*Submitted exclusively to the London Mathematical Society*
doi:10.1112/0000/000000

# Solving the "Isomorphism of Polynomials with Two Secrets" Problem

Submission to ANTS 2014

Abstract

In this paper, we study the Isomorphism of Polynomial (IP) problem with $m = 2$ homogeneous quadratic polynomials of $n$ variables over a finite field of odd characteristic: given two quadratic polynomials $(\boldsymbol{a}, \boldsymbol{b})$ on $n$ variables, we find two bijective linear maps $(s, t)$ such that $\boldsymbol{b} = t \circ \boldsymbol{a} \circ s$. We give an algorithm computing $s$ and $t$ in time complexity $\widetilde{O}(n^4)$ for all instances. This problem was introduced in cryptography by Patarin back in 1996. The special case of this problem when $t$ is the identity is called the isomorphism with one secret (IP1S) problem. Generic algebraic equation solvers (for example using Gröbner bases) solve quite well random instances of the IP1S problem. For the particlar *cyclic* instances of IP1S, a cubic-time algorithm was later given **[13]** and explained in terms of pencils of quadratic forms over all finite fields; in particular, the cyclic IP1S problem in odd characteristic reduces to the computation of the square root of a matrix.

We give here an algorithm solving all cases of the IP1S problem in odd characteristic using two new tools, the Kronecker form for a singular quadratic pencils, and the reduction of bilinear forms over a non-commutative algebra. Finally, we show that the second secret in the IP2S problem may be recovered in cubic time.

## *Introduction*

### *The IP1S and IP2S problems*

The *Isomorphism of Polynomial with Two Secrets* (IP2S) problem is the following. Given a field $k$ and two $m$-uples $\boldsymbol{a} = (a_1, \ldots, a_m)$ and $\boldsymbol{b} = (b_1, \ldots, b_m)$ in $n$ variables $(x_1, \ldots, x_m)$, compute two invertible linear maps $s \in \mathrm{GL}_n(k)$ of the variables $x_i$ and $t \in \mathrm{GL}_m(k)$ of the polynomials $a_i$ such that

$$\boldsymbol{b} = t \circ \boldsymbol{a} \circ s.$$

The particular case where we restrict $t$ to the identity transformation is also known as the *Isomorphism of Polynomials with One Secret* (IP1S). Both these problems have been introduced in cryptography by Patarin in **[16]** to construct an efficient authentication scheme, as an alternative to the Graph Isomorphism Problem (GI) proposed by Goldreich, Micali and Wigderson **[10]**. The IP problem was appealing since it seems more difficult than the Graph Isomorphism problem **[17]**. Agrawal and Saxena reduced **[1]** the Graph Isomorphism problem to the particular case of IP1S using two polynomials, one of them being a quadratic form encoding the adjacency matrix of the graph, and the other one being the cubic $\sum x_i^3$, over a finite field of odd characteristic. For the case of quadratic polynomials, the status of this problem is unclear despite recent intensive research in the cryptographic community since this case is the most interesting for practical schemes. There exists a claimed reduction between the quadratic IP1S problem and the GI problem **[17]**, but we realized that this proof is incomplete. Indeed, the proof works by induction and decompose any permutation as the composition of transpositions. It is possible to write a system of quadratic polynomials such that the only

---

2000 *Mathematics Subject Classification* 15A21,15A22,15A63,11T71.

solutions of the IP1S problem will be the identity or a transposition by modifying a bit the systems proposed in [**17**]. However, it is not obvious how we can compose the systems of equations such that the solutions will be the composition of the solutions.

The defining parameters of the IP problems are the number $n$ of variables, the number $m$ of polynomials, and their degree. For efficiency reasons, the degree is generally small, involving only quadratic and cubic equations. To our knowledge, no significant progress has been done on the cubic case.

We limit ourselves to the special case of two equations, both of which being homogeneous polynomials of degree two. According to previous literature [**18**, **7**, **4**, **6**], this is the most difficult case.

The case with only one homogeneous quadratic equation amounts to reduction of quadratic forms, which has been known for centuries [**9**, **12**]. In the non-homogeneous case, the presence of affine terms gives linear relations between the secret unknowns [**17**], and this extra information actually helps generic solvers, for example those using Gröbner bases, as shown in [**7**]. The case with more than two equations is easier since we can relinearize the systems [**4**].

*Previous work*

Some recent advances have been made on the IP1S problem in the case of two homogeneous quadratic equations.

Bouillaguet, Fouque and Macario-Rat in 2011 [**5**] used pencil of quadratic forms to recover the secret mappings $s$ and $t$ when three equations are available and one of the quadratic equations $\boldsymbol{a}$ comes from a special mapping $X \mapsto X^{q^\theta+1}$ over $\mathbb{F}_q$. In the case of the IP problem, this is optimal using an information theoretic argument.

Macario-Rat, Plût and Gilbert explained in 2013 [**13**] how to solve cyclic instances of the IP1S problem for $m = 2$ over finite fields of any characteristic. A pencil $\boldsymbol{b} = (b_\infty, b_0)$ is *cyclic* if $b_\infty$ is invertible and $b_\infty^{-1} b_0$ is a cyclic matrix, *i.e.* its characteristic polynomial is equal to its minimal polynomial. Although the cyclic case is generic in the geometric sense (*i.e.* defined by the non-cancellation of some polynomial functions of the coefficients of $\boldsymbol{b}$), it is not the general case in a practical sense. In the cyclic instances, Gröbner basis works well [**4**] since in this case, the number of solutions is small. For all other instances, the number of solutions is large, and it is well-known that in this case, such algorithms are less efficient.

Finally, very recently Berthomieu, Faugère and Perret in [**3**] proposed a polynomial algorithm for IP1S with any number of equations when $2 \neq 0$. Given two families of polynomials over a field $k$, they give a solution to the IP1S problem over a tower $k'$ of real quadratic extensions (a *real quadratic extension* being obtained by adjoining the square root of a sum of squares) of $k$. This solves the IP1S problem over the original field $k$ only if $k$ is *Euclidean*, *i.e.* has no real quadratic extension. This is the case for example if $k$ is a closed real field such as $\mathbb{R}$ or the field $\mathbb{R}_{\text{alg}}$ of real algebraic numbers, or an algebraically closed field; since any quadratic extension of a finite field is real, no finite field is Euclidean.

*Our contributions*

This work covers the IP1S and IP2S problems for $m = 2$ equations over a non-binary field, although the complexity estimate depends on computing square roots and thus only applies to finite fields.

We first reduce the general IP1S problem to the *regular case*, which is the case where $b_\infty$ is invertible. This is the object of section 1 of this document and uses the Kronecker classification of pencils of quadratic forms. Although this dates back to Kronecker, the classic proof uses complex analysis; we give a proof over any field where $2 \neq 0$.

We then prove that the regular case of the IP1S problem simplifies to a reduction problem for some quadratic forms over a local algebra. As this is a well-understood theory (in odd characteristic), we are able to give a polynomial-time answer to all instances of IP1S in section 2.

The last section explains how we recover the second ("outer") secret in the two-secret IP2S problem. As applying an outer linear combination to a pencil leaves the singular part of the pencil unchanged (up to isomorphism), we can use the regular part alone to recover the inner secret. This is done using the factorization of the characteristic polynomial.

*Mathematical background and notations*

Throughout this document, $k$ is a field such that $2 \in k^{\times}$. Let $V$ be a $n$-dimensional vector space over the field $k$. We study the IP1S and IP2S problems for *quadratic forms* on $V$, which are homogeneous polynomials of degree 2 in some coordinates on $V$. To a quadratic form $q$, one may associate the *polar form* $b$ defined by

$$b(x, y) = q(x + y) - q(x) - q(y);$$

this is a symmetric bilinear forms, and it satisfies the *polarity identity*

$$b(x, x) = 2q(x).$$

Since $2 \neq 0$ in $k$, the polarity identity is a bijection between quadratic forms and bilinear forms. Therefore, instead of quadratic forms, we shall study directly bilinear forms.

In the case where $2 = 0$ in $k$, the situation is much more complicated; the polarity identity is no longer a bijection, but polar forms are instead alternate bilinear forms. This means that their classification is very different from the odd-characteristic case [**14**], and relies on symplectic groups and Artin-Schreier type equations, *i.e.* of the type $x^2 + x + C = 0$.

Let $V^{\vee}$ be the dual of the vector space $V$. A bilinear form $b$ on $V$ is the same as a linear map $b : V \to V^{\vee}$. The bilinear form is *regular* if it defines an invertible linear map $V \to V^{\vee}$. In this case, to for any endomorphism $u$ of $V$, there exists a unique endomorphism $u^{\star}$ of $V$ such that $b(x, u(y)) = b(u^{\star}(x), y)$; the endomorphism $u^{\star}$ is called the *left-adjoint* of $u$. If $b$ is symmetric then left- and right-adjoints coincide.

