Geometric Ideas for Cryptographic Equation Solving in Even Characteristic

Sean Murphy and Maura B. Paterson*

Information Security Group, Dept. of Mathematics,
Royal Holloway, University of London,
Egham, Surrey TW20 0EX, U.K.

Abstract. The GeometricXL algorithm is a geometrically invariant version of the XL algorithm that uses polynomials of a much smaller degree than either a standard Groebner basis algorithm or an XL algorithm for certain multivariate equation systems. However, the GeometricXL algorithm as originally described is not well-suited to fields of even characteristic. This paper discusses adaptations of the GeometricXL algorithm to even characteristic, in which the solution to a multivariate system is found by finding a matrix of low rank in the linear span of a collection of matrices. These adaptations of the GeometricXL algorithm, termed the EGHAM process, also use polynomials of a much smaller degree than a Groebner basis or an XL algorithm for certain equation systems. Furthermore, the paper gives a criterion which generally makes a Groebner basis or standard XL algorithm more efficient in many cryptographic situations.

Keywords: XL Algorithm, GeometricXL Algorithm, EGHAM process.

1 Introduction

The solution of a system of multivariate equations over a field is a problem that has recently attracted much attention in cryptology. The classical method for analysing such an equation system is to calculate its Gröbner basis by using Buchberger's algorithm or a related method [2,6,7]. Furthermore, other techniques have been proposed for solving a multivariate equation system in a cryptographic context, such as the `XL` algorithm [5]. However, a Gröbner basis algorithm with the lexicographic ordering and an `XL` algorithm are closely related [1].

The geometric properties of the `XL` algorithm are discussed in [12]. In particular, the `XL` algorithm is not a geometrically invariant algorithm, that is a simple change of co-ordinate system can vastly increase or decrease the running time of the `XL` algorithm. The `GeometricXL` algorithm, proposed in [12], is a geometrically invariant algorithm which can solve certain multivariate equation systems using polynomials of a much smaller degree than a Gröbner basis algorithm or

* M.B. Paterson was supported by EPSRC grants GR/S42637 and EP/D053285.

M.G. Parker (Ed.): IMACC 2009, LNCS 5921, pp. 202–221, 2009.

an XL algorithm. However, the GeometricXL algorithm as described in [12] cannot easily be used in a field of even characteristic, which is of course a situation of great cryptographic importance. The main contribution of this paper is to give an adaptation of the GeometricXL algorithm that is specifically tailored for use in a field of even characteristic. This adaptation of the GeometricXL algorithm, like the original GeometricXL algorithm, is one that attempts to find a linear combination of a collection of matrices that has low rank, a problem sometimes termed MinRank. We note that some related issues concerning the MinRank problem in cryptology are considered in [8]. We term the adaptation of the GeometricXL algorithm given in this paper the EGHAM process, and we note that the EGHAM process can solve certain multivariate equation systems in even characteristic using polynomials of a much smaller degree than a Gröbner basis algorithm or an XL algorithm. Furthermore, a criterion (the $\mathcal{LS}$-criterion) used by the EGHAM process generally greatly reduces the number of equations under consideration. This reduction criterion can also be applied directly to a standard Gröbner basis or XL algorithm in many cryptographic situations, so directly making these algorithms far more efficient.

2 The XL Algorithm

We consider the polynomial ring $\mathbb{F}[x_0, \ldots, x_n]$ of polynomials in $n+1$ variables over a field $\mathbb{F}$. An XL algorithm transforms a homogeneous (without loss of generality) equation system into a homogeneous equation system $f_1 = \ldots = f_m = 0$ of degree D by multiplying the original polynomials by selected monomials [5]. We generally suppose that this equation system has a unique (projective) solution, a common situation in cryptology, though most of our comments are more generally applicable. The aim of an XL algorithm is to solve this new system by linearisation [5], that is by regarding each monomial of degree D as an independent variable and then applying basic linear algebra. The GeometricXL algorithm [12] exploits the geometrical properties of the new equation system to give a solution method that is most applicable when the field characteristic is either zero or exceeds D. We discuss the GeometricXL algorithm in this case in this section and give an alternative description of the GeometricXL algorithm.

2.1 The GeometricXL Algorithm

The critical step of the XL algorithm [12] is an attempt to solve a system of homogeneous equations $f_1 = \ldots = f_m = 0$ of degree D in a field of characteristic p by finding a bivariate polynomial in $\langle f_1, \ldots, f_m \rangle$. However, the set of bivariate polynomials is not invariant under collineation (change of co-ordinates), so the XL algorithm is not geometrically invariant. The GeometricXL algorithm is a geometric invariant generalisation of the XL algorithm. The GeometricXL algorithm focusses on *rank-2 product polynomials* (Definition 1), an invariant generalisation of the bivariate polynomial, and the GeometricXL algorithm is motivated by Lemma 1, the geometric invariance result of [12].

Definition 1. A *rank-2 product polynomial* is a homogeneous polynomial of degree D in the polynomial ring $\mathbb{F}[x_0, \ldots, x_n]$ of the form

$$\prod_{i=1}^{D} (\theta_i L - \theta'_i L') \,,$$

where L and L' are homogeneous linear polynomials and θ_i, θ'_i are constants in some extension field $\overline{\mathbb{F}}$ of $\mathbb{F}$. We let $\mathcal{R}^D_{\mathbb{F},n}$ denote the set of all such rank-2 product polynomials of degree D in $\mathbb{F}[x_0, \ldots, x_n]$.

Lemma 1. The set $\mathcal{R}^D_{\mathbb{F},n}$ of all rank-2 product polynomials of degree D in the polynomial ring $\mathbb{F}[x_0, \ldots, x_n]$ is invariant under collineation.

The `GeometricXL` algorithm requires us to find a linear combination g of $f_1, \ldots, f_m$ such that $g = \sum_{l=1}^{m} \lambda_l f_l$ is a rank-2 product polynomial, that is $g \in \mathcal{R}^D_{\mathbb{F},n}$. If such a rank-2 product polynomial can be found, then we know that any solution to the original system $f_1 = \ldots = f_m = 0$ satisfies $\theta_i L - \theta'_i L' = 0$ for some value of i. This gives us linear expressions in $x_0, x_1, \ldots, x_n$, which provides information about the solution and potentially allows us to eliminate one variable from the equation system, giving us a smaller equation system and so on.

For any homogeneous polynomial h of degree d and any monomial $\mathbf{x} = x_0^{e_0} \ldots x_n^{e_n}$ of degree $k \leq d$ (so $e_0 + \ldots + e_n = k$), we denote the k^{th} order partial derivative of h with respect to $\mathbf{x}$ by $\mathbf{D}^k_{\mathbf{x}} h$, so $\mathbf{D}^k_{\mathbf{x}} h = \frac{\partial^k h}{\partial \mathbf{x}}$. We can now represent all the possible k^{th} order partial derivatives of h as a matrix in which each row is the polynomial $\mathbf{D}^k_{\mathbf{x}} h$ of degree $d - k$ represented as a vector of its coefficients. There are $\binom{n+k}{k}$ monomials of degree k in $n+1$ variables, so we can define an $\binom{n+k}{k} \times \binom{n+d-k}{d-k}$ *partial derivatives* matrix

$$C_h^{(k)} = \left(\mathbf{D}^k_{\mathbf{x}} h\right).$$

The `GeometricXL` algorithm works as a rank-2 product polynomial can be identified using Lemma 2 (given by results of [12]) from its partial derivatives of order $D - 1$ in fields of certain characteristics.

Lemma 2. Suppose g is a homogeneous polynomial of degree D in $\mathbb{F}[x_0, \ldots, x_n]$, where the field $\mathbb{F}$ has characteristic zero or characteristic exceeding D. The polynomial g is a rank-2 product polynomial if and only if the partial derivatives matrix $C_g^{(D-1)}$ satisfies

$$C_g^{(D-1)} = \left(\mathbf{D}^{D-1}_{\mathbf{x}} g\right) = (a_{\mathbf{x}} L + a'_{\mathbf{x}} L')$$

for some homogeneous linear polynomials L and L' and constants $a_{\mathbf{x}}$ and $a'_{\mathbf{x}}$. An equivalent condition is that for a field $\mathbb{F}$ with charateristic zero or characteristic exceeding D, then $g \in \mathcal{R}^D_{\mathbb{F},n}$ if and only if $C_g^{(D-1)}$ has rank at most 2. Moreover, if $g \in \mathcal{R}^D_{\mathbb{F},n}$ then $C_g^{(D-1)}$ has rank at most 2 in a field $\mathbb{F}$ of any characteristic.

The GeometricXL algorithm attempts to find some linear combination of $f_1, \ldots, f_m$ such that $g = \sum_{l=1}^{m} \lambda_l f_l \in \mathcal{R}^D_{\mathbb{F},n}$. The same linear combination of partial derivatives matrices of $f_1, \ldots, f_m$ satisfies

$$C_g^{(D-1)} = \left(\mathbf{D}_{\mathbf{x}}^{D-1} g\right) = \sum_{l=1}^{m} \lambda_l \left(\mathbf{D}_{\mathbf{x}}^{D-1} f_l\right) = \sum_{l=1}^{m} \lambda_l C_{f_l}^{(D-1)}.$$

This matrix $C_g^{(D-1)}$ has rank 2 by Lemma 2, so all of the 3-minors (3×3 subdeterminants) of $C_g^{(D-1)} = \sum_{l=1}^{m} \lambda_l C_{f_l}^{(D-1)}$ vanish. This gives a system of cubic equations in $\lambda_1, \ldots, \lambda_m$. For some equation systems and choices of m and n, this cubic system is easily soluble, for example by linearisation. This process is in essence the GeometricXL algorithm, and it uses polynomials of a much smaller degree for certain equation systems than either a Gröbner basis or XL algorithm [12].

