# Polynomial-Time Algorithms for Quadratic Isomorphism of Polynomials: The Regular Case

Jérémy Berthomieu, Jean-Charles Faugère, Ludovic Perret

# POLYNOMIAL-TIME ALGORITHMS FOR QUADRATIC ISOMORPHISM OF POLYNOMIALS

JÉRÉMY BERTHOMIEU AND JEAN-CHARLES FAUGÈRE AND LUDOVIC PERRET

INRIA, *Paris-Rocquencourt Center,* POLSYS *Project*
UPMC, *Univ Paris 06,* LIP6
CNRS, UMR 7606, LIP6

ABSTRACT. Let $\mathbb{K}$ be a field, $\mathbf{f} = (f_1, \ldots, f_m)$ and $\mathbf{g} = (g_1, \ldots, g_m)$ be two sets of $m \geqslant 1$ non-linear polynomials over $\mathbb{K}[x_1, \ldots, x_n]$. We consider the computational problem of finding – if any – an invertible transformation on the variables mapping $\mathbf{f}$ to $\mathbf{g}$. The corresponding equivalence problem is known as *Isomorphism of Polynomials with one Secret* (`IP1S`) and is a fundamental problem in multivariate cryptography; the problem is also called `PolyProj` when $m = 1$. Agrawal and Saxena show that Graph Isomorphism (`GI`) reduces to equivalence of cubic polynomials with respect to an invertible linear change of variables. This strongly suggests that solving equivalence problems efficiently, *i.e.* in polynomial-time, is a very challenging algorithmic task. Then, following Kayal at SODA'11, we search for large families of polynomials equivalence which can be solved efficiently. The main result is a randomized polynomial-time algorithm for solving `IP1S` for quadratic instances, a particular case of importance in cryptography and somewhat justifying *a posteriori* the fact that `GI` reduces to only cubic instances of `IP1S`. To this end, we show that `IP1S` for quadratic polynomials can be reduced to a variant of the classical module isomorphism problem in representation theory, which involves to test the orthogonal simultaneous conjugacy of symmetric matrices. We show that we can essentially *linearize* the problem by reducing quadratic-`IP1S` to test the orthogonal simultaneous similarity of symmetric matrices; this latter problem was shown by Chistov, Ivanyos and Karpinski to be equivalent of finding an invertible matrix in the linear space $\mathbb{K}^{n\times n}$ of $n \times n$ matrices over $\mathbb{K}$ and to compute the square root in a matrix algebra. While computing square roots of matrices can be be done efficiently using numerical methods, it seems difficult to control the bit complexity of such methods. However, we present exact and polynomial-time algorithms for computing the square root in $\mathbb{K}^{n\times n}$ for various fields (including finite fields). We then consider `#IP1S`, the counting version of `IP1S` for quadratic instances. In particular, we provide a (complete) characterization of the automorphism group of homogeneous quadratic polynomials. Finally, we also consider the more general *Isomorphism of Polynomials* (`IP`) problem where we allow an invertible linear transformation on the variables *and* on the set of polynomials. A randomized polynomial-time algorithm for solving `IP` when $\mathbf{f} = (x_1^d, \ldots, x_n^d)$ is presented. From an algorithmic point of view, the problem boils down to factoring the determinant of a linear matrix (*i.e.* a matrix whose components are linear polynomials). This extends to `IP` a result of Kayal obtained for `PolyProj`.

## 1. INTRODUCTION

A fundamental question in computer science is to provide algorithms allowing to test if two given objects are *equivalent* with respect to some transformation. In this paper, we consider equivalence of non-linear polynomials in several variables. Equivalence of polynomials has profound connections with a rich varieties of fundamental problem in computer science, ranging – among others topics – from cryptography (*e.g.* [Pat96a, Pat96b, TX12, TX13, YTY11]), arithmetic complexity (*via* Geometric

*E-mail address*: jeremy.berthomieu@lip6.fr, jean-charles.faugere@inria.fr, ludovic.perret@lip6.fr.

