
(x_1+x_2)(x_1+x_3)(x_2+x_3)&=a_3-a_1a_2.
\end{aligned}$$

Thus the set of bad Tschirnhaus transformations is the zero locus of

$$b_1^3-2a_1b_1^2b_2+(a_1^2+a_2)b_1b_2^2+(a_3-a_1a_2)b_2^3.$$

Note that this contains the constant Tschirnhaus transformations, since these have $b_1=b_2=0$. *As another example, the Tschirnhaus transformation* $T(x)=x^2$ *is bad if and only if* $a_3-a_1a_2=0$, *in which case we have*

$$p(x)=x^3+a_1x^2+a_2x+a_1a_2=(x^2+a_2)(x+a_1)$$

and we can see explicitly that $p(x)$ *has two roots (namely* $i\sqrt{a_2}$ *and* $-i\sqrt{a_2}$*) that map to the same root via* T.

B.2 Recovering Roots from a Modern Perspective

Fix an algebraically closed field K and let $K_n=K(a_1,\ldots,a_n)$, with $a_1,\ldots,a_n$ indeterminates. Let $p(x)=x^n+a_1x^{n-1}+\ldots+a_n$. Following Wolfson in [21], we can define a *Tschirnhaus transformation* to be a $\overline{K_n}$-linear automorphism of $\overline{K_n}[x]/(p(x))$. Since $1,x,\ldots,x^{n-1}$ form a basis for this field as a $\overline{K_n}$-vector space, any such automorphism must send

$$x\mapsto b_0+b_1x+\ldots+b_{n-1}x^{n-1}$$

for some $b_0,\ldots,b_{n-1}\in\overline{K_n}$, and is completely determined by this choice. Conversely, given any degree $n-1$ polynomial $T(x)=b_0+b_1x+\ldots+b_{n-1}x^{n-1}$,

the assignment $x \mapsto T(x)$ yields an $\overline{K_n}$-linear endomorphism, and this is an automorphism when its determinant is nonzero. For $b_0, \ldots, b_{n-1} \in K_n$, Wolfson shows that $T(x)$ is a Tschirnhaus transformation in this sense if and only if T is not the constant polynomial. On the other hand, the determinant is a polynomial in the b_i's, so there are choices of T with coefficients in a finite field extension of K_n that do not define a Tschirnhaus transformation.

Given such a Tschirnhaus transformation $\Phi : x \mapsto T(x)$ we can compute its inverse explicitly. For $k = 0, \ldots, n-1$ we have

$$\Phi(x^k) = T(x)^k = (b_0 + b_1 x + \ldots + b_{n-1}x^{n-1})^k.$$

Reducing the right-hand side modulo the degreee n polynomial $p(x)$ we can express each $\Phi(x^k)$ as a (degree at most $n-1$) polynomial in x, and so obtain the matrix for Φ relative to the basis $\{1, x, x^2, \ldots, x^{n-1}\}$. Inverting this matrix then yields the inverse Tschirnhaus transformation, a degree $n-1$ polynomial $S(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$ with the property that $S(T(x))$ is congruent to x modulo $p(x)$.

We can connect to the classical point-of-view by specializing to particular values of $a_1, \ldots, a_n \in K$. (More precisely, choose a map $K(a_1, \ldots, a_n) \to K$.) Then $p(x)$ is a polynomial with coefficients in K, and the assignment $x \mapsto T(x)$ on $\overline{K_n}[x]/(p(x))$ sends any root x_i of p to $T(x_i)$, so defines a Tschirnhaus transformation in the classical sense. Moreover, since $S(T(x))$ is congruent to x modulo $p(x)$, for any root x_i of p we must have $S(T(x_i)) = x_i$, so computing the inverse Tschirnhaus transformation S as above provides a method for recovering the roots of the original polynomial from the transformed roots. This method does not work in all possible cases, however, for two reasons. First, not every classical Tschirnhaus transformation defines a $\overline{K_n}[x]/(p(x))$-automorphism, and second, the coefficients $c_0, \ldots, c_{n-1}$ of the inverse transformation S will in general be rational functions of $a_1, \ldots, a_n$, and so S may not be well-defined after specializing. Both of these correspond to the determinant of Φ being zero for particular choices of $a_1, \ldots, a_n$ and T, which in turn corresponds to T being a bad transformation of $p(x)$ in the sense that $T(x_i) = T(x_j)$ for some distinct roots x_i and x_j of p. In the next subsection we show this for the $n = 3$ case by computing the determinant of a general Tschirnhaus transformation Φ.