It is a consequence of Lemma 2 that the performance of the GeometricXL algorithm as originally described in [12] depends greatly on the field characteristic. When the characteristic p of the field $\mathbb{F}$ satisfies $p = 0$ or $p > D$, then identifying a partial derivatives matrix of rank at most 2 gives a rank-2 product polynomial (Lemma 2) and so gives information about the solution to the original system. However, when the characteristic p satisfies $0 < p \leq D$, then a partial derivatives matrix of rank at most 2 may or may not give a rank-2 product polynomial. In particular, the GeometricXL algorithm of [12] is not well-suited for fields of even characteristic.

2.2 An Alternative Description of the GeometricXL Algorithm

The GeometricXL algorithm as described in [12] requires the use of $(D-1)^{th}$-order partial derivatives matrices in order to solve a homogeneous multivariate polynomial system of degree D. However, we now give an equivalent description of the GeometricXL algorithm in terms of first order partial derivatives matrices when the field characteristic is either zero or it exceeds the degree D.

Definition 2. Let h be a homogeneous polynomial of degree D in the polynomial ring $\mathbb{F}[x_0, \ldots, x_n]$, where the field has characteristic p and either $p > D$ or $p = 0$. Furthermore let $\mathbf{x} = x_0^{e_0} \ldots x_n^{e_n}$ denote a monomial of degree k ($0 \leq k \leq D$), so $e_0 + \ldots + e_n = k$. The k^{th}-order *catalecticant matrix* [11] of h is

$$\widetilde{C}_h^{(k)} = \left(\frac{1}{e_0! \ldots e_n!} \cdot \frac{\partial^k h}{\partial x_0^{e_0} \ldots \partial x_n^{e_n}}\right) = \left(\frac{1}{e_0! \ldots e_n!} \mathbf{D}_{\mathbf{x}} h\right).$$

Lemma 3. The catalecticant matrix $\widetilde{C}_h^{(k)}$ satisfies $\left(\widetilde{C}_g^{(k)}\right)^T = \widetilde{C}_g^{(d-k)}$ [11], and the catalecticant and partial derivatives matrices of order k, $\widetilde{C}_h^{(k)}$ and $C_h^{(k)}$, share the same row space and have the same rank, with in particular $\widetilde{C}_h^{(1)} = C_h^{(1)}$.

The GeometricXL algorithm tries to find a rank-2 product polynomial g. Lemma 3 shows that the column space of first order partial derivatives

matrix $C_g^{(1)}$ is identical to the row space of the $(D-1)^{th}$ order partial derivatives matrix $C_g^{(D-1)}$, so giving Lemma 4.

Lemma 4. If the characteristic of $\mathbb{F}$ is either zero or exceeds D, then a multivariate polynomial g over $\mathbb{F}$ of degree D is a rank-2 product polynomial, that is $g \in \mathcal{R}^D_{\mathbb{F},n}$, if and only if its first partial derivatives matrix $C_g^{(1)}$ has rank 2.

Lemma 4 means that the `GeometricXL` algorithm could be carried out by using the cubic system derived from the first order partial derivatives matrix rather than the $(D-1)^{th}$ order partial derivatives matrix. Furthermore, a basis for the column space of $C_g^{(1)}$ gives a pair of homogeneous linear polynomials L and L' of use in the product form of g. We give an example of an application of this alternative `GeometricXL` algorithm in Appendix A.

3 A Rank-2 Product Polynomial in Even Characteristic

We now suppose in this and subsequent sections that the field $\mathbb{F}$ is of even characteristic, and we wish to find solutions to $f_1 = \ldots = f_m = 0$, where $f_1, \ldots, f_m$ are homogeneous polynomials of degree D in $\mathbb{F}[x_1, \ldots, x_m]$. For a `GeometricXL` algorithm in even characteristic, we wish to find a linear combination of $f_1, \ldots, f_m$ that is a rank-2 product polynomial, that is we wish to find g such that

$$g = \sum_{l=1}^{m} \lambda_l f_l = \prod_{i=1}^{D} (\theta_i L + \theta'_i L') = \sum_{i=0}^{D} \alpha_i^2 \, L^i \, (L')^{D-i},$$

for some $\alpha_i \in \mathbb{F}$ (as $\mathbb{F}$ has even characteristic), $\theta_i, \theta'_i \in \overline{\mathbb{F}}$ (some extension field of $\mathbb{F}$) and homogeneous linear polynomials $L, L' \in \mathbb{F}[x_0, \ldots, x_n]$. These homogeneous linear polynomials L and L' can be written as

$$L = \sum_{j=0}^{n} a_j x_j \;\text{ and }\; L' = \sum_{j=0}^{n} a'_j x_j.$$

The alternative description of the `GeometricXL` algorithm given in Section 2.2 finds a rank-2 product polynomial by finding a first order partial derivatives matrix of rank 2 in the case that the field characteristic p satisfies $p = 0$ or $p > D$. However, this property still holds in even characteristic, though the converse is not true, as the irreducible polynomial $x_0^2 + x_1 x_2$ over GF(2) with a partial derivatives matrix of rank 2 demonstrates.

We now discuss the properties of the partial derivatives matrix of a rank-2 product polynomial in even characteristic. We let W_D denote the vector space of homogeneous polynomials over $\mathbb{F}$ of degree D in $n+1$ variables, so W_D has dimension $\binom{n+D}{D}$ [9]. In the terminology of [12], W_D is $\mathbb{S}^D(V^*)$, the D^{th} symmetric power of the dual space V^* of the standard vector space V of dimension $n+1$ over $\mathbb{F}$. We now define certain subspaces of W_D that we consider in the development of a `GeometricXL` algorithm for even characteristic.

Definition 3. The $\mathcal{L}^2\mathcal{S}$-*subspace* of W_D for even degree $D = 2s + 2$ is the subspace $U_s = \langle x_i x_j \mathbf{x}^2 | \mathbf{x} \in W_s \rangle < W_{2s+2}$.

Definition 4. The $\mathcal{L}^1\mathcal{S}$-*subspace* of W_D for odd degree $D = 2s + 1$ is the subspace $U'_s = \langle x_i \mathbf{x}^2 | \mathbf{x} \in W_s \rangle < W_{2s+1}$.

Definition 5. The $\mathcal{L}^0\mathcal{S}$-*subspace* of W_D for even degree $D = 2s$ is the subspace $U''_s = \langle \mathbf{x}^2 | \mathbf{x} \in W_s \rangle < W_{2s}$.

Lemma 5. Any $\mathcal{L}^2\mathcal{S}$-subspace U_s, $\mathcal{L}^1\mathcal{S}$-subspace U'_s and $\mathcal{L}^0\mathcal{S}$-subspace U''_s is invariant under collineation. The dimensions of these subspaces are given by:

$$\begin{aligned} Dim(U_s) &= \tbinom{n+1}{2}\tbinom{n+s}{s} + \tbinom{n+s+1}{s+1}, \\ Dim(U'_s) &= \tbinom{n+1}{1}\tbinom{n+s}{s}, \\ Dim(U''_s) &= \tbinom{n+s}{s}. \end{aligned}$$

The partial derivative mapping is a linear mapping, so any series of partial derivatives defines linear transformations $W_{2s+2} \to W_{2s+1} \to W_{2s} \to W_{2s-1}$. Thus any series of repeated partial differentiation in even characteristic gives rise to a series of linear transformations $U_s \to U'_s \to U''_s \to \{0\}$ or informally $\mathcal{L}^2\mathcal{S} \to \mathcal{L}^1\mathcal{S} \to \mathcal{L}^0\mathcal{S} \to 0$. Our analysis of rank-2 product polynomials in even characteristic now proceeds by considering even and odd degree polynomials as separate cases.

3.1 A Rank-2 Product Polynomial of Even Degree

We can write the even degree D as $D = 2s + 2$, so a rank-2 product polynomial $g \in \mathcal{R}^{2s+2}_{\mathbb{F},n}$ can be expressed as

$$g = \sum_{i=0}^{2s+2} \alpha_i^2 \, L^i (L')^{2s+2-i} = \sum_{i=0}^{s+1} \alpha_{2i}^2 \, L^{2i} (L')^{2(s+1-i)} + \sum_{i=0}^{s} \alpha_{2i+1}^2 \, L^{2i+1} (L')^{2s+1-2i}.$$

Thus we can express a rank-2 product polynomial g of even degree as

$$g = \left(\sum_{i=0}^{s+1} \alpha_{2i} \, L^i (L')^{(s+1-i)} \right)^2 + LL' \left(\sum_{i=0}^{s} \alpha_{2i+1} \, L^i (L')^{s-i} \right)^2.$$

We denote the first square of degree $2(s + 1)$ by S^* and the second square of degree $2s$ by S, so g is given by

$$g = LL'S + S^*.$$

As $\mathbb{F}$ has even characteristic, any partial derivative of S or S^* vanishes, so a partial derivative of $g \in \mathcal{R}^{2s+2}_{\mathbb{F},n}$ is given by

$$\frac{\partial g}{\partial x_l} = \frac{\partial (LL')}{\partial x_l} S = \frac{\partial L}{\partial x_l} L'S + \frac{\partial L'}{\partial x_l} LS = a_l (L'S) + a'_l (LS).$$

We have therefore shown that the partial derivative of a rank-2 product polynomial of even degree with respect to any variable is a linear combination of $L'S$ and LS. The above comments are summarised in Lemma 6.