Complexity Theory (GCT) for instance, *e.g.* [Bür12, Kay12, Mul12, MS01]), testing low degree affine-invariant properties [BFL13, GT09, GWX13]). As we will see, the notion of equivalence can come with different flavours that impact the intrinsic hardness of problem considered.

Agrawal and Saxena show in [AS06, Sax06] that Graph Isomorphism reduces to equivalence of cubic polynomials with respect to an invertible linear change of variables (a similar reduction holds between $\mathbb{F}$-algebra Isomorphism and cubic equivalence of polynomials). This strongly suggests that solving equivalence problems efficiently is a very challenging algorithmic task.

In cryptography, the hardness of deciding equivalence between two sets of $m$ polynomials with respect to an invertible linear change of variables is the security core of several cryptographic schemes: the seminal zero-knowledge ID scheme of Patarin [Pat96a, Pat96b], and more recently group/proxy signature schemes [TX12, TX13, YTY11]. Note that there is subtle difference between the equivalence problem considered in [Kay11, AS06, Sax06] and the one considered in cryptographic applications. Whilst [Kay11, AS06, Sax06] restrict their attention to $m = 1$, arbitrary $m \geq 1$ is usually considered in cryptographic applications. In the first case, the problem is called *Polynomial Equivalence* (`PolyEquiv`), whereas it is called *Isomorphism of Polynomials with One Secret* (`IP1S`) problem in the former case. We emphasize that the hardness of equivalence can drastically varies in function of $m$. An interesting example is the case of quadratic forms. The problem is completely solved when $m = 1$, but no polynomial-time algorithm exists for deciding simultaneous equivalence of quadratic forms. In this paper, we close this gap by presenting a randomized polynomial-time algorithm for solving simultaneous equivalence of quadratic forms for various fields.

Equivalence of multivariate polynomials is also a fundamental problem in Multivariate Public-Key Cryptography (`MPKC`). This is a family of asymmetric (encryption and signature) schemes whose public-key is given by a set of $m$ multivariate equations [MI88, Pat96a]. To minimize the public-key storage, the multivariate polynomials considered are usually quadratics. The basic idea of `MPKC` is to construct a public-key which is equivalent to a set of quadratic multivariate polynomials with a specific structure [WP05, WP11]. Remark that the notion of equivalence considered in this context is more general than the one considered for `PolyEquiv` or `IP1S`. Indeed, the equivalence is induced by an invertible linear change of variables and an invertible linear combination on the polynomials. The corresponding equivalence problem is known [Pat96a, Pat96b] as *Isomorphism of Polynomials* (`IP` or `IP2S`). Unlike `IP1S`, there is no lower bound on the computational complexity of `IP`, *i.e.* no known[1] reduction from `GI` to `IP` for instance.

`PolyEquiv`, `IP`, and `IP1S` are not NP-Hard unless the polynomial-hierarchy collapses [PGC98, Per04]. However, the situation changes drastically when considering the equivalence for more general linear transformations (in particular, not necessarily invertible). In this context, the problem is called `PolyProj`. At SODA'11, Kayal [Kay12] showed that `PolyProj` turns to be NP-Hard. This is maybe due to the fact that various fundamental questions in arithmetic complexity can be re-interpreted as particular instances of `PolyProj` (*cf.* [MS01, Bür12, Kay12, Mul12]).

Typically, the famous VP vs VNP question [Val79] can be formulated as an equivalence problem between the determinant and permanent polynomials. Such a connexion is in fact the core motivation of Geometric Complexity Theory. The problem of computing the symmetric rank [CGLM08, Ba11] of a symmetric tensor also reduces to an equivalence problem involving a particular multivariate polynomials [Kay12]. To mention another fundamental problem, the task of minimizing the cost of computing matrix multiplication reduces to a particular equivalence problem [BI11, BI13, CU13, Kay12].