An *(affine) pencil of symmetric bilinear forms* over $V$, or a *symmetric pencil* in short, is the data of a pair of symmetric bilinear forms $\boldsymbol{b} = (b_{\infty}, b_0)$ over $V$. We write this pencil in affine form as $b_{\lambda} = -\lambda b_{\infty} + b_0$, and in projective form as $b_{\lambda:\mu} = -\lambda b_{\infty} + \mu b_0$, where $b_0$ and $b_{\infty}$ are symmetric bilinear forms.

Two elements $x$ and $y$ of $V$ are *orthogonal* for a bilinear form $b$ if $b(x, y) = 0$. They are orthogonal for a pencil $(b_{\lambda})$ if, for all $\lambda$, $b_{\lambda}(x, y) = 0$. We write $x \perp_b y$, or $x \perp y$ when the bilinear form or pencil is clear from context. The orthogonal of a sub-space $W \subset V$ is $W^{\perp}$. A space $W$ *self-orthogonal* if $W \subset W^{\perp}$.

We write $R^{m \times n}$ for the vector space of matrices with entries in $R$ having $m$ lines and $n$ columns, and ${}^{\mathrm{t}}A$ for the transpose of a matrix $A$. A *symmetric* matrix is a matrix such that $A = {}^{\mathrm{t}}A$. Symmetric bilinear forms $b$ correspond to symmetric matrices $B$. A bilinear form is regular iff its matrix is invertible. For any endomorphism $u$ with matrix $U$, the adjoint endomorphism (relatively to $B$) has matrix $U^{\star} = B^{-1} \cdot {}^{\mathrm{t}}U \cdot B$. The *companion matrix* of a polynomial $p$ is the matrix of multiplication by $p$ in the basis $\left\{1, x, \ldots, x^{\deg p - 1}\right\}$ of polynomials with degree $< \deg p$.

# 1. *IP1S in the possibly singular case*

## 1.1. *Regular and singular pencils*

Let $b = (b_\lambda)$ be a bilinear pencil over the space $V$. The *characteristic polynomial* of the symmetric pencil $(b_\lambda)$ is either the polynomial $f(\lambda) = \det(\lambda b_\infty + b_0)$, or its homogeneous form $f(\lambda : \mu) = \det(\lambda b_\infty + \mu b_0)$. If $\dim_k V = n$, then $f(\lambda : \mu)$ is homogeneous of degree $n$. The pencil $(b_\lambda)$ is called *regular* if the characteristic polynomial is not zero, and *singular* otherwise. We solve the isomorphism problem for regular pencils in section 2 below.

We reduce to the regular case by proving that the singular part of a symmetric pencil is reducible to the canonical form of Kronecker. This form is described in [**8**, XII(56)]; however, the proof given there only applies to pencils over $\mathbb{C}$, as its uses the computation of square roots of matrices via interpolation on the spectrum. We give here an algorithmic proof that applies to any field $k$ such that $2 \neq 0$.

## 1.2. *Reduction of (possibly singular) pencils to the Kronecker form*

The pencil $(b_\lambda)$ defines a symmetric bilinear form on the module $V_\infty = V \otimes_k k[\lambda]$; if $(b_\lambda)$ is singular, then this form has a non-trivial kernel $W$. Elements of $W$ are called *isotropic* for $(b_\lambda)$. An element $x = x_0 + \lambda x_1 + \ldots + \lambda^h x_h$ is isotropic iff

$$b_0 x_0 = 0, \quad b_0 x_1 = b_\infty x_0, \quad \ldots b_0 x_h = b_\infty x_{h-1}, \quad b_\infty x_h = 0. \tag{1.1}$$

A *minimal isotropic vector* for $(b_\lambda)$ is one with minimal degree $h$; this degree is the *minimal index* of $(b_\lambda)$. If $(b_\lambda)$ is regular, then the minimal index is $+\infty$. By choosing a basis of $W$ adapted to the filtration of $V_\infty$ by the degree of polynomials, we see that $W$ as a basis $(w_1, \ldots, w_r)$ such that, if $h_i$ is the degree of the isotropic vectol $w_i$, then $(w_i, \ldots, w_r)$ generate no isotropic vector of degree $< h_i$. The degree $h_i$ are called the *minimal indices* of the pencil $(b_\lambda)$.

PROPOSITION 1.2. *Let $e = \sum \lambda^i e_i$ be a minimal isotropic vector for $(b_\lambda)$. Then*

(i) *The $h+1$ vectors $e_0, \ldots, e_h$ are $k$-linearly independent.*
(ii) *The $h$ linear forms $b_0 e_1, \ldots, b_0 e_h$ are $k$-linearly independent.*
(iii) *For all $i, j$, $b_0(e_i, e_j) = b_\infty(e_i, e_j) = 0$.*

*Proof.* We first prove (ii). Assume that there exists a non-trivial linear relation $\alpha_1 b_0 e_1 + \ldots + \alpha_h b_0 e_h = 0$ and define vectors $e'_0 \ldots, e'_{h-1}$ by $e'_i = \alpha_{h-i} e_0 + \ldots + \alpha_h e_i$. These vectors satisfy the relations

$$\begin{aligned} b_0 e'_0 &= \alpha_h b_0 e_0 = 0, \\ b_0 e'_i &= \alpha_{h-i+1} b_0 e_1 + \ldots + \alpha_m b_0 e_{i-1} = b_\infty e'_{i-1}, \\ b_\infty e'_{h-1} &= b_\infty(\alpha_1 e_0 + \ldots + \alpha_h e_{h-1}) \\ &= b_0(\alpha_1 e_1 + \ldots + \alpha_h e_h) \\ &= 0. \end{aligned} \tag{1.3}$$

This means that $(e'_0 + \cdots + \lambda^{h-1} e'_{h-1})$ is isotropic and of degree $\leq h-1$ for $b_\lambda$, which contradicts the minimality of $e$.

To prove (i), let $\alpha_0 e_0 + \ldots + \alpha_h e_h = 0$ be a non-trivial linear relation. Then since $\alpha_1 b_0(e_1) + \ldots + \alpha_h b_0(e_h) = 0$, by (ii) we must have $\alpha_1 = \ldots = \alpha_h = 0$, which in turn implies $e_0 = 0$. However, in this case we see that $e_1 + \cdots + \lambda^{h-1} e_h$ is isotropic of degree $\leq h-1$.

We now prove (iii). For all $i, j$, note that we have

$$b_\infty(e_i, e_j) = b_0(e_i, e_{j+1}) = b_0(e_{j+1}, e_i) = b_\infty(e_{j+1}, e_{i-1}) = b_\infty(e_{i-1}, e_{j+1}). \tag{1.4}$$

From this and the fact that $b_\infty(e_i, e_h) = b_\infty(e_h, e_i) = 0$ and $b_0(e_i, e_0) = b_0(e_0, e_i) = 0$, we deduce that for all $0 \le i, j \le h$, we have $b_\infty(e_i, e_j) = b_0(e_i, e_j) = 0$. $\square$

A *Kronecker module* is a vector space $V$ with a symmetric pencil $(b_\lambda)$ such that the coordinates $e_i$ of a minimal isotropic vector $\sum \lambda^i e_i$ span a space $E$ satisfying $E = E^\perp$.

PROPOSITION 1.5. *Let $(b_\lambda)$ be a symmetric pencil with minimal isotropic vector $e = e_0 + \ldots + \lambda^h e_h$. Then $V$ has, as an orthogonal direct factor, a Kronecker module $K_E$ containing the vectors $e_i$.*

*Proof.* Let $E \subset V$ be the sub-space spanned by the vectors $e_i$ and $E^\perp$ be its orthogonal. Prop. 1.2 shows that $\dim E = h+1$, $\dim V/E^\perp = h$, and $E \subset E^\perp$. We show that $E^\perp/E$ is an orthogonal direct factor of $V$; its orthogonal supplement will be the required Kronecker module.

$$\begin{tikzcd}
E \arrow[r] \arrow[d, equal] & E^\perp \arrow[r] \arrow[d] \arrow[l, bend right, dotted, "u"'] & E^\perp/E \arrow[d] \\
E \arrow[r] & V \arrow[r] \arrow[d] & V/E \arrow[d] \\
& V/E^\perp \arrow[r, equal] \arrow[u, dotted, bend left, "v"] & V/E^\perp
\end{tikzcd} \tag{1.6}$$

A split extension $0 \to K_E \to V \to E^\perp/E \to 0$ is given by a retraction $u$ of the injection $E \hookrightarrow E^\perp$ and a section $v$ of the projection $V \to V/E^\perp$; this extension is orthogonal if, for all $x \in E^\perp, y \in V/E^\perp$, $(x - u(x)) \perp v(y)$.