Lemma 6. Let $g \in \mathbb{F}[x_0, \ldots, x_n]$ be a rank-2 product polynomial of even degree $2s+2$. If the field $\mathbb{F}$ has even characteristic, then $g \in \mathcal{R}^{2s+2}_{\mathbb{F},n}$ has the following properties:

1. $g \in U_s$, the $\mathcal{L}^2\mathcal{S}$-subspace;
2. $\frac{\partial g}{\partial x_l} \in U'_s$, the $\mathcal{L}^1\mathcal{S}$-subspace;
3. the partial derivatives matrix $C^{(1)}_g$ has rank at most 2.

3.2 A Rank-2 Product Polynomial of Odd Degree

We can write the odd degree D as $D = 2s+1$, so a rank-2 product polynomial $g \in \mathcal{R}^{2s+1}_{\mathbb{F},n}$ can be expressed as

$$g = \sum_{i=0}^{2s+1} \alpha_i^2 \, L^i (L')^{2s+1-i} = \sum_{i=0}^{s} \alpha_{2i}^2 \, L^{2i} (L')^{2s+1-2i} + \sum_{i=0}^{s} \alpha_{2i+1}^2 \, L^{2i+1} (L')^{2s-2i}.$$

We can thus express a rank-2 product polynomial g of odd degree as

$$g = L' \left(\sum_{i=0}^{s} \alpha_{2i} L^i L'^{s-i} \right)^2 + L \left(\sum_{i=0}^{s} \alpha_{2i+1} L^i L'^{s-i} \right)^2$$

The above expression for g consists of two squares of degree $2s$, which we denote by S' and S respectively. We can thus express g as

$$g = LS + L'S'.$$

As S and S' are square polynomials over a field of even characteristic, any partial derivative of S or S' is zero. Thus a partial derivative of $g \in \mathcal{R}^{2s+1}_{\mathbb{F},n}$ is given by

$$\frac{\partial g}{\partial x_l} = \frac{\partial L}{\partial x_l} S + \frac{\partial L'}{\partial x_l} S' = a_l S + a'_l S'.$$

We have therefore shown that the partial derivative of a rank-2 product polynomial of odd degree with respect to any variable is a linear combination of S and S'. The above comments are summarised by Lemma 7.

Lemma 7. Let $g \in \mathbb{F}[x_0, \ldots, x_n]$ be a rank-2 product polynomial of odd degree $2s+1$. If the field $\mathbb{F}$ has even characteristic, then $g \in \mathcal{R}^{2s+1}_{\mathbb{F},n}$ has the following properties:

1. $g \in U'_s$, the $\mathcal{L}^1\mathcal{S}$-subspace,
2. $\frac{\partial g}{\partial x_l} \in U''_s$, that is any partial derivative of g is a square;
3. the partial derivatives matrix $C^{(1)}_g$ has rank at most 2.

3.3 A Necessary Criterion for a Rank-2 Product Polynomial

Definition 6. The $\mathcal{LS}$*-criterion* for a homogeneous multivariate polynomial g is that g is an element either of the $\mathcal{L}^2\mathcal{S}$-subspace (even degree) or the $\mathcal{L}^1\mathcal{S}$-subspace (odd degree).

Lemmas 6 and 7 show that for a polynomial $g = \sum_{l=1}^{m} \lambda_l f_l$ to be a rank-2 product polynomial, g has to satisfy the $\mathcal{LS}$*-criterion*. For equation systems of cubic or higher degree, Lemma 5 shows that the dimension of the $\mathcal{L}^2\mathcal{S}$-subspace or the $\mathcal{L}^1\mathcal{S}$-subspace is generally far smaller than the dimension of W_D. For such equation systems, we can therefore obtain many linear constraints on $\lambda_1, \ldots, \lambda_m$ for $g = \sum_{l=1}^{m} \lambda_l f_l$ to be a rank-2 product polynomial. These linear constraints can be processed very efficiently using basic linear algebra. Thus this criterion alone can easily greatly reduce the size of or even solve the equation system.

We give an example of solving a cubic system over a field of even characteristic by considering membership of the $\mathcal{L}^1\mathcal{S}$-subspace U_1' in Appendix B. However, both the $\mathcal{L}^1\mathcal{S}$-subspace and and $\mathcal{L}^2\mathcal{S}$-subspace contain many polynomials that are not rank-2 product polynomials, so there may be a requirement for further processing after this preliminary linear filtering. Furthermore, this criterion cannot be applied to quadratic systems as $U_0 = W_2$. We discuss further techniques to identify rank-2 product polynomials in Section 4.

4 Identification of a Rank-2 Product Polynomial

The basic idea of the `GeometricXL` algorithm to solve the homogeneous system $f_1 = \ldots = f_m = 0$ of degree D in $n+1$ variables is to find a linear combination such that $g = \sum_{l=1}^{m} \lambda_l f_l$ is a rank-2 product polynomial, that is $g \in \mathcal{R}^D_{\mathbb{F},n}$. However, in even characteristic we can use the properties of rank-2 product polynomials in even characteristic given by Lemma 6 and Lemma 7 to help identify such polynomials. This should enable us subsequently to develop a method for fields of even characteristic based on the `GeometricXL` algorithm. However, we note that such an algorithm still has the potential problem discussed in Section 7.5 of [12], namely the possibility of nested multiple linear factors only one of which corresponds to a solution.

4.1 Multivariate Quadratic Systems

We consider a field $\mathbb{F}$ of even characteristic and a homogeneous quadratic equation system $f_1 = \ldots = f_m = 0$ over $\mathbb{F}$. We need to find a linear combination $g = \sum_{l=1}^{m} \lambda_l f_l$ such that g is a rank-2 product polynomial of degree 2. However, any such $g \in \mathcal{R}^2_{\mathbb{F},n}$ can be regarded as the product of the two homogeneous linear polynomials L and L' (Section 3.1), that is g is of the form

$$(a_0x_0 + \ldots + a_0x_0)(a_0'x_0 + \ldots + a_n'x_n) = \sum_{i=0}^{n} a_i a_i' x_i^2 + \sum_{i=1}^{n} \sum_{j=0}^{i-1} (a_i a_j' + a_i' a_j) x_i x_j.$$

We can write $\Delta_{ij} = a_i a'_j + a_j a'_i$, so the product of two homogeneous linear polynomials can be expressed as

$$g = LL' = (a_0 x_0 + \ldots a_n x_n)(a'_0 x_0 + \ldots a'_n x_n) = \sum_{i=0}^{n} a_i a'_i x_i^2 + \sum_{i=1}^{n} \sum_{j=0}^{i-1} \Delta_{ij} x_i x_j.$$

We can write the homogeneous quadratic polynomial f_l $(1 \leq l \leq m)$ as

$$f_l = \sum_{i=0}^{n} d_{ii}^{(l)} x_i^2 + \sum_{i=1}^{n} \sum_{j=0}^{i-1} d_{ij}^{(l)} x_i x_j$$

for coefficients $d_{ij}^{(l)}$, so a rank-2 product polynomial $g = \sum_{l=1}^{m} \lambda_l f_l$ satisfies

$$\begin{array}{rcccccc} g = & \sum_{i=0}^{n} & \left(\sum_{l=1}^{m} \lambda_l d_{ii}^{(l)} \right) & x_i^2 + \sum_{i=1}^{n} \sum_{j=0}^{i-1} & \left(\sum_{l=1}^{m} \lambda_l d_{ij}^{(l)} \right) & x_i x_j \\ = & \sum_{i=0}^{n} & a_i a'_i & x_i^2 + \sum_{i=1}^{n} \sum_{j=0}^{i-1} & \Delta_{ij} & x_i x_j. \end{array}$$

Thus for g to be a rank-2 product polynomial, we can see by equating coefficients of $x_i x_j$ $(j < i)$ that we require $\lambda_1, \ldots, \lambda_m$ such that $\Delta_{ij} = \sum_{l=1}^{m} d_{ij}^{(l)} \lambda_l$.

Let A be the $2 \times (n+1)$ matrix with rows given by the (unknown) coefficients of the linear polynomials L and L', so

$$A = \begin{pmatrix} a_0 \ldots a_i \ldots a_j \ldots a_n \\ a'_0 \ldots a'_i \ldots a'_j \ldots a'_n \end{pmatrix},$$

then the Δ_{ij} are the 2-minors (2×2 sub-determinants) of A. Now, there are $\binom{n+1}{4}$ 4-minors of the $4 \times (n+1)$ matrix $\overline{A} = \left(\frac{A}{A} \right)$, and these are given by

$$\mathcal{A}_{i_1,i_2,i_3,i_4} = \Delta_{i_1,i_2} \Delta_{i_3,i_4} + \Delta_{i_1,i_3} \Delta_{i_2,i_4} + \Delta_{i_1,i_4} \Delta_{i_2,i_3}.$$

However, the matrix $\overline{A}$ clearly has rank at most 2, so every 4-minor of $\overline{A}$ is identically 0. Thus we obtain $\binom{n+1}{4}$ identities $\mathcal{A}_{i_1,i_2,i_3,i_4} = 0$. As each 4-minor $\mathcal{A}_{i_1,i_2,i_3,i_4}$ of $\overline{A}$ gives rise to a homogeneous quadratic expression in Δ_{ij}, so each 4-minor identity $\mathcal{A}_{i_1,i_2,i_3,i_4} = 0$ gives a homogeneous quadratic identity in Δ_{ij}.