Example 5. $n = 3$ *Let* $p(x) = x^3 + a_1x^2 + a_2x + a_3$*, with* $a_1, \ldots, a_3$ *indeterminants. For any* $(b_0, b_1, b_2) \in \overline{K(a_1, a_2, a_3)}^3$*, the assignment* $x \mapsto b_0 + b_1x + b_2x^2$

defines a $\overline{K(a_1, a_2, a_3)}$*-linear endomorphism*

$$\Phi : \overline{K(a_1, a_2, a_3)}[x]/(p(x)) \to \overline{K(a_1, a_2, a_3)}[x]/(p(x)),$$

which is an automorphism when $\det \Phi \neq 0$*. To compute the determinant and inverse of* Φ *we first compute its matrix relative to the* $\overline{K(a_1, a_2, a_3)}$*-basis* $\{1, x, x^2\}$*. We have*

$$\begin{aligned} 1 &\mapsto 1 \\ x &\mapsto b_0 + b_1 x + b_2 x^2 \\ x^2 &\mapsto (b_0 + b_1 x + b_2 x^2)^2. \end{aligned}$$

After reducing modulo $p(x) = x^3 + a_1 x^2 + a_2 x + a_3$*, we have*

$$\begin{aligned} (b_0 + b_1 x + b_2 x^2)^2 \equiv\ & (b_0^2 - 2b_1 b_2 a_3 + b_2^2 a_1 a_3) + \\ & (2b_0 b_1 - 2b_1 b_2 a_2 + b_2^2(a_1 a_2 - a_3))x + \\ & (b_1^2 + 2b_0 b_2 - 2b_1 b_2 a_1 + b_2^2(a_1^2 - a_2))x^2 \end{aligned}$$

so the matrix of Φ *is*

$$\begin{bmatrix} 1 & 0 & 0 \\ b_0 & b_1 & b_2 \\ b_0^2 - 2b_1 b_2 a_3 + b_2^2 a_1 a_3 & 2b_0 b_1 - 2b_1 b_2 a_2 + b_2^2(a_1 a_2 - a_3) & b_1^2 + 2b_0 b_2 - 2b_1 b_2 a_1 + b_2^2(a_1^2 - a_2) \end{bmatrix}$$

and so

$$\det \Phi = b_1^3 - 2a_1 b_1^2 b_2 + (a_1^2 + a_2) b_1 b_2^2 + (a_3 - a_1 a_2) b_2^3.$$

Note that this is exactly the polynomial derived in section 2.2 describing the locus of "bad" Tschirnhaus transformations.

For example, for $b_0 = 0, b_1 = 0, b_2 = 1$ *we have*

$$\det \Phi = a_3 - a_1 a_2 \neq 0$$

so the assignment $x \mapsto x^2$ *defines a Tschirnhaus transformation. Inverting this matrix for this transformation, we find that* Φ^{-1} *satisfies*

$$\begin{aligned} 1 &\mapsto 1 \\ x &\mapsto -\frac{a_1 a_3}{a_1 a_2 - a_3} + \frac{a_2 - a_1^2}{a_1 a_2 - a_3} x + \frac{1}{a_1 a_2 - a_3} x^2 \\ x^2 &\mapsto x \end{aligned}$$

so $S(x) = -\frac{a_1 a_3}{a_1 a_2 - a_3} + \frac{a_2 - a_1^2}{a_1 a_2 - a_3} x + \frac{1}{a_1 a_2 - a_3} x^2$ *gives an inverse to* $T(x) = x^2$, *in the sense that* $S(T(x)) = x$ *modulo* $p(x)$. *Moreover, if we specialize to a polynomial* $p(x) \in K[x]$ *by choosing values of* a_1, a_2, a_3 *in* K, *then transform* $p(x)$ *to* $q(y)$ *via the assignment* $y = x^2$, *we can recover the roots of* p *from the roots of* q *simply by applying the polynomial* S *to the roots of* q, *provided that* $a_1 a_2 - a_3 \neq 0$.