Write $u(x) = \sum u_i(x) e_i$ where $u_0, \ldots, u_h \in (E^\perp)^\vee$ and let the section $v$ be defined by elements $v_1, \ldots, v_h \in V$ such that $b_0(e_i, v_j) = 1$ if $i = j$ and $0$ otherwise. The orthogonality condition then becomes

$$b_0(v_j, x) = u_j(x), \quad b_\infty(v_j, x) = u_{j-1}(x), \qquad \text{for all } x \in E^\perp,\ j = 1, \ldots, h. \tag{1.7}$$

These relations uniquely determine $u_0$ and $u_h$, and solutions $(u_1, \ldots, u_{h-1})$ exist iff the values $v_i$ also satisfy the relations $b_0(v_j, x) = b_\infty(v_{j+1}, x)$ for $j = 1, \ldots, h-1$ and $x \in E^\perp$.

Define a map $\partial_h : (E^\perp)^h \to ((E^\perp)^\vee)^{h-1}$ by

$$\partial_h(v_1, \ldots, v_h) = (b_0(v_1) - b_\infty(v_2), \ldots, b_0(v_h) - b_\infty(v_{h-1})). \tag{1.8}$$

Elements of the cokernel of $\partial_h$ are exactly isotropic vectors of degree $\le h-1$ in $E^\perp$; since $b$ has minimal index $\ge h$, the map $\partial_h$ is surjective. This proves that the map $V^h \to (V/E^\perp)^h \oplus ((E^\perp)^\vee)^{h-1}$ defined by the relations between the $v_j$ is surjective, and therefore that suitable $v_j$ exist. This proves the orthogonality of the decomposition $V = K_E \oplus (E^\perp/E)$. $\square$

Define matrices $K'_h$ of size $(h+1) \times h$ and $K_h$ of size $(2h+1) \times (2h+1)$ by

$$K'_h = \begin{pmatrix} \lambda & & 0 \\ 1 & \ddots & \\ & \ddots & \lambda \\ 0 & & 1 \end{pmatrix}, \quad K_h = \begin{pmatrix} 0 & K'_h \\ {}^{\mathrm{t}}K'_h & 0 \end{pmatrix}. \tag{1.9}$$

PROPOSITION 1.10. *Let $(V, b_\lambda)$ be a Kronecker module with minimal index $h$. There exists a basis of $V$ in which the pencil $(b_\lambda)$ has the matrix $K_h$.*

Note in particular that the case $h = 0$ corresponds to the matrix $K_0$, which is the zero matrix of size $1 \times 1$, and to a vector belonging to all the kernels of $b_\lambda$.

*Proof.* Let $e_0 + \ldots + \lambda^h e_h$ be a minimal isotropic vector for $(b_\lambda)$ and $E$ be the span of the $e_i$; we need to prove that $E$ has a supplement which is self-orthogonal for the pencil $(b_\lambda)$. Such a supplement corresponds to a retraction $w$ of $V \hookrightarrow E$ such that, for all $x, y \in V$, $(x - w(x)) \perp (y - w(y))$, or:

$$b_\lambda(x, y) = b_\lambda(x, w(y)) + b_\lambda(w(x), y) \quad \text{for all } \lambda \text{ and for } x, y \in V. \tag{1.11}$$

A basis of $V/E^\perp$ is given by vectors $f_1, \ldots, f_d \in V$ such that $b_0(e_i, f_j) = 1$ if $i = j$ and $0$ otherwise. Since $E = E^\perp$, the family $e_0, \ldots, e_h; f_1, \ldots, f_h$ is a basis of $V$. Write $w(f_j) = \sum w_{ij} e_i$. The equations (1.11) then amount to

$$w_{i,j} + w_{j,i} = b_0(f_i, f_j); \quad w_{i-1,j} + w_{j-1,i} = b_\infty(f_i, f_j). \tag{1.12}$$

This defines the values $w_{i,i} = \frac{1}{2} b_0(f_i, f_i)$ and $w_{i-1,i} = \frac{1}{2} b_\infty(f_i, f_i)$, which is possible since $2 \in k^\times$. All other values follow from the relation $w_{i,j} - w_{i-1,j+1} = b_0(f_i, f_j) - b_\infty(f_i, f_{j+1})$. $\square$

Define matrices $K'_0, K'_\infty$ of size $(h+1) \times d$ and $K_0, K_\infty$ of size $(2h+1) \times (2h+1)$ by

$$K'_0 = \begin{pmatrix} 0 & & 0 \\ 1 & \ddots & \\ & \ddots & 0 \\ 0 & & 1 \end{pmatrix}, \quad K'_\infty = \begin{pmatrix} 1 & & 0 \\ 0 & \ddots & \\ & \ddots & 1 \\ 0 & & 0 \end{pmatrix}, \qquad K_\lambda = \begin{pmatrix} 0 & K'_\lambda \\ {}^{\mathrm{t}}K'_\lambda & 0 \end{pmatrix}. \tag{1.13}$$

Proposition 1.14. *Let $(b_\lambda)$ be a symmetric pencil with minimal index $h$. There exists a basis of $V$ in which the pencil $(b_\lambda)$ has the matrix*

$$B_\lambda = \begin{pmatrix} K_\lambda & 0 \\ 0 & B'_\lambda \end{pmatrix},$$

*where $B'_\lambda$ is a symmetric pencil with minimal index at least $h$.*

Note in particular that the case $h = 0$ corresponds to the matrix $K_0$, which is the zero matrix of size $1 \times 1$, and to a vector belonging to all the kernels of $b_\lambda$.

*Proof.* Let $(e_0, \ldots, e_h)$ be a minimal isotropic vector. By Prop. 1.2, there exist vectors $f_1, \ldots, f_h$ such that $b_0(e_i, f_j) = 1$ when $i = j$ and $0$ otherwise, and the family $(e_0, \ldots, e_h, f_1, \ldots, f_h)$ is free. For all $i, j$, note that we have

$$b_\infty(e_i, e_j) = b_0(e_i, e_{j+1}) = b_0(e_{j+1}, e_i) = b_\infty(e_{j+1}, e_{i-1}) = b_\infty(e_{i-1}, e_{j+1}). \tag{1.15}$$

From this and the fact that $b_\infty(e_i, e_h) = b_\infty(e_h, e_i)$ and $b_0(e_i, e_0) = b_0(e_0, e_i) = 0$, we deduce that for all $0 \le i, j \le h$, we have $b_\infty(e_i, e_j) = b_0(e_i, e_j) = 0$. Therefore, in any basis completing the family $(e_0, \ldots, e_h; f_1, \ldots, f_h)$, the pencil $(b_\lambda)$ has the symmetric matrix

$$B_\lambda = \begin{pmatrix} 0 & K'_\lambda & 0 \\ {}^{\mathrm{t}}K'_\lambda & A_\lambda & {}^{\mathrm{t}}C_\lambda \\ 0 & C_\lambda & B'_\lambda \end{pmatrix}, \tag{1.16}$$

where the blocks have size $d+1$, $d$ and $n - (2d+1)$. We first prove that we may assume that $C_\lambda = 0$, using a change of coordinates of the form

$$P = \begin{pmatrix} 1 & 0 & X \\ 0 & 1 & 0 \\ 0 & Y & 1 \end{pmatrix}. \tag{1.17}$$

The action of $P$ on the sub-matrix $C_\lambda$ of $B_\lambda$ is given by $C_\lambda \leftarrow C_\lambda + {}^{\mathrm{t}}XK'_\lambda + B_\lambda Y$. Now let $x_0, \ldots, x_h$; $y_1, \ldots, y_h$; $c_1, \ldots, c_h$; $c'_1, \ldots, c'_h$ be the columns of ${}^{\mathrm{t}}X, Y, C_0$ and $C_\infty$. We then have to solve the equations

$$\begin{cases} c'_i + x_i + B'_0 y_i = 0 \\ i = 1, \ldots, h \end{cases} ; \quad \begin{cases} c'_i + x_{i-1} + B'_\infty y_i = 0 \\ i = 1, \ldots, h \end{cases} . \tag{1.18}$$

This uniquely determines the values $x_0$ and $x_h$. The equations for $x_1, \ldots, x_{h-1}$ have solutions iff the values $y_1, \ldots, y_h$ satisfy the relations $B'_0 y_i - B'_\infty y_{i+1} = c'_{i+1} - c_i$ for $i = 1, \ldots, h-1$. This translates into matrix form as

$$\begin{pmatrix} B'_0 & -B'_\infty & & 0 \\ & \ddots & \ddots & \\ 0 & & B'_0 & -B'_\infty \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_h \end{pmatrix} = \begin{pmatrix} c'_2 - c_1 \\ \vdots \\ c'_h - c_{h-1} \end{pmatrix} . \tag{1.19}$$

Let $\mathscr{B}$ be the left-side matrix. Then any element of the kernel of ${}^{\mathrm{t}}\mathscr{B}$ defines an isotropic vector of degree $\leq h-1$ for $(b_\lambda)$ [**8**, XII(10)]. This proves that ${}^{\mathrm{t}}\mathscr{B}$ is injective and hence that $\mathscr{B}$ is surjective. Therefore, equations (1.19) and (1.18) have solutions.