We saw above that for $g = \sum_{l=1}^{m} \lambda_l f_l$ to be a rank-2 product polynomial, we require that $\Delta_{ij} = \sum_{l=1}^{m} d_{ij}^{(l)} \lambda_l$. Thus the $\binom{n+1}{4}$ identities $\mathcal{A}_{i_1,i_2,i_3,i_4} = 0$ give rise to a homogeneous quadratic system with $\binom{n+1}{4} \sim \frac{1}{24} n^4$ equations satisfied by $\lambda_1, \ldots, \lambda_m$. We can potentially solve this system using linearisation or some other simple technique. If there is a unique solution to this quadratic system in $\lambda_1, \ldots, \lambda_m$, then this can directly determine the solution of the original equation system. More generally, an analysis of this quadratic system gives much information about the original quadratic system, which could then be used with other techniques to provide a solution to the original system.

We make some comments about geometric aspects of this process in Section 5.2, and demonstrate the use of this process in finding a solution to a quadratic system in Appendix C.

4.2 Multivariate Systems of Quartic or Higher Even Degree

We consider a field $\mathbb{F}$ of even characteristic and a homogeneous equation system $f_1 = \ldots = f_{m'} = 0$ of degree $D = 2s + 2$ ($s > 0$) over $\mathbb{F}$, where without loss of generality this equation system may have been obtained by applying the $\mathcal{L}^2\mathcal{S}$ criterion of Section 3.3 to a larger system $f_1 = \ldots = f_m = 0$ (so $m' \leq m$). We need to find a linear combination $g = \sum_{l=1}^{m'} \lambda_l f_l$ such that g is a rank-2 product polynomial, that is $g \in \mathcal{R}^{2s+2}_{\mathbb{F},n}$. In the quadratic case ($s = 0$), we consider the coefficients of the non-square monomials $x_i x_j$ (so $i \neq j$) to give conditions for a rank-2 product polynomial (Section 4.1). In the case of quartic and higher even degree, we first consider the coefficients Γ_{ij} of $x_i^{2s+1} x_j$ (for $i \neq j$) in g, a natural generalisation of this idea.

If g is a rank-2 product polynomial of degree $2s + 2$, so $g \in \mathcal{R}^{2s+2}_{\mathbb{F},n}$, then $g = LL'S + S^*$, where L and L' are the homogeneous linear polynomials of Section 3 and S and S^* are homogeneous square polynomials of degree $2s$ and $2s + 2$ respectively (Section 3.1). Thus if we let s_i denote the coefficient of x_i^{2s} in S we have

$$\begin{aligned} g &= (a_i x_i + a_j x_j + \ldots)(a'_i x_i + a'_j x_j + \ldots)(s_i x_i^{2s} + \ldots) + S^* \\ &= \Gamma_{ij} x_i^{2s+1} x_j + \ldots = s_i \Delta_{ij} x_i^{2s+1} x_j + \ldots = (b_i a'_j + b'_i a_j) x_i^{2s+1} x_j + \ldots, \end{aligned}$$

where $\Delta_{ij} = a_i a'_j + a'_i a_j$ is a 2-minor of the matrix A of Section 4.1 and $b_i = s_i a_i$ and $b'_i = s_i a'_i$. Thus we have $\Gamma_{ij} = s_i \Delta_{ij} = b_i a'_j + b'_i a_j$ for $i \neq j$. For completeness, we set $\Gamma_{ii} = b_i a'_i + b'_i a_i = s_i a_i a'_i + s_i a_i a'_i = 0$. The matrix $\Gamma = (\Gamma_{ij})$ can be expressed as $\Gamma = B + B'$, where $B = \mathbf{b}\mathbf{a}'^T$ and $B' = \mathbf{b}'\mathbf{a}^T$ for appropriate column vectors of coefficients $\mathbf{b}$, $\mathbf{a}$, $\mathbf{b}'$ and $\mathbf{a}'$, so B and B' are both matrices of rank 1. Thus the matrix Γ of coefficients of $x_i^{2s+1} x_j$ (for $i \neq j$ with $\Gamma_{ii} = 0$) of a rank-2 product polynomial has rank at most 2 as it is the sum $\Gamma = B + B'$ of two matrices of rank 1. There are $\binom{n+1}{3}^2$ 3-minors of Γ, and they are given by

$$\begin{aligned} \mathcal{B}_{i_1,i_2,i_3,j_1,j_2,j_3} = \; & \Gamma_{i_1,j_1}\Gamma_{i_2,j_2}\Gamma_{i_3,j_3} + \Gamma_{i_1,j_1}\Gamma_{i_2,j_3}\Gamma_{i_3,j_2} + \Gamma_{i_2,j_1}\Gamma_{i_1,j_2}\Gamma_{i_3,j_3} \\ & + \Gamma_{i_2,j_1}\Gamma_{i_1,j_3}\Gamma_{i_3,j_2} + \Gamma_{i_3,j_1}\Gamma_{i_1,j_2}\Gamma_{i_2,j_3} + \Gamma_{i_3,j_1}\Gamma_{i_1,j_3}\Gamma_{i_2,j_2}. \end{aligned}$$

However, every 3-minor of the matrix Γ of rank 2 vanishes, so we obtain $\binom{n+1}{3}^2$ identities $\mathcal{B}_{i_1,i_2,i_3,j_1,j_2,j_3} = 0$.

For g to be a rank-2 product polynomial, we can see by equating coefficients of $x_i^{2s+1} x_j$ ($i \neq j$) that we require $\lambda_1, \ldots, \lambda_{m'}$ such that $\Delta_{ij} = \sum_{l=1}^{m'} d_{ij}^{(l)} \lambda_l$, where $d_{ij}^{(l)}$ denote the coefficient of $x_i^{2s+1} x_j$ in f_l. Thus the $\binom{n+1}{3}^2$ identities $\mathcal{B}_{i_1,i_2,i_3,j_1,j_2,j_3} = 0$ give rise to a homogeneous cubic system with $\binom{n+1}{3}^2 \sim \frac{1}{36} n^6$ equations satisfied by $\lambda_1, \ldots, \lambda_{m'}$. It may now be possible to solve this resulting cubic system in $\lambda_1, \ldots, \lambda_{m'}$ by linearisation or some other method, so providing a solution to the original equation system. We provide an example of this process to solve a homogeneous quartic system in Appendix D.

We also note that it is very easy to produce further homogeneous cubic equations in $\lambda_1, \ldots, \lambda_{m'}$ if required, as Γ is far from being the only matrix of coefficients having rank 2. For example, a similar argument to that given above for Γ shows that the matrix of coefficients of $x_0^2 x_i^{2s-1} x_j$ also has rank 2 and so on.

4.3 Multivariate Systems of Odd Degree

We consider a field $\mathbb{F}$ of even characteristic and a homogeneous equation system $f_1 = \ldots = f_{m'} = 0$ of odd degree $D = 2s + 1$ over $\mathbb{F}$, where without loss of generality this equation system may have been obtained by applying the $\mathcal{L}^1\mathcal{S}$ criterion of Section 3.3 to a larger system $f_1 = \ldots = f_m = 0$ (so $m' \leq m$). We need to find a linear combination $g = \sum_{l=1}^{m'} \lambda_l f_l$ such that g is a rank-2 product polynomial, that is $g \in \mathcal{R}_{\mathbb{F},n}^{2s+1}$. In a similar way to the case for even degree, we consider the coefficients Λ_{ij} of $x_i^{2s}x_j$ in g, including the coefficients Λ_{ii} of x_i^{2s+1}.

If g is a rank-2 product polynomial of degree $2s+1$, so $g \in \mathcal{R}_{\mathbb{F},n}^{2s+1}$, then we can express g as $g = LS + L'S'$, where L and L' are homogeneous linear polynomials and S and S' are homogeneous square polynomials of degree $2s$ (Section 3.2). We can thus express a summand of g as

$$LS = c_{ij}x_i^{2s}x_j + \ldots = (s_i x_i^{2s} + \ldots)(a_j x_j + \ldots) = s_i a_j x_i^{2s} x_j + \ldots,$$

so the matrix $C = (c_{ij})$ has rank 1 as $C = \mathbf{s}\mathbf{a}^T$ for appropriate column vectors of coefficients $\mathbf{s}$ and $\mathbf{a}$. This means we can express g as

$$g = \Lambda_{ij}x_i^{2s}x_j + \ldots = LS + L'S' = (c_{ij} + c'_{ij})x_i^{2s}x_j + \ldots.$$

Thus the matrix $\Lambda = (\Lambda_{ij})$ of coefficients of $x_i^{2s}x_j$ of a rank-2 product polynomial has rank at most 2 as it is the sum $\Lambda = C + C'$ of two matrices of rank 1. There are $\binom{n+1}{3}^2$ 3-minors of Λ, and they are given by

$$\begin{aligned}\mathcal{C}_{i_1,i_2,i_3,j_1,j_2,j_3} = \quad & \Lambda_{i_1,j_1}\Lambda_{i_2,j_2}\Lambda_{i_3,j_3} + \Lambda_{i_1,j_1}\Lambda_{i_2,j_3}\Lambda_{i_3,j_2} + \Lambda_{i_2,j_1}\Lambda_{i_1,j_2}\Lambda_{i_3,j_3} \\ & + \Lambda_{i_2,j_1}\Lambda_{i_1,j_3}\Lambda_{i_3,j_2} + \Lambda_{i_3,j_1}\Lambda_{i_1,j_2}\Lambda_{i_2,j_3} + \Lambda_{i_3,j_1}\Lambda_{i_1,j_3}\Lambda_{i_2,j_2}.\end{aligned}$$

However, every 3-minor of Λ vanishes as Λ has rank 2, so we obtain $\binom{n+1}{3}^2$ identities $\mathcal{C}_{i_1,i_2,i_3,j_1,j_2,j_3} = 0$.