C Determining a Tschirnhaus Transformation for the Solution of the Cubic

Let $p(x) = x^3 + a_2x + a_3$.

Fix an algebraic closure $\overline{K}$ and suppose p factors as

$$p(x) = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$$

over $\overline{K}$.

We will show there is a Tschirnhaus transformation $T(x) = b_0 + b_1x + b_2x^2$ with coefficients in a solvable extension (in fact, a single quadratic extension suffices) of K such that the transformed polynomial

$$q(y) = (y - T(\lambda_1))(y - T(\lambda_2))(y - T(\lambda_3)) = y^3 + A_1y^2 + A_2y + A_3$$

satisfies $A_1 = A_2 = 0$, and hence is in solvable form. Note that though we assume $a_1 = 0$ in the original polynomial p, this does not guarantee $A_1 = 0$ in the transformed polynomial, so it is necessary to still include this condition.

In terms of b_0, b_1, b_2, to satisfy $A_1 = 0$ we require

$$\begin{aligned} 0 = A_1 & \\ &= -T(\lambda_1) - T(\lambda_2) - T(\lambda_3) \\ &= -3b_0 - b_1(\lambda_1 + \lambda_2 + \lambda_3) - b_2(\lambda_1^2 + \lambda_2^2 + \lambda_3^2) \\ &= -3b_0 + a_1b_1 - b_2(a_1^2 - 2a_2) \\ &= -3b_0 + 2a_2b_2 \end{aligned}$$

For $A_2 = 0$, observe that

$$\begin{aligned} A_2 &= \prod_{i \neq j} T(\lambda_i)T(\lambda_j) \\ &= \frac{1}{2}\left((\sum_{i=1}^{3} T(\lambda_i))^2 - \sum_{i=1}^{3} T(\lambda_i)^2 \right) \\ &= \frac{1}{2}\left(A_1^2 - \sum_{i=1}^{3} T(\lambda_i)^2 \right). \end{aligned}$$

Then if $A_1 = 0$, to further satisfy $A_2 = 0$ it suffices to choose T so that

$$\begin{aligned}
0 &= \sum_{i=1}^{3} T(\lambda_i)^2 \\
&= \sum_{i=1}^{3} (b_0 + b_1\lambda_i + b_2\lambda_i^2)^2 \\
&= \sum_{i=1}^{3} (b_0^2 + b_1^2\lambda_i^2 + b_2^2\lambda_i^4 + 2b_0b_1\lambda_i + 2b_0b_2\lambda_i^2 + 2b_1b_2\lambda_i^3) \\
&= 3b_0^2 + 2b_0b_1\left(\sum_{i=1}^{3}\lambda_i\right) + (b_1^2 + 2b_0b_2)\left(\sum_{i=1}^{3}\lambda_i^2\right) + 2b_1b_2\left(\sum_{i=1}^{3}\lambda_i^3\right) + b_2^2\left(\sum_{i=1}^{3}\lambda_i^4\right).
\end{aligned}$$

Now, using Newton's Identities, we can compute

$$\begin{aligned}
\sum_{i=1}^{3}\lambda_i &= -a_1 = 0, \\
\sum_{i=1}^{3}\lambda_i^2 &= a_1^2 - 2a_2 = -2a_2, \\
\sum_{i=1}^{3}\lambda_i^3 &= -a_1^3 + 3a_1a_2 - 3a_3 = -3a_3, \\
\sum_{i=1}^{3}\lambda_i^4 &= a_1^4 - 4a_1^2a_2 + 4a_1a_3 + 2a_2^2 = 2a_2^2
\end{aligned}$$