We now prove that we may also assume $A_\lambda = 0$ in (1.16). The action of a coordinate change $Q$ of the form

$$Q = \begin{pmatrix} 1 & Z & \\ & 1 & \\ & & 1 \end{pmatrix} \tag{1.20}$$

on $A_\lambda$ is given by $A_\lambda \leftarrow A_\lambda + {}^{\mathrm{t}}ZK_\lambda + {}^{\mathrm{t}}K_\lambda Z$. Let $Z = (z_{i,j})$, $A_0 = (a_{i,j})$ and $A_\infty = a'_{i,j}$; the equations to solve are then

$$z_{i,j} + z_{j,i} = a_{i,j}, \quad z_{i-1,j} + z_{j-1,i} = a'_{i,j}, \quad \text{for } i, j = 1, \ldots, h. \tag{1.21}$$

Since the matrices $A_0$ and $A_\infty$ are symmetric, only the equations for $i \geq j$ are relevant. We then check that, since $2 \neq 0$ in $k$, this is a regular system of $h(h+1)$ equations in the $h(h+1)$ unknowns $z_{i,j}$. Therefore, there exists a unique solution matrix $Z$. This concludes the proof of Prop. 1.14. □

Note that the Kronecker block $K_\lambda$ of size $2h+1$ has the following intrinsic definition: define $e(x) = \sum x^i e_i$ and $f(y) = \sum y^{i-1} f_i$. Then the bilinear pencil $b_\lambda$ is defined by

$$b_\lambda\left(e(x),\, f(y)\right) \;=\; (x+\lambda)F(xy), \quad \text{where } F(t) = 1 + \ldots + t^{h-1}. \tag{1.22}$$

Proposition 1.23 (Kronecker form). *Let $(b_\lambda)$ be a symmetric pencil on $V$. There exists a basis of $V$ in which the pencil has a block-diagonal matrix with diagonal blocks $(K_{h_1}, \ldots, K_{h_r}, B')$, where $K_h = K_{h,0} + \lambda K_{h,\infty}$ is the square matrix of size $2h+1$ defined by equation (1.13), the integers $h_1 \leq \ldots \leq h_r$ are the minimal indices of $(b_\lambda)$, and $B'$ is the matrix of a regular pencil.*

## 2. *IP1S for regular pencils*

We give here an algorithm for solving the IP1S problem in the case of two regular pencils. Assume that $\boldsymbol{b} = (b_\lambda)$ is regular, and let $f \neq 0$ be its characteristic polynomial. Then, for any $\lambda$ such that $f(\lambda) \neq 0$, the bilinear form $b_\lambda$ is regular.

### 2.1. *Localisation of the IP1S problem*

Lemma 2.1. *Let $\boldsymbol{b}$ be a regular symmetric pencil on the vector space $V$. Let $f(\lambda : \mu) = \det(\lambda b_\infty + \mu b_0)$ be the homogeneous characteristic polynomial of $S$, and let $f = \prod g_i$ be a factorisation of $f$ in mutually coprime factors.*

*Then there exists a unique decomposition $V = \bigoplus V_i$ such that the spaces $V_i$ are pairwise orthogonal for all forms of $\boldsymbol{b}$ and the restriction $S|_{V_i}$ has characteristic polynomial $g_i$.*

*Proof.* Let $V_\infty = \operatorname{Ker} b_\infty$ and $V'$ be the orthogonal of $b_\infty$ relatively to the bilinear form $b_0$. Then the decomposition $V = V' \oplus V_\infty$ is orthogonal for all forms $b_\lambda$; replacing $V$ by $V'$, we may assume that $b_\infty$ is a regular bilinear form. This implies that $b_0$ has an adjoint endomorphism $m = b_\infty^{-1} b_0$ such that $b_0(x, y) = b_\infty(x, ay) = b_\infty(ax, y)$; in particular, all elements of the algebra $k[m]$ are self-adjoint with respect to $b_\infty$.

Let $f(\lambda) = f(\lambda : 1)$ be the affine characteristic polynomial. It is enough to prove the result for the decomposition $f = gh$ where $g, h$ are mutually prime. Let $u, v$ be polynomials such that $ug + vh = 1$ and $x, y \in V$ such that $g(m)(x) = 0$ and $h(m)(y) = 0$; we may then write

$$\begin{aligned} b_\infty(x, y) &= b_\infty(x,\ u(m)g(m)y + v(m)h(m)y) \\ &= b_\infty(u(m)g(m)x, y) \ + \ b_\infty(x, v(m)h(m)y) \\ &= 0. \end{aligned} \tag{2.2}$$

Since $y' = ay$ also verifies $h(m)(y') = 0$, equation (2.2) also proves that $b_0(x, y) = b_\infty(x, y') = 0$, and hence $x, y$ are orthogonal for all forms $b_\lambda$. □

The decomposition of $V$ obtained by applying Lemma 2.1 to the full factorisation of $f$ over $k[x]$ is the *primary decomposition* of the pencil $(b_\lambda)$. The restriction of the pencil to each summand $V_i$ has as its characteristic polynomial a power of a prime polynomial; such a pencil is called *local*.

If two regular pencils $\boldsymbol{b}, \boldsymbol{b}'$ are isomorphic (in the IP1S sense), then they have the same characteristic polynomial, and computing an isomorphism between $\boldsymbol{b}$ and $\boldsymbol{b}'$ is the same as computing it on each factor of the primary decomposition. Therefore, in what follows, we shall assume that both pencils are local.

Note that when $k = \mathbb{F}_q$ is a finite field, it may happen that $\lambda^q \mu - \lambda \mu^q$ divides $f(\lambda : \mu) \neq 0$, so that $f(\lambda) = 0$ for all $\lambda \in \mathbb{P}^1(k)$. In this case, although $(b_\lambda)$ is a regular pencil, all forms $b_\lambda$ are degenerate. However, the decomposition given by Lemma 2.1 still applies, and all the local pencils given by this decomposition contain at least one non-degenerate form, namely $b_0$ on $V_\infty$ and $b_\infty$ in all other cases. Swapping $b_\infty$ and $b_0$ when required, we may assume that all local pencils are *finite*, *i.e.* that $b_\infty$ is a regular bilinear form.

Let $b_\lambda = \lambda b_\infty + b_0$ be a finite pencil. We may use the characteristic endomorphism $m = b_\infty^{-1} b_0$ to write $\boldsymbol{b}$ in the form

$$b_\lambda = b_\infty \ (\lambda + m). \tag{2.3}$$

The image of $\boldsymbol{b}$ by a linear change of variables $s$ is then

$${}^{\mathrm{t}}s \cdot b_\lambda \cdot s = {}^{\mathrm{t}}s \cdot b_\infty \cdot s \ (\lambda + s^{-1} \cdot m \cdot s). \tag{2.4}$$

Let $b'_\lambda = b'_\infty(\lambda + m')$ be a pencil isomorphic to $\boldsymbol{b}$; then there exists a change of variables $t$ such that $t^{-1} \cdot m' \cdot t = m$, and the pencil ${}^{\mathrm{t}}t \cdot b'_\lambda \cdot t$ is of the form $b'_\infty(\lambda + m)$, so that we may assume that $m' = m$. Computing the isomorphism between $b_\lambda$ and $b'_\lambda$ then amounts to computing $s$ such that

$${}^{\mathrm{t}}s \cdot b_\lambda \cdot s = b'_\lambda, \qquad s \cdot m = m \cdot s. \tag{2.5}$$

We define the *symmetrizing space* $\mathscr{S}(m)$ and the *commutant* $\mathscr{C}(m)$ as

$$\begin{aligned} \mathscr{S}(m) &= \{b \text{ symmetric bilinear such that } bm \text{ is symmetric}\}, \\ \mathscr{C}(m) &= \{a \in \operatorname{End} V \text{ such that } am = ma\}. \end{aligned} \tag{2.6}$$

The invertible elements of $\mathscr{C}(m)$ form the *commutant group* $\mathscr{C}(m)^\times$.