For g to be a rank-2 product polynomial, we can see by equating coefficients of $x_i^{2s}x_j$ $(i \neq j)$ that we require $\lambda_1, \ldots, \lambda_{m'}$ such that $\Delta_{ij} = \sum_{l=1}^{m'} d_{ij}^{(l)}\lambda_l$, where $d_{ij}^{(l)}$ denote the coefficient of $x_i^{2s}x_j$ in f_l. Thus the $\binom{n+1}{3}^2$ identities $\mathcal{C}_{i_1,i_2,i_3,j_1,j_2,j_3} = 0$ give rise to a homogeneous cubic system with $\binom{n+1}{3}^2 \sim \frac{1}{36}n^6$ equations satisfied by $\lambda_1, \ldots, \lambda_{m'}$. It may now be possible to solve this resulting cubic system in $\lambda_1, \ldots, \lambda_{m'}$ by linearisation or some other method, so providing a solution to the original equation system. We provide an example of this process to solve a quintic system in Appendix E. Furthermore, as in Section 4.2, we note that is very easy to produce further homogeneous cubic equations in $\lambda_1, \ldots, \lambda_{m'}$ if required as there are many other coefficient matrices having rank 2, for example the matrix of coefficients of $x_0^2 x_i^{2s-2}x_j$.

5 A Geometrical Interpretation

The geometric techniques of Section 4 can be interpreted using the Grassmannian variety [3,9,10]. We give some basic properties of the Grassmannian variety in Section 5.1 and discuss their application in Section 5.2.

5.1 The Grassmannian Variety and Exterior Algebra

We recall that W_1 denotes the vector space of homogeneous linear polynomials over $\mathbb{F}$ of degree D in $n+1$ variables (Section 3). Thus the two linear polynomials L and L' at the heart of Definition 1 are elements of W_1, so the pair (L, L') defines a (projective) line in the projective space $\mathcal{P}(W_1)$. The *Grassmannian* $Gr_2(W_1)$ is the set of all 2-dimensional subspaces of W_1 or equivalently the set of all projective lines in this projective space $\mathcal{P}(W_1)$ [9,10].

The tensor product $W_1 \bigotimes W_1$ is the $(n+1)^2$-dimensional vector space with basis vectors the set of formal symbols $x_i \otimes x_j$ and a bilinear inclusion map from $W_1 \times W_1$ to $W_1 \bigotimes W_1$ [4,12]. The symmetric square $\mathbb{S}^2(W_1)$ is the subspace of all symmetric tensors $(\{t_{ij} \in W_1 \bigotimes W_1 \mid t_{ij} = t_{ji}\})$, a subspace of dimension $\frac{1}{2}(n+1)(n+2)$ [9,12]. In even characteristic, the symmetric square can be decomposed as

$$\mathbb{S}^2(W_1) \cong \langle (x_i \otimes x_i)_i \rangle \oplus \frac{\mathbb{S}^2(W_1)}{\langle (x_i \otimes x_i)_i \rangle},$$

where the second (quotient) summand is the degree-2 part of the *exterior algebra*, a space of dimension $\frac{1}{2}n(n+1)$, which we denote by $\mathbb{E}^2(W_1)$. Thus we have $\mathbb{S}^2(W_1) \cong \langle (x_i \otimes x_i)_i \rangle \oplus \mathbb{E}^2(W_1)$. The Grassmannian or *Plücker embedding* of the Grassmannian $Gr_2(W_1)$ in the degree-2 part of the exterior algebra is an injective mapping $\psi\colon Gr_2(W_1) \to \mathcal{P}(\mathbb{E}^2(W_1))$ defined by $(L, L') \mapsto L \wedge L'$ or equivalently

$$(L, L') = \left(\sum_{i=0}^{n} a_i x_i, \sum_{i=0}^{n} a'_i x_i \right) \mapsto \sum_{i=0}^{n} \sum_{j=0}^{i-1} (a_i a'_j + a'_i a_j)(x_i \wedge x_j).$$

This vector of co-ordinates $(a_i a_j + a'_i a_j)$ is known as the Grassmannian or *Plücker co-ordinates* of the (projective) line defined by L and L'. Thus the Grassmannian co-ordinates of the line defined by L and L' are given by the 2-minors of the matrix A of Section 4.1, with rows given by L and L'.

The Grassmannian embedding allows the representation of (projective) lines in $\mathcal{P}(W_1)$ as distinct points in the projective space $\mathcal{P}(\mathbb{E}^2(W_1))$, which is isomorphic to $\mathrm{PG}(\frac{1}{2}n(n+1)-1, \mathbb{F})$. The *Grassmannian variety* $\mathcal{G}$ of $\mathcal{P}(\mathbb{E}^2(W_1))$ is the set of all such embedded lines [3,9]. Thus the *Grassmannian variety* $\mathcal{G}$ is simply $\psi(Gr_2(W_1))$, the image of the Grassmannian $Gr_2(W_1)$, so $\mathcal{G}$ is defined by

$$\mathcal{G} = \left\{ \left\langle (\Delta_{21}, \Delta_{31}, \ldots, \Delta_{n+1,n-1}, \Delta_{n+1,n})^T \right\rangle \in \mathcal{P}(\mathbb{E}^2(W_1)) \;\middle|\; \mathcal{A}_{i_1,i_2,i_3,i_4} = 0 \right\},$$

where $\mathcal{A}_{i_1,i_2,i_3,i_4}$ is the quadratic identity of Section 4.1. Thus the Grassmannian variety $\mathcal{G}$ can be defined by the intersection of quadrics in $\mathcal{P}(\mathbb{E}^2(W_1))$.

5.2 The Grassmannian Variety and the `GeometricXL` Algorithm

We consider first a `GeometricXL` algorithm for homogeneous quadratic systems in even characteristic, discussed in Section 4.1. We need to find $g = \sum_{i=1}^{m} \lambda_l f_l$ such that g is the product of two homogeneous linear polynomials L and L'. We

can think of g in the natural and obvious way as an element of $\mathbb{S}^2(W_1)$. Thus we can define the canonical projection $\pi(g)$ of g onto the exterior algebra $\mathbb{E}^2(W_1)$, so $\pi(g)$ is the square-free part of g. However, g is a product of linear polynomials if and only if $\pi(g) \in \mathcal{G}$, the Grassmannian variety. Thus the geometrical interpretation of the process of Section 4.1 is that it is a process that first attempts to find polynomials with no square terms in the variety

$$\mathcal{G} \bigcap \langle \pi(f_1), \ldots, \pi(f_m) \rangle ,$$

and then analyses these polynomials to find rank-2 product polynomials.

There are some further obvious geometric comments that can be made about higher degree equations systems. For example, for odd degree systems any solution lies on the secant variety of the variety of all polynomials which are the product of a linear polynomial and a square polynomial, and such secant varieties are the basis of the `GeometricXL` algorithm when the characteristic exceeds D or is zero [12]. However, a full geometric interpretation is still needed for cubic and higher degree equation systems, and could provide interesting ideas for solution methods. Such an interpretation is very likely to depend on the Grassmannian variety $\mathcal{G}$ as any rank-2 product polynomial depends fundamentally on the linear polynomials L and L', or equivalently such an interpretation depends fundamentally on a point of the Grassmannian variety $\mathcal{G}$.

6 The `EGHAM` Process

In the common cryptographic situation of attempting to find a unique solution to a homogeneous equation system $f_1 = \ldots = f_m = 0$ over a field of even characteristic, the goal of the XL algorithm is to find a bivariate polynomial $g = \sum_{i=1}^{m} \lambda_i f_i$, and the goal of the Gröbner basis algorithm (under lexicographic ordering) is to find such a bivariate polynomial g in the reduced Gröbner basis. However, we have shown that any such linear combination of homogeneous polynomials generating such a bivariate polynomial g must satisfy the $\mathcal{LS}$-criterion. Thus the $\mathcal{LS}$-criterion (Definition 6) can be applied as part of a standard Gröbner basis or `XL` algorithm in this situation. Applying the $\mathcal{LS}$-criterion generally greatly reduces the number of polynomials under consideration by an `XL` algorithm or Gröbner basis algorithm. Furthermore, the reduced set of equations obtained by applying the $\mathcal{LS}$-criterion can be considered for any order of the variables, as the $\mathcal{LS}$-criterion is independent of the order of the variables. This means that the `XL` algorithm or Gröbner basis algorithm with the $\mathcal{LS}$-criterion is far more efficient at finding an appropriate bivariate polynomial or concluding that no such bivariate polynomial exists for a given degree (under any variable order).