Thus to determine T it suffices to find a solution to the system of equations

$$\begin{aligned}
-3b_0 + 2a_2b_2 &= 0 \\
3b_0^2 + 2a_2^2b_2^2 - 2a_2(b_1^2 + 2b_0b_2) - 6a_3b_1b_2 &= 0.
\end{aligned}$$

References

[1] Richard Brauer. A note on systems of homogeneous algebraic equations. *Bulletin of the American Mathematical Society*, 51(10):749–755, 1945.

[2] Richard Brauer. On the resolvent problem. *Annali di Matematica Pura ed Applicata*, 102(1):45–55, 1975.

[3] Joe Buhler and Zinovy Reichstein. On tschirnhaus transformations. In *Topics in Number theory*, pages 127–142. Springer, 1999.

[4] Alexander Chen, Yang-Hui He, and John McKay. Erland Samuel Bring's "transformation of algebraic equations". *arXiv preprint arXiv:1711.09253*, 2017.

[5] Jacques Dixmier. Histoire du 13e probleme de hilbert. *Cahiers du séminaire d'histoire des mathématiques*, 3:85–94, 1993.

[6] Benson Farb and Jesse Wolfson. Resolvent degree, hilbert's 13th problem and geometry. *L'Enseignement Mathématique*, 65(3):303–376, 2020.

[7] Raymond Garver. On the removal of four terms from an equation by means of a tschirnhaus transformation. *Bulletin of the American Mathematical Society*, 35(1):73–78, 1929.

[8] Sir William Rowan Hamilton. *Inquiry Into the Validity of a Method Recently Proposed by George B. Jerrard, Esq. for Transforming and Resolving Equations of Elevated Degrees Undertaken at the Request of the Association*. Richard and John E. Taylor, 1836.

[9] Joe Harris. Galois groups of enumerative problems. *Duke Mathematical Journal*, 46(4):685–724, 1979.

[10] Curtis Heberle and Alexander J. Sutherland. Upper bounds on resolvent degree via sylvester's obliteration algorithm. 2021.

[11] Curtis R. Heberle. Removal of 5 terms from a degree 21 polynomial, 2021.

[12] David Hilbert. Über die gleichung neunten grades. *Mathematische Annalen*, 97(1):243–250, 1927.

[13] George Birch Jerrard. *Mathematical Researches*. Longman, Bristol and London, 1834.

[14] Joseph Lagrange. Réflexions sur la résolution algébrique des équations. *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin*, 1771.

[15] Beniamino Segre. The algebraic equations of degrees 5, 9, 157,..., and the arithmetic upon an algebraic variety. *Annals of Mathematics*, pages 287–301, 1945.

[16] Alexander J. Sutherland. GN Chebotarev's "on the problem of resolvents". *arXiv preprint arXiv:2107.01006*, 2021.

[17] Alexander J Sutherland. Upper bounds on resolvent degree and its growth rate. *arXiv preprint arXiv:2107.08139*, 2021.

[18] James Joseph Sylvester. On the so-called tschirnhausen transformation. 1887.

[19] Ehrenfried Walther von Tschirnhaus. Methodus auferendi omnes terminos intermedios ex data aeqvatione (method of eliminating all intermediate terms from a given equation). *Acta Eruditorum (1683)*, pages 204–207.

[20] Anders Wiman. *Über die Anwendung der Tschirnhausentransformation auf die Reduktion algebraischer Gleichungen.* Almquist & Wiksells Boktr., 1927.

[21] Jesse Wolfson. Tschirnhaus transformations after hilbert. *L'Enseignement Mathématique*, 66(3):489–540, 2021.

[22] Trevor D Wooley. Solvable points on smooth projective varieties. *Monatshefte für Mathematik*, 180(2):391–403, 2016.