PROPOSITION 2.7. *Let $m$ be an endomorphism of $V$.*

(i) *The set $\mathscr{S}(m)$ contains a regular bilinear form.*
(ii) *For any regular bilinear form $t \in \mathscr{S}(m)$ and any endomorphism $a$ of $V$, the bilinear form $ta$ belongs to $\mathscr{S}(m)$ if and only if $a$ is self-adjoint with respect to $t$ and $a \in \mathscr{C}(m)$.*
(iii) *Any finite pencil with characteristic endomorphism $m$ is of the form $b_\lambda = ta(\lambda + m)$ where $a \in \mathscr{C}(m)^\times$.*
(iv) *Let $b_\lambda = ta(\lambda + m)$ be a finite pencil and $s \in \mathscr{C}(m)$. Let $s^\star = t^{-1} \cdot {}^{\mathrm{t}}s \cdot t$ be the adjoint of $s$ relatively to the bilinear form $t$. Then*

$$ {}^{\mathrm{t}}s \cdot b_\lambda \cdot s = t\,(s^\star a s)\,(\lambda + m). \tag{2.8}$$

*Proof.* Point (i) is explicitly proven in Prop. 2.18 below. Assuming that $a$ is self-adjoint with respect to $t$, point (ii) follows from

$$ {}^{\mathrm{t}}(tam) \;=\; {}^{\mathrm{t}}m\,{}^{\mathrm{t}}(ta) \;=\; {}^{\mathrm{t}}m\,ta = tma; \tag{2.9}$$

since $t$ is regular, it is cancellable in the resulting equation $tma = tam$. □

PROPOSITION 2.10. *The congruence problem for finite symmetric pencils is equivalent to the following: given an endomorphism $m$ of $V$ and two invertible self-adjoint matrices $a, a' \in \mathscr{C}(m)$, compute a matrix $x \in \mathscr{C}(m)^\times$ such that $x^\star a x = a'$.*

In the particular case where $m$ is cyclic, the commutant $\mathscr{C}(m)$ is the (commutative) polynomial algebra $k[m]$. In this case, solving the IP1S problem is straightforward [**13**]. The proof given here specializes in the cyclic case to the proof of [**13**]. Namely, if $m$ is cyclic, then Prop. 2.10 amounts to equivalence of 1-dimensional quadratic forms over $k[m]$, which is simply a square root computation.

## 2.2. *The local IP1S problem in matrix form*

Assume that $b_\lambda$ is a finite local pencil with characteristic endomorphism $m$ and characteristic polynomial $p^d$, where $p$ is an irreducible polynomial of degree $e$. Let $M_p$ be the companion matrix of $p$; then $k[M_p]$ is isomorphic to the extension field $K = k[\mu]/(p(\mu))$. For any matrix $A = (a_{i,j})$ of size $u \times v$ with coefficients in $K$, let $A^\flat$ be the ("flattened") matrix of size $eu \times ev$ with blocks of size $e \times e$ given by $a_{i,j}(M_p)$. We have $1^\flat = 1$ and $(AB)^\flat = A^\flat B^\flat$ whenever the product exists. We write $A \mapsto A^\sharp$ for the inverse map where it is defined.

For any integer $u$, let $H_u$ be the companion matrix of the polynomial $x^u$. Then there exists a basis of $V$ in which the matrix $M$ of $m$ is block-diagonal, with diagonal blocks $M_{n_i} = (H_{n_i} + \mu)^\flat$, for integers $n_1 \geq \ldots \geq n_r$.

LEMMA 2.11. *For all integers $u, v$, define a matrix $J_{u,v}$ of size $u \times v$ as*

$$J_{u,v} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \\ 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix} \text{ if } u \geq v, \quad J_{u,v} = \begin{pmatrix} 0 & \dots & 0 & 1 & & 0 \\ \vdots & & \vdots & & \ddots & \\ 0 & \dots & 0 & 0 & & 1 \end{pmatrix} \text{ if } u \leq v. \tag{2.12}$$

(i) *For all integers $u, v$, $H_u J_{u,v} = J_{u,v} H_v$.*
(ii) *The space of all matrices $A$ of size $u \times v$ such that $H_u A = A H_v$ is exactly $k[H_u] J_{u,v}$.*
(iii) *$J_{u,v} J_{v,w} = H_v^d J_{v,w}$ where $d$ is the distance between $v$ and the interval $[u, w]$. In particular, $J_{u,v} J_{v,u} = H_u^{|u-v|}$.*

PROPOSITION 2.13. *Let $M$ be the block-diagonal matrix with diagonal blocks $(H_{n_i} + \mu)^\flat$. The commuting space of $M$ is the space of all matrices $A^\flat$, where $A$ is a block matrix $A = (A_{i,j})$, with $A_{i,j} \in k[H_{n_i}] J_{n_i,n_j} = J_{n_i,n_j} k[H_{n_j}]$.*

According to Prop. 2.13, we may replace all elements $A$ of $\mathscr{C}(M)$ by their images $A^\sharp$ in $\mathscr{C}(M^\sharp)$. We may therefore assume that $e = 1$, which means that $K = k$. In this case, as $\mathscr{C}(M) = \mathscr{C}(M - \mu)$, we may further assume that $\mu = 0$. This means that $M$ is the block-diagonal matrix with diagonal blocks $H_{n_i}$ for integers $n_1 \geq \ldots \geq n_r$.

Let $A \in \mathscr{C}(M)$. Each entry $A_{i,j}$ may be written as a polynomial

$$A_{i,j} = a_{i,j}(H_{n_i}) J_{n_i,n_j} = J_{n_i,n_j} a_{i,j}(H_{n_j}) \tag{2.14}$$

where $a_{i,j}(H) \in k[H]/H^{n_j}$.

We simplify the notation and write $A = (a_{i,j})$ where $a_{i,j} \in k[H]$. We note however that elements of $\mathscr{C}(M)$ do not multiply as matrices with coefficients in $k[H]$, due to the relations of Lemma 2.11. An easy way to perform the computations is given in Prop. 2.15 below.

PROPOSITION 2.15. *Let $R = k[H]/H^{n_1}$. For all $i, j$, let $e_{i,j} = \max(0, n_i - n_j)$. For any matrix $A = (A_{i,j}) \in \mathscr{C}(M)$, where $A_{i,j} = a_{i,j}(H_{n_i}) J_{n_i,n_j}$, define*

$$\psi(A) = (H^{e_{i,j}}\ a_{i,j}(H)) \ \in\ R^{r \times r}. \tag{2.16}$$

*Then $\psi$ is a $k$-algebra morphism from $\mathscr{C}(M)$ to $R^{r\times r}$.*

*Proof.* The matrices of $\mathscr{C}(M)$ multiply according to the relations of Lemma 2.11. We only need to prove that the integers $e_{i,j}$ are an integral of the exponents distance$(n_k, [n_i, n_j])$ of Lemma 2.11:

$$e_{i,k} - e_{i,j} + e_{k,j} = \mathrm{distance}(n_k, [n_i, n_j]). \tag{2.17}$$

This can be verified by checking for all orderings of the triple $(i, j, k)$. $\square$

*The adjunction involution.* We now describe the adjunction involution $A \mapsto A^\star$ of the commuting space $\mathscr{C}(M)$.

PROPOSITION 2.18. *For each integer $u$, write $T_u$ for the anti-identity matrix of size $u$.*
(i) *$T_u$ is invertible and both $T_u$ and $T_u H_u$ are symmetric.*
(ii) ${}^{\mathrm{t}}J_{u,v} T_u = T_v J_{v,u}$.

(iii) *Let $T$ be the block-diagonal matrix with diagonal blocks $T_{n_i}$. Then $T \in \mathscr{S}(M)^\times$.*

PROPOSITION 2.19. *Let $A = (a_{i,j}(H)) \in \mathscr{C}(M)$. Then*

$$A^\star = (a_{ji}(H)).$$

*In particular, $TA$ is symmetric if, and only if, $a_{i,j} = a_{ji}$ in $k[H]/H^{\min(n_i,n_j)}$.*

As a corollary of Prop. 2.15 and 2.19, we get the following. Let $D$ be the diagonal matrix $(H^{n_1-n_i}) \in R^{r\times r}$. For any $A = (a_{i,j} \in \mathscr{C}(M)$, let

$$\varphi(A) = D \cdot \psi(A) = (H^{\max(n_1-n_i,n_1-n_j)} a_{i,j}) \in R^{r\times r}. \tag{2.20}$$

We then have $\varphi(A^\star) = {}^{\mathrm{t}}\varphi(A)$. This implies that, for all $A, X \in \mathscr{C}(M)$:

$$\varphi(X^\star \, A \, X) = {}^{\mathrm{t}}\psi(X) \, \varphi(A) \, \psi(X). \tag{2.21}$$

*Structure of the commutant group.* We show here how to compute in the commutant group $\mathscr{C}(M)^\times$. The main result can be stated in two equivalent ways, as a formula to compute the determinant of elements of $\mathscr{C}(M)^\times$, or as a Gaussian elimination algorithm in the commutant group. For $A \in \mathscr{C}(M)$, we define the *big block* of index $(u, v)$ of $A$ as the submatrix $(a_{i,j})$, where $i, j$ run over the range where $n_i = u$ and $n_j = v$. Prop. 2.23 states that $A$ is invertible if and only if all its diagonal big blocks are invertible as matrices with coefficients in $k[H]/H^{n_i}$.