**Organization of the Paper and Main Results.** Let $\mathbb{K}$ be a field, $\mathbf{f}$ and $\mathbf{g}$ be two sets of $m$ polynomials over $\mathbb{K}[x_1,\ldots,x_n]$. The Isomorphism of Polynomials (`IP`) problem, introduced by Patarin [Pat96a, Pat96b], is as follows:

**Isomorphism of Polynomials (`IP`)**
**Input:** $\big((\mathbf{f} = (f_1,\ldots,f_m) \text{ and } \mathbf{g} = (g_1,\ldots,g_m)\big) \in \mathbb{K}[x_1,\ldots,x_n]^m \times \mathbb{K}[x_1,\ldots,x_n]^m$.
**Question:** Find – if any – $(A,B) \in \mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_m(\mathbb{K})$ such that:

$$\mathbf{g}(\mathbf{x}) = B \cdot \mathbf{f}(A \cdot \mathbf{x}), \text{ with } \mathbf{x} = (x_1,\ldots,x_n)^{\mathrm{T}}.$$

[1] If $m = 1$, `IP` degenerates to `PolyEquiv`. To be more precise, there is no lower bound for `IP` when $m > 1$.

While IP is a fundamental problem in multivariate cryptography, there is quite few algorithms [PGC98, FP06, BFV13] solving IP. In particular, Faugère and Perret [FP06] proposed to solve IP by reducing it to a system of non-linear equations whose variables are the unknown coefficients of the matrices. It was conjectured [FP06], but never proved, that the corresponding system of non-linear equations can be solved in polynomial time as soon as the IP instances considered are not homogeneous. Under this conjecture, Bouillaguet, Fouque and Véber presented [BFV13] exponential (in the number of variables $n$) algorithms for solving quadratic homogeneous instances of IP over finite fields.

This situation is clearly unsatisfying, and suggests that an important open problem for IP is to identify large class of instances which can be solved in (randomized) polynomial time. We take a first step in this program by considering IP for a specific set of polynomials. In Section 5, we prove the following:

**Theorem 1.** *Let* $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{K}[x_1, \ldots, x_n]^n$. *Let* $d > 0$ *be an integer, and define* $\mathbf{POW}_{n,d} = (x_1^d, \ldots, x_n^d) \in \mathbb{K}[x_1, \ldots, x_n]^m$. *There is a randomized polynomial time algorithm which recovers – if any –* $(A, B) \in \mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_n(\mathbb{K})$ *such that:*

$$\mathbf{g} = B \cdot \mathbf{POW}_{n,d}(A \cdot \mathbf{x}).$$

This extends a similar results of Kayal [Kay11, Section 5] who considered PolyEquiv for a sum of $d$-powers polynomial. We show that solving IP for $\mathbf{POW}_{n,d}$ reduces to factor the determinant of a Jacobian matrix (in [Kay11], the Hessian matrix is considered). This illustrates, how powerful partial derivatives can be in equivalence problems [CKW11, Per05].

An important special case of IP is the IP *problem with one secret* (IP1S for short), where $B$ is the identity matrix. From a cryptographic point of view, the most natural case encountered for equivalence problems is non homogeneous polynomials with affine transformations. For IP1S, we show that such case be handled in the same way as homogeneous instances with linear transformations (see proposition 5). As such, we focus our attention to solve IP1S for quadratic homogeneous forms. To simplify the presentation in this introduction, we mainly deal with fields of characteristic $> 2$ whereas results for fields of characteristic 0 and 2 are also given latter in this paper. Now, we define formally the basic equivalence problem:

**Definition 1.** (IP1s) Let $\big(\mathbf{f} = (f_1, \ldots, f_m), \mathbf{g} = (g_1, \ldots, g_m)\big) \in \mathbb{K}[x_1, \ldots, x_n]^m \times \mathbb{K}[x_1, \ldots, x_n]^m$. We shall say that $\mathbf{f}$ and $\mathbf{g}$ are equivalent, denoted $\mathbf{f} \sim \mathbf{g}$ if there exists $A \in \mathrm{GL}_n(\mathbb{K})$ such that:

$$\mathbf{g}(x) = \mathbf{f}(A \cdot \mathbf{x}).$$

IP1S is then the problem of finding – if any – $A \in \mathrm{GL}_n(\mathbb{K})$ that makes $\mathbf{g}$ equivalent to $\mathbf{f}$ (*i.e.* $A \in \mathrm{GL}_n(\mathbb{K})$ such that $\mathbf{g}(\mathbf{x}) = \mathbf{f}(A \cdot \mathbf{x})\big)$.

We present a randomized polynomial-time algorithm for solving IP1S with quadratic polynomials. To do so, we show that such a problem can be reduced to the variant of a classical problem of representation theory over finite dimensional algebras. When $m = 1$, the IP1S problem can be easily solved by computing a reduced form of the input quadratic forms. In our more general setting we need to also to provide a canonical form of the problem.

*Canonical Form of* IP1S. Let $\big(\mathbf{f} = (f_1, \ldots, f_m), \mathbf{g} = (g_1, \ldots, g_m)\big) \in \mathbb{K}[x_1, \ldots, x_n]^m \times \mathbb{K}[x_1, \ldots, x_n]^m$ be homogeneous quadratic polynomials. Let $H_1, \ldots, H_m$ be the Hessian matrices associated of $f_1, \ldots, f_m$ (resp. $H'_1, \ldots, H'_m$ be the Hessian matrices of $g_1, \ldots, g_m$). Recall that the Hessian matrix associated to a $f_i$ is defined as $H_i = \left(\frac{\partial^2 f_i}{\partial x_k \partial x_\ell}\right)_{k,\ell} \in \mathbb{K}^{n \times n}$. Consequently, IP1S for quadratic forms is equivalent to finding $A \in \mathrm{GL}_n(\mathbb{K})$ such that:

$$H'_i = A^{\mathrm{T}} \cdot H_i \cdot A, \text{ for all } i, 1 \leq i \leq m. \tag{1}$$

Note that the success probability of the algorithms presented here will depend of the size of the field. To amplify the success probability over a small field, we will use the fact that matrices are conjugate over $\mathbb{K}$ if, and only if, they are conjugate over an algebraic extension $\mathbb{L}$ [dSP10]. Thus, we will then search linear change of variables with coefficients in some algebraic extension $\mathbb{L} \supseteq \mathbb{K}$ (but of limited degree).

Tacking as variables the entries of $A$, we can see that (1) naturally yields to a non-linear system of equations. However, we show that one can essentially linearize equations (1). To this end, we show in

Section 2 that any quadratic homogeneous instance IP1S can be reduced, under a randomized process, to a canonical form on which – in particular – all the quadratic form are non-degenerate. More precisely:

**Theorem 2.** *Let $\mathbb{K}$ be a field of* $\operatorname{char}\mathbb{K} > 2$. *There exists a randomized polynomial-time algorithm which given a quadratic homogeneous instance of* IP1S *returns "*NoSolution*" if the two systems are not equivalent or a canonical form* $\big((\sum_{i=1}^n x_i^2, f_2, \ldots, f_m), (\sum_{i=1}^n x_i^2, g_2, \ldots, g_m)\big)$, *where the $f_i$ and $g_i$ are* non degenerate *homogeneous quadratic polynomials in $\mathbb{L}[x_1, \ldots, x_n]$ such that $\mathbb{L}$ is an algebraic extension of $\mathbb{K}$ of degree $O\big(\log(n)\big)$. Any solution on the canonical form can be efficiently mapped to a solution to the initial instance (and conversely).*