We can therefore include the $\mathcal{LS}$-criterion as part of an adaptation, using the ideas of Section 4, of the `GeometricXL` algorithm [12] for use in fields of even characteristic. This gives us a process for implementing an even (characteristic) `GeometricXL` heuristic algorithmic method, which we term the `EGHAM` process and which we describe in Figure 1.

- Generate a homogeneous system $f_1 = \ldots = f_m = 0$ of degree D from an original equation system in even characteristic.
- Apply the $\mathcal{LS}$-criterion (Definition 6), that is consider only linear combinations of $f_1, \ldots, f_m$ in the $\mathcal{L}^2\mathcal{S}$-subspace or $\mathcal{L}^1\mathcal{S}$-subspace for systems of cubic or higher degrees, so generally reducing the size of the problem from m equations to m' equations.
- Construct a quadratic or cubic equation system in the coefficients $\lambda_1, \ldots, \lambda_{m'}$ for $\sum_{i=1}^{m'} \lambda_i f_i$ to be a rank-2 product polynomial, for example by considering the matrix of coefficients of $x_i^{D-1}x_j$ (Section 4).
- Analyse this quadratic or cubic system, perhaps by linearisation, to find a rank-2 product polynomial in $\langle f_1, \ldots, f_{m'} \rangle$, which can then be factored to provide information about the solution of (or even solve) $f_1 = \ldots = f_m = 0$.
- Apply this solution information directly to the original equation system.

Fig. 1. Basic Description of the `EGHAM` Process

The `EGHAM` process is an adaptation of the `GeometricXL` algorithm to fields of even characteristic, and so is a geometric generalisation of an `XL` algorithm for such fields. Thus the `EGHAM` process generates equations of at worst the same degree as either a Gröbner basis (with lexicographic ordering) or an `XL` algorithm, though usually by processing a far smaller equation system through the application of the $\mathcal{LS}$-criterion. However, as is clearly demonstrated by the examples in the Appendices, the `EGHAM` process can use polynomials of a much smaller degree for many equation systems in even characteristic than a Gröbner basis algorithm or an `XL` algorithm.

7 Conclusions

A major contribution of this paper is the development of the $\mathcal{LS}$-criterion (Definition 6) in the solution of homogeneous cryptographic equation systems in fields of even characteristic. We have used the $\mathcal{LS}$-criterion to develop the `EGHAM` process, an adaptation of the `GeometricXL` algorithm [12] which is suitable for use in fields of even characteristic. The `EGHAM` process can find the solution of a cryptographic equation system in even characteristic much more efficiently than a standard Gröbner basis or `XL` algorithm in many cases.

Acknowledgments

We wish to thank Martin Albrecht and our referees for their comments.

References

1. Ars, G., Faugère, J.-C., Imai, H., Kawazoe, M., Sugita, M.: Comparison between XL and Gröbner Basis Algorithms. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 338–353. Springer, Heidelberg (2004)

2. Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD thesis, Universität Innsbruck (1965)
3. Burau, W.: Mehrdimensionale Projecktive und Höhere Geometrie, Berlin (1961)
4. Cohn, P.: Classical Algebra. John Wiley, Chichester (2000)
5. Courtois, N., Klimov, A., Patarin, J., Shamir, A.: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 392–407. Springer, Heidelberg (2000)
6. Faugère, J.-C.: A New Efficient Algorithm for Computing Gröbner bases (F4). Journal of Pure and Applied Algebra 139, 61–88 (1999)
7. Faugère, J.-C.: A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5). In: Mora, T. (ed.) International Symposium on Symbolic and Algebraic Computation – ISSAC 2002, pp. 75–83 (2002)
8. Faugère, J.-C., Levy-dit-Vehel, F., Perret, L.: Cryptanalysis of MinRank. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 280–296. Springer, Heidelberg (2008)
9. Harris, J.: Algebraic Geometry: A First Course. Graduate Text in Mathematics, vol. 133. Springer, Heidelberg (1992)
10. Hirschfeld, J.W.P., Thas, J.A.: General Galois Geometries. Oxford University Press, Oxford (1991)
11. Iarrobino, A., Kanev, V.: Power Sums, Gorenstein Algebras and Determinantal Loci. Lecture Notes in Mathematics, vol. 1725. Springer, Heidelberg (1999)
12. Murphy, S., Paterson, M.B.: A Geometric View of Cryptographic Equation Solving. Journal of Mathematical Cryptology 2, 63–107 (2008)

A The Alternative `GeometricXL` Algorithm

We demonstrate the alternative `GeometricXL` algorithm (Section 2.2) on a homogeneous cubic system $f_1 = f_2 = f_3 = 0$ of three equations in three variables over GF(37). We give the coefficents of f_1, f_2, f_3 below with respect to the lexicographic monomial ordering $x_0^3, x_0^2x_1, \ldots, x_2^3$.

$$\begin{array}{cccccccccc} 23 & 27 & 15 & 25 & 11 & 24 & 26 & 7 & 21 & 36 \\ 21 & 35 & 2 & 18 & 4 & 1 & 29 & 5 & 32 & 33 \\ 32 & 13 & 28 & 10 & 8 & 13 & 24 & 10 & 19 & 15 \end{array}$$

We need to find a linear combination $\lambda_1 C_{f_1}^{(1)} + \lambda_2 C_{f_2}^{(1)} + \lambda_3 C_{f_3}^{(1)}$ of these first order partial derivatives matrices $C_{f_1}^{(1)}$, $C_{f_2}^{(1)}$ and $C_{f_3}^{(1)}$ that has rank 2. Thus we need to find $\lambda_1, \lambda_2, \lambda_3$ such that

$$\begin{aligned} \lambda_1 & \begin{pmatrix} 32 & 17 & 30 & 25 & 11 & 24 \\ 27 & 13 & 11 & 4 & 14 & 21 \\ 15 & 11 & 11 & 7 & 5 & 34 \end{pmatrix} \\ + \lambda_2 & \begin{pmatrix} 26 & 33 & 4 & 18 & 4 & 1 \\ 35 & 36 & 4 & 13 & 10 & 32 \\ 2 & 4 & 2 & 5 & 27 & 25 \end{pmatrix} \\ + \lambda_3 & \begin{pmatrix} 22 & 26 & 19 & 10 & 8 & 13 \\ 13 & 20 & 8 & 35 & 20 & 19 \\ 28 & 8 & 26 & 10 & 1 & 8 \end{pmatrix} \end{aligned}$$

has rank 2. We can identify a matrix of rank 2 by considering its 3-minors, and, as an example, the first 3-minor of the above matrix is given by

$$34\lambda_1^3+22\lambda_1^2\lambda_2+30\lambda_1^2\lambda_3+19\lambda_1\lambda_2^2+9\lambda_1\lambda_2\lambda_3+9\lambda_1\lambda_3^2+22\lambda_2^3+20\lambda_2^2\lambda_3+27\lambda_2\lambda_3^2+5\lambda_3^3.$$

There are 15 3-minors of the above 3×6 matrix, and we require them all to vanish for this matrix to have rank 2. This gives a system of 15 homogeneous cubic equations in $\lambda_1, \lambda_2, \lambda_3$. However, there are only 10 cubic monomials in 3 variables, so we can solve this system by direct linearisation to obtain $\lambda_1 = \lambda_3$ and $\lambda_2 = 26\lambda_3$ as the unique solution. We thus consider the polynomial $g = f_1 + 26f_2 + f_3$ which has a vector of coefficients given by $(9, 25, 21, 22, 12, 26, 27, 36, 21, 21)$ (with respect to lexicographic ordering) and partial derivatives matrix of rank 2

$$C_g^{(1)} = C_{f_1}^{(1)} + 26C_{f_2}^{(1)} + C_{f_3}^{(1)} = \begin{pmatrix} 27 & 13 & 5 & 22 & 12 & 26 \\ 25 & 7 & 12 & 7 & 35 & 21 \\ 21 & 12 & 15 & 36 & 5 & 26 \end{pmatrix}.$$

We can now either factor g directly or by noting that any factor of g is a linear combination (possibly over an extension field) of $27x_0 + 25x_1 + 21x_2$ and $13x_0 + 7x_1 + 12x_2$, which are given by a basis for the column space of $C_g^{(1)}$. Thus we obtain a factorisation over GF(37) of a linear combination of f_1, f_2, f_3 as

$$f_1 + 26f_2 + f_3 = 9(x_0 + 32x_1 + 3x_2)(x_0^2 + 16x_0x_1 + 24x_0x_2 + 29x_1^2 + 24x_1x_2 + 9x_2^2)$$

For a solution in GF(37), we obtain $x_0 = -(32x_1 + 3x_2)$, which on substitution into f_1 gives (over GF(37))

$$0 = x_1^3 + x_1^2x_2 + 9x_1x_2^2 + 33x_2^3 = (x_1 + 24x_2)(x_1^2 + 14x_1x_2 + 6x_2^2).$$

Thus over GF(37) we obtain $x_1 = -24x_2 = 13x_2$, so $x_0 = -(32.13+3)x_2 = 25x_2$. This gives $x_1 = 2x_0$ and $x_2 = 3x_0$, so the solution to the homogeneous cubic system $f_1 = f_2 = f_3 = 0$ is given by $(x_1, x_2, x_3) = \mu(1, 2, 3)$ for $\mu \in \mathrm{GF}(37)$. For comparison, calculating this solution using a Gröbner basis or an `XL` algorithm requires the generation of polynomials of degree 6.