LEMMA 2.22. *Let $s$ be such that $n_1 = \ldots = n_s > n_{s+1}$. Define $n'_i = n_i - 1$ if $i \le s$, and $n'_i = n_i$ if $i > s$.*

*For any matrix $A \in \mathscr{C}(M)$ given by the block decomposition $A = (a_{i,j}(H_{n_i})J_{n_i,n_j})$, define $A'$ as the square matrix of size $n - s$ given by the blocks $(a_{i,j}(H_{n'_i})J_{n'_i,n'_j})$. Then*

$$\det A \;=\; \det(a_{i,j}(0))_{1\le i,j\le s} \cdot \det A'.$$

*Proof.* Let $\sigma$ the unique permutation of $[1, n]$ such that $\sigma(n_i) = i$ for $i = 1, \ldots, s$, and $\sigma$ is increasing on all other indices. Then the matrix $A^\sigma$ deduced from $A$ by applying $\sigma$ both on the lines and the columns of $A$ is lower block-triangular, with two diagonal blocks respectively equal to the matrix $(a_{i,j}(0))_{i,j\le s}$ and to $A'$. Since $\det A = \det A^\sigma$, this proves the lemma. □

PROPOSITION 2.23. *Let $A = (a_{i,j}(H)) \in \mathscr{C}(M)$. Then*

$$\det A \;=\; \prod_{d\ge 1} \det(a_{i,j}(0) | n_i = n_j = d)^d$$

*where $a_{i,j}(0)$ is the image modulo $H$ of $a_{i,j} \in k[H]$.*

*Proof.* By induction on $n_1$, with Lemma 2.22 providing the induction step. The base case $n_1 = 1$ corresponds to $k[H] = k$ and therefore $A = (a_{i,j}(0))$. □

PROPOSITION 2.24. *The commutant group $\mathscr{C}(M)^\times$ is generated by the following matrices:*

(i) *big-block-diagonal matrices, i.e. matrices whose only non-zero big blocks are those on the diagonal;*

(ii) *small-block transvection matrices.*

*Proof.* By Prop. 2.23, an invertible matrix $A \in \mathscr{C}(M)$ has all its diagonal big blocks invertible. Therefore we may apply the Gaussian elimination algorithm to factor $A$ as a product $A = LU$, where $L$ is lower triangular with diagonal elements 1, and $U$ is upper triangular. □

### 2.3. *Classification of local symmetric pencils*

We shall need the following classic result about bilinear forms over local algebras.

PROPOSITION 2.25. *Let $R$ be a local ring with residue field $k$ and let $\{\delta_i\}$ be a set of representatives for $k^\times$ modulo squares. Then any regular symmetric matrix with entries in $R$ is congruent over $R$ to a diagonal matrix $(1, \dots, 1, \delta_i)$ for some $i$.*

*Proof.* The Gram orthogonalization algorithm works; cf. [**14**, I(3.4)] or [**15**, 92:1]. □

In the present case, since $k$ is a finite field, we have $k^\times/(k^\times)^2 = \{1, \delta\}$ for some element $\delta$.

PROPOSITION 2.26. *Let $A$ be an invertible, self-adjoint element of $\mathscr{C}(M)$. Then there exists $X \in \mathscr{C}(M)^\times$ such that $X^* A X$ is big-block-diagonal.*

*Proof.* We prove this by induction on the number of big blocks of $A$, using Gram orthogonalization on the big blocks of $A$. Let $B$ be the first diagonal big block of $A$. We may then write $A$ as a block matrix

$$A = \begin{pmatrix} B & C \\ {}^{\mathrm{t}}C & A' \end{pmatrix}, B \in R^{d \times d}. \tag{2.27}$$

Since $A$ is invertible, all its diagonal big blocks are invertible; in particular the matrices $B$ and $A'$ are invertible. By the induction hypothesis, there exists $X'$ such that $\Delta = (X')^* A' X'$ is big-block diagonal.

We then define

$$X = \begin{pmatrix} 1 & -B^{-1}C \\ 0 & X' \end{pmatrix} \quad \text{and see that} \quad X^\star A X = \begin{pmatrix} B & 0 \\ 0 & \Delta \end{pmatrix}. \tag{2.28}$$

□

We note that the regularity hypothesis on $A$ is essential for Prop. 2.26. As a counter-example, assume that the Jordan sequence is $n_1 > n_2$ with $n_2 \geq 2$, and let $A = \begin{pmatrix} H_{n_1} & J_{n_1,n_2} \\ J_{n_2,n_1} & H_{n_2} \end{pmatrix} = \begin{pmatrix} H & 1 \\ 1 & H \end{pmatrix}$. Then, using the notations from (2.21), no matrix of the form $\psi(X) = \begin{pmatrix} x_1 & Hx_2 \\ x_3 & x_4 \end{pmatrix}$ diagonalizes $\varphi(A) = \begin{pmatrix} H & H \\ H & H^2 \end{pmatrix}$ in $R^{2\times 2}$, and therefore $A$ is not not big-block diagonalizable by a matrix commuting with $M$.

PROPOSITION 2.29. *Let $A$ be an invertible, self-adjoint element of $\mathscr{C}(M)$. Then $A$ is congruent to a diagonal matrix, where each diagonal big block is either the identity matrix, or the diagonal matrix $(1, \dots, 1, \delta)$.*

*Proof.* Use propositions 2.26 and 2.25. □

2.4. *Solving the general case of IP1S*

THEOREM 2.30. *Let $k$ be a finite field of characteristic $\neq 2$ and $(b_\lambda)$ be a pencil of $n$-dimensional symmetric bilinear forms over $k$. It is possible, using no more than $\widetilde{O}(hn^3) \leq \widetilde{O}(n^4)$ operations in $k$, where $h \leq n$ is the largest of the minimal indices of $(b_\lambda)$, to compute an isomorphism between $(b_\lambda)$ and a (unique) block-diagonal pencil with diagonal blocks of the following form:*

(i) Kronecker blocks $K_h = \begin{pmatrix} 0 & K'_h \\ {}^{t}K'_h & 0 \end{pmatrix}$ *for integers $h \geq 0$, as defined in Prop. 1.23;*

(ii) finite local blocks $L_{p,d,u}$, *defined as the $d \times d$-block matrix*

$$L_{p,d,u} = \begin{pmatrix} 0 & & & T_p u(\lambda + M_p) \\ & & \cdot^{\cdot^{\cdot}} & T_p u \\ & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \\ T_p u(\lambda + M_p) & T_p u & & 0 \end{pmatrix},$$

*where $p$ is an irreducible polynomial, $M_p$ is the companion matrix of $p$, $T_p$ is a prescribed invertible matrix such that both $T_p$ and $T_pM_p$ are symmetric, $d$ is an integer, and $u$ is either the identity matrix or a prescribed non-square element of the field $k[M_p]$, with the extra condition that for fixed $(p, d)$, at most one of the values $u$ may be different from 1;*

(iii) infinite local blocks $L_{1,d,u}$, *defined as the $d \times d$-matrix*

$$L_{1,d,u} = u \begin{pmatrix} 0 & & & 1 \\ & & \cdot^{\cdot^{\cdot}} & \lambda \\ & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \\ 1 & \lambda & & 0 \end{pmatrix},$$

*where $d$ is an integer, $u$ is either 1 or a prescribed non-square element of $k$, and for fixed $d$, at most one of the values $u$ may be different from 1.*

The only place where the finiteness of $k$ is required for this theorem to hold is for the computation of square roots, needed for Prop. 2.25. This theorem solves the IP1S problem in cubic time: given two pencils $\boldsymbol{a}$ and $\boldsymbol{b}$, we only have to transform both of them to the canonical form above. This form will be the same iff the two pencils are isomorphic in the IP1S sense, and in this case, composing the two transformations gives an answer to the computational IP1S problem.

*Algorithm and Complexity.* The algorithm of Theorem 2.30 for a pencil $\boldsymbol{b}$ decomposes in the three following steps.

(i) Compute the Kronecker decomposition: as long as the kernel of the matrix $b_\lambda$ is not trivial, compute a minimal isotropic vector $e = \sum \lambda^i e_i$ and the according Kronecker block according to the linear algebra described in Prop. 1.14.