*Conjugacy problem.* When IP1S is given in canonical form, equations (1) can be rewritten as $A^{\mathrm{T}}A = \mathrm{Id}$ and $H_i' = A^{\mathrm{T}} \cdot H_i \cdot A = A^{-1} \cdot H_i \cdot A$ forall $i$, such that $2 \leq i \leq m$. Our task is now to solve the following problem:

**Definition 2 (Orthogonal Simultaneous Matrix Conjugacy (OSMC)).** Let $\mathbb{K}^{n\times n}$ be the set of $n \times n$ matrices with entries in $\mathbb{K}$. Let $\{H_1, \ldots, H_m\}$ and $\{H_1', \ldots, H_m'\}$ be two families of matrices in $\mathbb{K}^{n\times n}$. The OSMC problem is the task to recover – if any – an orthogonal matrix $X \in \mathbb{L}^{n\times n}$, with $\mathbb{L}$ being an algebraic extension of $\mathbb{K}$, such that:

$$X^{-1} H_i X = H_i', \qquad \forall i, 1 \leq i \leq m,$$

In [CIK97], Chistov, Ivanyos and Karpinski show that OSMC is equivalent to:

(i) Solving the Simultaneous Matrix Conjugacy problem (SMC) between $\{H_i\}_{1\leq i\leq m}$ and $\{H_i'\}_{1\leq i\leq m}$, that is to say finding an invertible matrix $Y \in \mathrm{GL}_n(\mathbb{K})$ such that:

$$Y^{-1} \cdot H_i \cdot Y = H_i' \quad \text{and} \quad Y^{-1} \cdot H_i^{\mathrm{T}} \cdot Y = H_i'^{\mathrm{T}} \quad \forall i, 1 \leq i \leq m. \tag{2}$$

(ii) Computing the square-root $W$ of the matrix $Z = Y \cdot Y^{\mathrm{T}}$. Then, the solution of the OSMC problem is given by $X = Y W^{-1}$.

In our context, the $H_i$'s (resp. $H_i'$'s) are symmetric (Hessian matrices). Thus, condition (2) yields a system of *linear* equations and one polynomial inequation:

$$H_1 \cdot Y = Y \cdot H_1', \ldots, H_m \cdot Y = Y \cdot H_m' \text{ and } \det(Y) \neq 0. \tag{3}$$

Let $V \subset \mathbb{K}^{n\times n}$ be the linear subspace of matrices defined by these linear equations. The SMC problem is then equivalent to recovering a non-singular matrix in $V$; in other words we have to solve a particular instance of the Edmonds' problem [Edm67]. Note that, if the representation of the group generated by $\{H_i\}_{1\leq i\leq m}$ is *irreducible*, we know that $V$ has dimension at most 1 (Schur's lemma, see [Lan02, Chap. XVII, Proposition 1.1] and [New67, Lemma 2] for a matrix version of this lemma). After putting the equations in triangular form, randomly sampling over the free variables an element in $V$ yields, thanks to Schwartz-Zippel-DeMillo-Lipton [DL78, Zip79] lemma, a solution to OSMC with overwhelming probability as soon as the chosen extension field $\mathbb{L}$ of $\mathbb{K}$ is big enough. As already explained, if the cardinality of $\mathbb{L}$ is too small we can amplify the probability of success by considering a bigger algebraic extension [dSP10]. Whilst a rather "easy" randomized polynomial-time algorithm solves SMC, the task of finding a deterministic algorithm is more delicate. In this particular case, Chistov, Ivanyos and Karpinski [CIK97] presented a deterministic poly-time algorithm for solving (2).