B The $\mathcal{LS}$-Criterion

We let $\mathbb{F} = \mathrm{GF}(2)(\theta)$, where $\theta^4 + \theta + 1 = 0$, be a field with 2^4 elements, and we represent elements of this field in hexadecimal, so, for example, `C` denotes $\theta^3+\theta^2$. We consider the solution of the homogeneous cubic system $f_1 = f_2 = f_3 = 0$ over $\mathbb{F}$ by applying the $\mathcal{LS}$-criterion (Definition 6), where f_1, f_2 and f_3 are given below.

$$\begin{array}{l} \mathtt{6}x_0^3 + \mathtt{7}x_0^2x_1 + \mathtt{9}x_0^2x_2 + \mathtt{2}x_0x_1^2 + \mathtt{C}x_0x_1x_2 + \mathtt{5}x_0x_2^2 + \mathtt{F}x_1^3 + \mathtt{0}x_1^2x_2 + \mathtt{D}x_1x_2^2 + \mathtt{6}x_2^3 \\ \mathtt{B}x_0^3 + \mathtt{B}x_0^2x_1 + \mathtt{D}x_0^2x_2 + \mathtt{0}x_0x_1^2 + \mathtt{8}x_0x_1x_2 + \mathtt{4}x_0x_2^2 + \mathtt{5}x_1^3 + \mathtt{6}x_1^2x_2 + \mathtt{3}x_1x_2^2 + \mathtt{A}x_2^3 \\ \mathtt{E}x_0^3 + \mathtt{9}x_0^2x_1 + \mathtt{D}x_0^2x_2 + \mathtt{D}x_0x_1^2 + \mathtt{1}x_0x_1x_2 + \mathtt{A}x_0x_2^2 + \mathtt{1}x_1^3 + \mathtt{3}x_1^2x_2 + \mathtt{C}x_1x_2^2 + \mathtt{5}x_2^3 \end{array}$$

We wish to to find a linear combination $g = \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3 \in \mathcal{R}^3_{\mathbb{F},n}$. The $\mathcal{LS}$-criterion for a cubic system is the $\mathcal{L}^1\mathcal{S}$ condition (Lemma 7 Part 1), that is

$g \in U_1' < W_3$. However, a polynomial in three variables in W_3 is in U_1' if and only if the coefficient of $x_0x_1x_2$ is zero, so we need to find $\lambda_1, \lambda_2, \lambda_3$ such that $\mathtt{C}\lambda_1 + \mathtt{8}\lambda_2 + \mathtt{1}\lambda_3 = 0$. Thus we have $(\lambda_1, \lambda_2, \lambda_3)^T \in \left\langle (\mathtt{1},\mathtt{0},\mathtt{C})^T, (\mathtt{0},\mathtt{1},\mathtt{8})^T \right\rangle$. We can now define $f_1' = f_1 + \mathtt{C}f_3$ and $f_2' = f_2 + \mathtt{8}f_3$, and find a linear combination of f_1' and f_2' which factors either by direct search or by some other technique. We thus obtain

$$f_1' + \mathtt{9}f_2' = f_1 + \mathtt{9}f_2 + \mathtt{8}f_3 = \mathtt{3}(x_0 + x_1 + \mathtt{2}x_2)(x_0^2 + \mathtt{4}x_0x_1 + \mathtt{9}x_0x_2 + \mathtt{4}x_1^2 + \mathtt{A}x_1x_2 + \mathtt{B}x_2^2).$$

This gives $x_0 = x_1 + \mathtt{2}x_2$ as the unique solution over $\mathbb{F}$, and upon substitution into f_1, f_2 and f_3, we obtain the following two linearly independent equations:

$$\begin{aligned} \mathtt{C}x_1^3 + \mathtt{6}x_1^2x_2 + \mathtt{E}x_1x_2^2 + \mathtt{7}x_2^3 &= \mathtt{C}(x_1 + \mathtt{7}x_2)^2(x_1 + \mathtt{9}x_2); \\ \mathtt{5}x_1^3 + \mathtt{5}x_1^2x_2 + \mathtt{1}x_1x_2^2 + \mathtt{0}x_2^3 &= \mathtt{5}x_1(x_1 + \mathtt{5}x_2)(x_1 + \mathtt{9}x_2). \end{aligned}$$

We thus deduce that $x_1 = \mathtt{9}x_2$ and $x_0 = (\mathtt{9} + \mathtt{2})x_2 = \mathtt{B}x_2$, so the solution to $f_1 = f_2 = f_3 = 0$ is given by $(x_0, x_1, x_2) = \mu(\mathtt{4}, \mathtt{2}, \mathtt{1})$ for $\mu \in \mathbb{F}$. For comparison, calculating this solution using a Gröbner basis or an `XL` algorithm requires the generation of polynomials of degree 6.

C A Quadratic System in Even Characteristic

We use the field $\mathbb{F} \cong \mathrm{GF}(2^4)$ of Appendix B. We consider the solution of the homogeneous quadratic system $f_1 = \ldots = f_7 = 0$ using the method of Section 4.1, where $f_1, \ldots, f_7 \in \mathbb{F}[x_0, \ldots, x_6]$. The coefficients of $f_1, \ldots, f_7$ are given with respect to the lexicographic ordering $x_0^2, x_0x_1, \ldots, x_6^2$ by the array below.

```
23BA9D3FCFB453A0E66DC9F5ED2E
7BFE286D5735E433E3D16EB4A5EC
32DAE094C4F5BCB39D206E351686
36EF2B2BC22D93359568C63868B8
6107046B74E7D368D9CAF94136DE
8A0402D168400B71268C39FB5842
8087DF04FFE925F02D4966BE05FD
```

We wish to find $\lambda_1, \ldots, \lambda_7$ such that $g = \lambda_1 f_1 + \ldots \lambda_7 f_7 \in \mathcal{R}^2_{\mathbb{F},n}$, so g is given by

$$\begin{aligned} g = \quad & (\mathtt{2}\lambda_1 + \mathtt{7}\lambda_2 + \mathtt{3}\lambda_3 + \mathtt{3}\lambda_4 + \mathtt{6}\lambda_5 + \mathtt{8}\lambda_6 + \mathtt{8}\lambda_7)x_0^2 \\ & + (\mathtt{3}\lambda_1 + \mathtt{B}\lambda_2 + \mathtt{2}\lambda_3 + \mathtt{6}\lambda_4 + \mathtt{1}\lambda_5 + \mathtt{A}\lambda_6 + \mathtt{0}\lambda_7)x_0x_1 \\ & + (\mathtt{B}\lambda_1 + \mathtt{F}\lambda_2 + \mathtt{D}\lambda_3 + \mathtt{E}\lambda_4 + \mathtt{0}\lambda_5 + \mathtt{0}\lambda_6 + \mathtt{8}\lambda_7)x_0x_2 + \ldots \\ = \quad & \Delta_{01}x_0x_1 + \Delta_{02}x_0x_2 + \ldots. \end{aligned}$$

We can now use the 2-minor identity (Section 4.1)

$$\mathcal{A}_{0,1,2,3} = \Delta_{01}\Delta_{23} + \Delta_{02}\Delta_{13} + \Delta_{03}\Delta_{12} = 0$$

to obtain a quadratic expression $Q(\lambda_1, \ldots, \lambda_7) = 0$, where the coefficients of Q are given with respect to the lexicographic ordering $\lambda_1^2, \lambda_1\lambda_2, \ldots, \lambda_7^2$ by the array

```
F945BAE6371D954722D04A00488A.
```

There are $\binom{7}{4} = 35$ such 2-minor identities giving rise to 35 quadratic expressions in $\lambda_1, \ldots, \lambda_7$ in total. As there are only 28 quadratic monomials in 7 variables, we can express this quadratic system as a linear system in 28 variables using a 35×28 matrix. This matrix has rank 27 and reducing it to echelon form gives the unique (up to multiplication) solution

$$(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7) = (2, \mathtt{C}, 7, 2, \mathtt{F}, 2, 1).$$

We can therefore obtain a linear combination of $f_1, \ldots, f_7$ which is a rank-2 product polynomial and so which factors to give

$$\begin{aligned} 0 &= 2f_1 + \mathtt{C}f_2 + 7f_3 + 2f_4 + \mathtt{F}f_5 + 2f_6 + f_7 \\ &= 6\left(x_0 + \mathtt{E}x_1 + 6x_2 + 6x_3 + \mathtt{B}x_4 + \mathtt{F}x_5 + 6x_6\right)\left(x_0 + 9x_1 + \mathtt{D}x_2 + \mathtt{C}x_3 + 2x_6\right). \end{aligned}$$

Thus we know that either $x_0 + \mathtt{E}x_1 + 6x_2 + 6x_3 + \mathtt{B}x_4 + \mathtt{F}x_5 + 6x_6 = 0$ or $x_0 + 9x_1 + \mathtt{D}x_2 + \mathtt{C}x_3 + 2x_6 = 0$. We can make these two substitutions to reduce the original problem in seven variables to one of two problems in six variables and so on. We thus find that the unique (projective) solution is $(1, 2, 4, 8, 3, 6, \mathtt{C})$. For comparison, calculating this solution using a Gröbner basis or an XL algorithm requires the generation of polynomials of degree 7.