(ii) Now $\boldsymbol{b}$ is regular. Compute and factor its characteristic polynomial $f(\lambda)$ and split $V$ as a orthogonal direct sum of primary components $V_p$ for each prime divisor $p$.

(iii) For each prime divisor $p$, write the local pencil $\boldsymbol{b}_p$ at $p$ as a matrix with entries in $K = k[\mu]/p(\mu)$. Perform big-block reduction to write $\boldsymbol{b}_p$ as a orthogonal direct sum of quadratic forms over $K[H]/H^{n_i}$, and then reduce each of these forms to one of the two canonical diagonal forms.

Most of the linear algebra steps, including computing the Frobenius rational normal form of the regular part of the pencil, may be done in $\widetilde{O}(n^3)$ field operations [**11**]. In particular, the Frobenius rational normal form covers the factoring of the characteristic polynomial. This may also be done, again in cubic time, using a dedicated factoring algorithm. The reduction of quadratic forms over the local algebras is just the reduction over the residual field (which uses a square root computation in said finite field), followed by a Hensel lift.

The only part not covered by classic algorithms is the reduction to Kronecker normal form performed in Step (1). The computation of a minimal isotropic vector $e = \sum \lambda^i e_i$ amounts to a kernel computation over the polynomial ring $k[\lambda]$. This requires handling polynomials of degree up to the minimal index $h_1$ of $(b_\lambda)$ and therefore has complexity $\widetilde{O}(h_1 n^3)$. As this is performed for all minimal indices $h_i$, the total complexity is $\widetilde{O}(n^4)$.

There exist cubic algorithms computing the Kronecker kernel of pencils of linear maps over a characteristic zero field [**2**]. These algorithms are not directly applicable over a finite field as they use some rotations over the real numbers and are mostly concerned with numerical stability; more importantly, they work with linear maps up to equivalence, whereas we need quadratic forms up to congruence. However, as the corresponding problem over a finite field has not been much studied, the existence of a faster algorithm for computing the Kronecker kernel is not unlikely.

*Decisional IP1S and extensions of scalars.* The solution of IP1S over an extension field in [**3**] raises the following question: given two pencils $\boldsymbol{a}$, $\boldsymbol{b}$ which are IP1S-equivalent over an extension $k'$ of the field $k$, are they always equivalent over the field $k$?

The structure given by theorem 2.30 gives an easy answer to this question. As the Kronecker blocks are invariant by extension of scalars, the problem reduces to the finite and infinite local blocks $L_{p,d,u}$. For an irreducible polynomial $p$, we have

$$L_{p,d,u} \otimes_k k' = \begin{cases} L_{p,d,u'}, & \text{if } p \text{ is irreducible over } k'; \\ \bigoplus L_{X-\mu,d,u'}, & \text{if } p \text{ splits as } \prod_\mu (X-\mu) \text{ over } k', \end{cases} \tag{2.31}$$

where $u'$ is the image in $k'^\times/(k'^\times)^2$ of $u$. The map $k^\times/(k^\times)^2 \to k'^\times/(k'^\times)^2$ is bijective when $[k' : k]$ is odd and zero when it is even. From this we deduce:

PROPOSITION 2.32. *Let $\boldsymbol{a}, \boldsymbol{b}$ be two pencils which are IP1S-equivalent over a field extension $k'$ of the finite field $k$.*

(i) *If the degree $[k' : k]$ is odd, then $\boldsymbol{a}$ and $\boldsymbol{b}$ are equivalent over $k$.*
(ii) *If the degree $[k' : k]$ is even, them $\boldsymbol{a}$ and $\boldsymbol{b}$ are equivalent over $k$ iff, for all local factors $L_{p,d,u}$, they have the same value $u(p,d) \in k^\times/(k^\times)^2$.*

In particular, when $k \to k'$ is a quadratic tower, solving the IP1S problem over $k'$ does not solve the decisional form of IP1S over $k$.

## 3. *Computation of the second secret for IP2S*

### 3.1. *Reduction to the regular case*

Two families of polynomials $(a_1, \dots, a_m)$ and $(b_1, \dots, b_m)$ are *isomorphic with two secrets* if there exist bijective linear transformations $s$ of the $n$ variables and $t$ of the $m$ polynomials such that $t \circ \boldsymbol{a} \circ s = \boldsymbol{b}$. Assume that $m = 2$. Then the second secret $t$ is a homography in two variables, which we write $\gamma \in \mathrm{GL}_2(k)$.

PROPOSITION 3.1. *Two pencils $\boldsymbol{a} = (a_\lambda)$ and $\boldsymbol{b} = (b_\lambda)$ are isomorphic with two secrets if, and only if, the regular parts of both pencils are isomorphic with two secrets.*

*Proof.* The minimal index of the pencil $\boldsymbol{b}$ is the minimal degree of an isotropic vector $e_0 + \ldots + \lambda^h e_h$ for $b_\lambda$; such a vector may be written in homogeneous form in $(\lambda : \mu)$ as $e(\lambda : \mu) = \sum \lambda^i \mu^{h-i} e_i$, which is isotropic for the quadratic form $b(\lambda : \mu) = \mu b_0 + \lambda b_\infty$. Now let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$ be a homography. Then the vector $e^\gamma$ defined by $e^\gamma(\lambda : \mu) = e(a\lambda + b\mu : c\lambda + d\mu)$ is isotropic for $b_{\gamma(\lambda)}$ iff $e$ is isotropic for $b$. This proves that the pencils $(b_{\gamma(\lambda)})$ and $(b_\lambda)$ have the same minimal index. Therefore, all their Kronecker blocks coincide. □

### 3.2. *IP2S in the regular case*

Let $(a_\lambda)$ and $(b_\lambda)$ be two *regular* pencils of bilinear forms such that $a_{\gamma(\lambda)}$ is isomorphic, in the IP1S sense, to $b_\lambda$. Then the homography $\gamma$ maps the characteristic polynomial $f(\lambda) = \det(a_\lambda)$ to $g(\lambda) = \det(b_\lambda)$. In particular, it maps the prime factors of $f$ to those of $g$, respecting both their degree and their exponent as a factor of the characteristic polynomial.

Let $S_{d,e}$ and $T_{d,e}$ be the set of factors of degree $d$ and exponent $e$ of the polynomials $f$ and $g$. Then any homography $\gamma$ mapping all the elements of $S_{d,e}$ to $T_{d,e}$ for each pair $(d, e)$ is a possible second secret in the IP2S problem. We compute the intersection for $(d, e)$ of the set $\Gamma_{d,e}$ of homographies mapping the prime polynomials of $S_{d,e}$ to $T_{d,e}$. In most cases, the first set $\Gamma_{d,e}$ already contains only one candidate, which is therefore the second secret $\gamma$. The discussion depends on the degree $d$ of the polynomials. We note that the sum of the size of the sets $S_{d,e}$ is the number of variables $n$; therefore, we may use the worst-case estimate $|S_{d,e}| = O(n)$ for each $(d, e)$.

We shall use the following classic results.

Proposition 3.2.

(i) *Let $(x_1, x_2, x_3)$ and $(y_1, y_2, y_3)$ be two (ordered) triples of distinct points of $\mathbb{P}^1(k)$. There exists a unique homography $\gamma \in \mathrm{PGL}_2(k)$ such that $\gamma(x_i) = y_i$.*

(ii) *Let $(x_1, x_2, x_3, x_4)$ and $(y_1, y_2, y_3, y_4)$ be two (ordered) quadruplets of distinct points. They are homographic iff they have the same cross-ratio $B(x) = B(y)$, where*

$$B(x) = \frac{(x_1 - x_3)(x_2 - x_4)}{(x_1 - x_4)(x_2 - x_3)}. \tag{3.3}$$

(iii) *Let $\{x_1, x_2, x_3, x_4\}$ and $\{y_1, y_2, y_3, y_4\}$ be two (unordered) sets of four points. They are homographic iff they have the same $j$-invariant $j(x) = j(y)$, where*

$$j(x) = \frac{(B(x)^2 - B(x) + 1)^3}{B(x)^2(1 - B(x))^2}. \tag{3.4}$$

(iv) *Let $u(x) = \sum u_i x^i$ and $v(x)$ be two monic polynomials of degree four. They are homographic iff they have the same $j$-invariant, where $j(u)$ is a polynomial of degree 6 in the coefficients of $u$.*

We note that the formula for the $j$-invariant given in (3.4) is, up to a constant factor, the formula for the $j$-invariant of an elliptic curve. Namely, two elliptic curves with equations $y^2 = f(x)$ and $y^2 = g(x)$, where $f, g$ are separable polynomials of degree $\leq 4$, are isomorphic iff the polynomials $f$ and $g$ are homographic.