D A Quartic System in Even Characteristic

We use the field $\mathbb{F} \cong \mathrm{GF}(2^4)$ of Appendix B. We consider the solution of the homogeneous quartic system $f_1 = f_2 = f_3 = f_4 = f_5 = 0$ using the method of Section 4.2, where $f_1, \ldots, f_5 \in \mathbb{F}[x_0, x_1, x_2, x_3, x_4]$ satisfy the $\mathcal{LS}$-Criterion (without loss of generality). The coefficients of $f_1, \ldots, f_5$ are given below with respect to the lexicographic ordering $x_0^4, x_0^3x_1, \ldots, x_4^4$.

```
49D32B5BD3D4AD69932C00A0A47A008C971A54E967A6950BB086D2FF0D95D8583B6103
2D68B5EC0F085974058900407984F0A59C80E7924EBA6B03A069D8B9E4DC2A2E7634EB
6E03B1E544DF3352E19D00C082A850CFED40169539B0259520FD730402F6C18FCBDC6D
475365A26C3E7F0CC9EC00E030E8301361A220DCAA9EC573D00D369E441F2A9701149E
D943065F4D8DB2F9629E00303CB9E0EDA6DF00E28151E25960567B58E1AB1441A76B8C
```

A rank-2 product polynomial in even degree is an element of the $\mathcal{L}^2\mathcal{S}$-subspace (Definition 3), and we note without loss of generality that $f_1, \ldots, f_5 \in U_1$, the $\mathcal{L}^2\mathcal{S}$-subspace of W_4.

A linear combination $g = \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3 + \lambda_4 f_4 + \lambda_5 f_5$ is given by

$$\begin{aligned} g = \quad & (4\lambda_1 + 2\lambda_2 + 6\lambda_3 + 4\lambda_4 + \mathtt{D}\lambda_5)x_0^4 \\ & + (9\lambda_1 + \mathtt{D}\lambda_2 + \mathtt{E}\lambda_3 + 7\lambda_4 + 9\lambda_5)x_0^3x_1 \\ & + (\mathtt{D}\lambda_1 + 6\lambda_2 + 0\lambda_3 + 5\lambda_4 + 4\lambda_5)x_0^3x_2 + \ldots \\ = \quad & \Gamma_{01}x_0^3x_1 + \Gamma_{02}x_0^3x_2 + \ldots. \end{aligned}$$

We can now use the cubic identities $\mathcal{B}$ for g to be a rank-2 product polynomial to obtain $\binom{5}{3} \times \binom{5}{3} = 100$ homogeneous cubic equations in $\lambda_1, \ldots, \lambda_5$ (Section 4.2). For example, the coefficients with respect to the lexicographic ordering $\lambda_1^3, \lambda_1^2\lambda_2, \ldots, \lambda_5^3$ of the cubic expression given by $\mathcal{B}_{0,1,2,0,1,2}$ is given below.

```
09CF5757921C325CC9D45345AC71F6C7A21
```

Thus we obtain 100 cubic expressions in the 35 cubic monomials in the variables $\lambda_1, \ldots, \lambda_5$, so we can express this cubic system as using a 100×35 matrix. This matrix has rank 34 and reducing it to echelon form gives the unique (projective) solution

$$(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (5, 2, 9, B, 1)\,.$$

Thus we construct the linear polynomial $g = 5f_1 + 2f_2 + 9f_3 + Bf_4 + 1f_5$, with coefficents given below, which is a rank-2 product polynomial.

```
18DABAA51A9A5379A68200304EB690F755CD63ED76419BCD705A2B95FBB4017D5E6587
```

We can indeed factor this linear combination of $f_1, \ldots, f_5$ to obtain

$$0 = g = (x_0 + Dx_1 + 9x_2 + 5x_3 + Bx_4)^2 \times \textit{Irreducible Quadratic}.$$

A solution over $\mathbb{F}$ therefore satisfies $x_0 + Dx_1 + 9x_2 + 5x_3 + Bx_4 = 0$. We can thus make a substitution to reduce the original problem in five variables to a problem in four variables. We can continue using this techniques on the smaller system to give $(1, E, 4, 6, 7)$ as the unique (projective) solution to the original system. For comparison, calculating this solution using a Gröbner basis or an XL algorithm requires the generation of polynomials of degree 15.

E A Quintic System in Even Characteristic

We use the field $\mathbb{F} \cong \mathrm{GF}(2^4)$ of Appendix B. We consider the solution of the homogeneous quintic system $f_1 = f_2 = f_3 = f_4 = f_5 = 0$ using the method of Section 4.2, where $f_1, \ldots, f_5 \in \mathbb{F}[x_0, x_1, x_2, x_3, x_4]$ satisfy the $\mathcal{LS}$-Criterion (without loss of generality). The coefficients of $f_1, \ldots, f_5$ are given below with respect to the lexicographic ordering $x_0^5, x_0^4 x_1, \ldots, x_4^5$.

```
63DAD00009001040B6DB008048BE3078F167000C00703000000000200C0300
0070103023E90040612D405CC4ED007070000E0B074B30010421B010BD32D7A

0A2B2D000A0060B25D010010178D50FE5700000A00C030000000000F0010D00
006070909CAF0040552CD0EE87A900C030000C060E0F7407869930F0C078736

4BC09900030050E4933F00A0ECE25004F66700010080D0000000000B00B0300
0070A0E1FDC100E07D8A2050625300D0D000090C0251130D947EF030FCF0B16

8A0D52000A00505FD51800B0324DC0200F39000B00909000000000700B0B00
0010F0AB1A4C0070DC90D0B8CBFA00907000040C0E00DD07C0E790F03EFEE84

2416BD00050060FCC4FA00D078973004AFF5000400304000000000200D0900
0010D09EAB24008004FB104FBA2E008050000C070664130C76D58080812CDDF
```

A rank-2 product polynomial in odd degree is an element of the $\mathcal{L}^1\mathcal{S}$-subspace (Definition 4), and we note without loss of generality that $f_1, \ldots, f_5 \in U_2'$, the $\mathcal{L}^1\mathcal{S}$-subspace of W_5.

A linear combination $g = \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3 + \lambda_4 f_4 + \lambda_5 f_5$ is given by

$$\begin{aligned} g = \quad & (6\lambda_1 + 0\lambda_2 + 4\lambda_3 + 8\lambda_4 + 2\lambda_5)x_0^5 \\ & +(3\lambda_1 + \mathtt{A}\lambda_2 + \mathtt{B}\lambda_3 + \mathtt{A}\lambda_4 + 4\lambda_5)x_0^4 x_1 \\ & +(\mathtt{D}\lambda_1 + 2\lambda_2 + \mathtt{C}\lambda_3 + 0\lambda_4 + 1\lambda_5)x_0^4 x_2 + \ldots \\ = \; & \Gamma_{00} x_0^5 + \Gamma_{01} x_0^4 x_1 + \Gamma_{02} x_0^4 x_2 + \ldots . \end{aligned}$$

We can now use the cubic identities $\mathcal{C}$ for g to be a rank-2 product polynomial to obtain $\binom{5}{3} \times \binom{5}{3} = 100$ homogeneous cubic equations in $\lambda_1, \ldots, \lambda_5$ (Section 4.2). For example, the coefficients with respect to the lexicographic ordering $\lambda_1^3, \lambda_1^2\lambda_2, \ldots, \lambda_5^3$ of the cubic expression given by $\mathcal{C}_{0,1,2,0,1,2}$ is given below.

```
16785F34B6C6BAC6AF0B48FA8D2CD5BCADA
```

Thus we obtain 100 cubic expressions in the 35 cubic monomials in the variables $\lambda_1, \ldots, \lambda_5$, so we can express this cubic system as using a 100×35 matrix. This matrix has rank 30 and reducing it to echelon form gives the following relations (amongst others):

$$0 = \lambda_1^2\lambda_5 + \mathtt{A}\lambda_5^3 = \lambda_2^2\lambda_5 + 1\lambda_5^3 = \lambda_3^2\lambda_5 + \mathtt{E}\lambda_5^3 = \lambda_4^2\lambda_5 + 7\lambda_5^3.$$

Thus analysing this equation system quickly shows that the unique (projective) solution is given by

$$(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (\mathtt{F}, 1, \mathtt{D}, 6, 1)\,.$$

Thus we construct the linear polynomial $g = \mathtt{F}f_1 + 1f_2 + \mathtt{D}f_3 + 6f_4 + 1f_5$, with coefficents given below, which is a rank-2 product polynomial.

```
2379C3000C00E0ABD4AA0090F13E608A2B980004005080000000000700D0D00
00F0A01CF25600E0CE1B40FCD25D00202000010F08351B0BE8E8C080A74B9D6
```

This linear combination of $f_1, \ldots, f_5$ factors to give

$$0 = g = (x_0 + 8x_1 + \mathtt{A}x_2 + \mathtt{D}x_3 + 6x_4) \times (\textit{Irreducible Quadratic})^2\,.$$

A solution over $\mathbb{F}$ therefore satisfies $x_0 + 8x_1 + \mathtt{A}x_2 + \mathtt{D}x_3 + 6x_4 = 0$. We can thus make a substitution to reduce the original problem in five variables to a problem in four variables. We can continue using this techniques on the smaller system to give $(1, 4, 4, \mathtt{A}, \mathtt{E})$ as the unique (projective) solution to the original system. For comparison, calculating this solution using a Gröbner basis or an XL algorithm requires the generation of polynomials of degree 20.