We now explain how we compute the set $\Gamma_{d,e}$ for each pair $(d, e)$.

*Case $d = 1$.* If $|S_{1,e}| \geq 3$, then we may immediately recover the homography $\gamma$: namely, fix a triple $(x_1, x_2, x_3)$ in $S_{1,e}$, and iterate over the triples in $T_{1,e}$. For each such triple, there exists a unique homography $\gamma$ such that $\gamma(x_i) = y_i$. This homography belongs to $H_{1,e}$ iff the images of all the other points of $S_{1,e}$ belong to $T_{1,e}$. Since there are $3!\binom{|S_{1,e}|}{3} = O(n^3)$ triples $(y_i)$, this computation requires $O(n^3)$ field operations.

If $1 \le |S_{1,e}| \le 2$, then $H_{1,e}$ may be explicitly computed as the union of the set of homographies mapping the elements of $S_{1,e}$ to those of $T_{1,e}$ for all permutations of $T_{1,e}$.

*Case* $d = 2$. Assume $|S_{2,e}| \ge 2$. Let $u_1, u_2 \in S_{2,e}$ and $v_1, v_2 \in T_{2,e}$ be monic polynomials of degree two. Any homography between the sets $\{u_1, u_2\}$ and $\{v_1, v_2\}$ will map $u_1 u_2$ to $v_1 v_2$. By Prop. 3.2(iv), there exists at most a bounded number of such homographies. Since there are $\binom{|S_{2,e}|}{2} = O(n^2)$ pairs $(v_1, v_2)$, this requires $O(n^2)$ field operations.

If $|S_{2,e}| = 1$, then $H_{2,e}$ is the set of all homographies mapping the unique element of $S_{2,e}$ to the unique element of $T_{2,e}$.

*Case* $d = 3$. Fix an element $u \in S_{3,e}$. For all $v \in T_{3,e}$, there exist at most $3! = 6$ homographies $\gamma$ mapping $u$ to $v$. Each candidate belongs to $H_{3,e}$ iff it maps all other elements of $S_{3,e}$ to elements of $T_{3,e}$. There are $|S_{3,e}| = O(n)$ candidates $u$ and therefore $O(n)$ candidate homographies $\gamma$.

*Case* $d = 4$. Fix an element $u \in S_{4,e}$. The candidates as homographic images of $u$ in $T_{4,e}$ are the $v$ such that $j(v) = j(u)$. Each candidate polynomial $v$ gives at most $4! = 24$ candidates homographies $\gamma$. This allows to compute $H_{4,e}$ in $O(n)$ field operations.

*Case* $d \ge 5$. The naïve method is to differentiate $(d-4)$ times the elements of $S_{d,e}$ to reduce to the case where $d = 4$. However, as this uses only the five leading coefficients, if the polynomials are specially chosen we may find too many homographies; for example, although the polynomials $x^d - 1$ and $x^d$ are not homographic, all their derivatives are. Instead, we first compose all the elements of $S_{d,e}$ and $T_{d,e}$ by a known, randomly chosen homography $r$. In general, for any two non-homographic elements $u_1, u_2 \in S_{d,e}$, the derivatives $(\partial/\partial x)^4 (u_i \circ r)$ are non-homographic. In the improbable case where they are homographic, we only need to change the random homography $r$. In this way, we may compute the set $\Gamma_{d,e}$ in at most $O(n)$ field operations.

*Computing the hidden homography.* The hidden homography $\gamma$ lies in the intersection of all sets $\Gamma_{d,e}$. As each one of these sets is likely to be extremely small or even reduced to $\{\gamma\}$, we compute them in increasing order of assumed complexity. We use the above estimates: for each $(d, e)$, we use the assumed complexity

$$C_{d,e} = \begin{cases} |S_{d,e}|^3, & d = 1; \\ |S_{d,e}|^2, & d = 2; \\ |S_{d,e}|, & d \ge 3, \end{cases} \tag{3.5}$$

and sort the pairs $(d, e)$ by increasing values of $C_{d,e}$. We finally find a bounded number of candidate homographies using no more than $O(n^3)$ operations in $k$.

## *Conclusion*

In this paper, we show that we can solve in polynomial-time the IP problem with two quadratic forms in a finite field of odd characteristic. The obvious questions are whether it is possible to generalize this to fields of characteristic two and to more than two equations.

The case of a binary base field is very important for cryptographical applications. The cyclic case was solved in **[13]**. To solve the general case, at least two roadblocks remain: quadratic forms over a local algebra behave differently [**15**, §93]; finally, extending from bilinear to quadratic forms requires a study of the action of a symplectic group on the diagonal coefficients, and this group becomes quite impractical in the non-cyclic case. We note however that the Kronecker decomposition works, with minimal changes in the proof, when $2 = 0$: namely, solving (1.12) is still possible, as in this case the polar form $b_\lambda$ is an *alternate* symmetric form.

On the other hand, studying the general problem with $m \geq 3$ quadratic equations departs from the classic results about pencils of quadratic forms; therefore, less tools are available. Even in the regular case, our work heavily uses the factorization of the characteristic polynomial. An analogous strategy for $m \geq 3$ would require working in homogeneous polynomials in $m$ variables and doing some serious algebraic geometry.

## *References*


**1.** Manindra Agrawal and Nitin Saxena. Equivalence of F-algebras and cubic forms. In Bruno Durand and Wolfgang Thomas, editors, *STACS*, volume 3884 of *Lecture Notes in Computer Science*, pages 115–126. Springer, 2006.

**2.** Th Beelen and Paul Van Dooren. An improved algorithm for the computation of Kronecker's canonical form of a singular pencil. *Linear Algebra and its Applications*, 105:9–65, 1988.

**3.** Jérémy Berthomieu, Jean-Charles Faugère, and Ludovic Perret. Polynomial-time algorithms for quadratic isomorphism of polynomials. *CoRR*, abs/1307.4974, 2013.

**4.** Charles Bouillaguet, Jean-Charles Faugère, Pierre-Alain Fouque, and Ludovic Perret. Practical Cryptanalysis of the Identification Scheme Based on the Isomorphism of Polynomial with One Secret Problem. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *Public Key Cryptography*, volume 6571 of *Lecture Notes in Computer Science*, pages 473–493. Springer, 2011.

**5.** Charles Bouillaguet, Pierre-Alain Fouque, and Gilles Macario-Rat. Practical key-recovery for all possible parameters of SFLASH. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT*, volume 7073 of *Lecture Notes in Computer Science*, pages 667–685. Springer, 2011.

**6.** Charles Bouillaguet, Pierre-Alain Fouque, and Amandine Véber. Graph-Theoretic Algorithms for the "Isomorphism of Polynomials" Problem. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT*, volume 7881 of *Lecture Notes in Computer Science*, pages 211–227. Springer, 2013.

**7.** Jean-Charles Faugère and Ludovic Perret. Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects. In Serge Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 30–47. Springer, 2006.

**8.** F.R. Gantmacher. *Theory of Matrices*, volume 2. Chelsea, New York, 1960.

**9.** Carl Friedrich Gauss. *Disquisitiones Arithmaticae*. 1801.

**10.** Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. *J. ACM*, 38(3):691–729, 1991.

**11.** Erich L. Kaltofen and Arne Storjohann. The complexity of computational problems in exact linear algebra. In Björn Engquist, editor, *Encyclopedia of Applied and Computational Mathematics*. Springer, 2011.

**12.** R. Lidl and H. Niederreiter. *Finite Fields*. Number vol. 20,ptie. 1 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.

**13.** Gilles Macario-Rat, Jérôme Plût, and Henri Gilbert. New Insight into the Isomorphism of Polynomial Problem IP1S and Its Use in Cryptography. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT (1)*, volume 8269 of *Lecture Notes in Computer Science*, pages 117–133. Springer, 2013.

**14.** John W. Milnor and Dale Husemoller. *Symmetric bilinear forms*. Springer, Berlin, Heidelberg, Paris, 1973.

**15.** Timothy O'Meara. *Introduction to quadratic forms*. Classics in mathematics. Springer, Berlin, Heidelberg, Paris, 2000. Reprint of the 1973 edition.

**16.** Jacques Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In Ueli M. Maurer, editor, *EUROCRYPT*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 1996.

**17.** Jacques Patarin, Louis Goubin, and Nicolas Courtois. Improved algorithms for isomorphisms of polynomials. In Kaisa Nyberg, editor, *EUROCRYPT*, volume 1403 of *Lecture Notes in Computer Science*, pages 184–200. Springer, 1998.

**18.** Ludovic Perret. A Fast Cryptanalysis of the Isomorphism of Polynomials with One Secret Problem. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 354–370. Springer, 2005.