*Matrix square root computation.* It is well known that computing square roots of matrices can be done efficiently using numerical methods (for instance, see [Gan59]). On the other hand, it seems difficult to control the bit complexity of numerical methods. In [CIK97, Section 3], the authors consider the problem of computing, in an exact way, the square root of matrices over algebraic number fields. As presented, it is not completely clear that the method proposed is polynomial-time. The issue is that the algorithm presented in [CIK97, Section 3] will have to deal with algebraic extensions of potentially non-polynomial size (since we have to work in the splitting field of some characteristic polynomial). So, the quest for an efficient algorithm for solving quadratic-IP1S required to design exact and polynomial-time algorithms for computing the square root in $\mathbb{K}^{n\times n}$ for various fields. In any case, for the sack of completeness, we propose two polynomial-time algorithms for this task. First, a general method which fixes the issue encountered in [CIK97, Section 3] is presented in Section 3.1. To do so, we adapt the technique of [Cai94] and compute the square root as the product of two matrices in an algebraic

extension which can both be computed in polynomial time. The delicate task being to control the size of the algebraic extensions occurring during the algorithm. We then present a second simpler method based on the *generalized Jordan normal form* (see Appendix A.3) which works (in polynomial time) over finite fields. In general, it deals with algebraic extensions of lesser degree than the first one. Putting things together, we obtain our main result:

**Theorem 3.** *There is a randomized polynomial-time algorithm to solve quadratic-*IP1S*. Also, as soon as one of the polynomials of the instance considered is non-degenerate, there is a deterministic polynomial-time algorithm for solving quadratic-*IP1S*.*

In Section 4, we consider the counting problem #IP1S associated to IP1S for quadratic (homogeneous) polynomials in its canonical form of Theorem 2. Remark that such counting problem is also related to cryptographic concerns. It corresponds to evaluating the number of equivalent secret-keys in MPKC [FLPW12, WP05, WP11]. Given homogeneous quadratic polynomials $\big(\mathbf{f}=(f_1,\ldots,f_m),\mathbf{g}=(g_1,\ldots,g_m)\big)\in\mathbb{K}[x_1,\ldots,x_n]^m\times\mathbb{K}[x_1,\ldots,x_n]^m$, we want to count the number of invertible matrices $A\in\mathrm{GL}_n(\mathbb{K})$ such that $\mathbf{g}(\mathbf{x})=\mathbf{f}(A\cdot\mathbf{x})$. To do so, we define:

**Definition 3.** Let $\mathbf{f}=(f_1,\ldots,f_m)\in\mathbb{K}[x_1,\ldots,x_n]^m$, we shall call *automorphism group of* $\mathbf{f}$ the set:

$$\mathscr{G}_{\mathbf{f}}=\{A\in\mathrm{GL}_n(\mathbb{K})\mid\mathbf{f}(A\cdot\mathbf{x})=\mathbf{f}(\mathbf{x})\}.$$

If $\mathbf{f}\sim\mathbf{g}$, the automorphism groups of $\mathbf{f}$ and $\mathbf{g}$ are similar. Thus, the size of the automorphism group of $\mathbf{f}$ allows to count the number of invertible matrices mapping $\mathbf{f}$ to $\mathbf{g}$. For quadratic homogeneous polynomials, the automorphism group coincides with the subset of regular matrices in the centralizer $\mathscr{C}(\mathscr{H})$ of the Hessian matrices $\mathscr{H}$ associated to $\mathbf{f}$. We prove the following structural results for $\mathscr{C}(\mathscr{H})$:

**Proposition 4.** *Let $\alpha$ be an algebraic element of degree $m$ over $\mathbb{K}$. Let $H=\sum_{i=1}^{m}H_i\alpha^{i-1}\in\mathbb{K}(\alpha)^{n\times n}$ be a matrix and let $D$ be its normal Jordan form. Assuming that $J_{\lambda_1,s_{1,1}},\ldots,J_{\lambda_1,s_{1,d_1}},\ldots,J_{\lambda_r,s_{r,1}},\ldots,J_{\lambda_r,s_{r,d_r}}$ are the blocks of $D$, then the centralizer of $\mathscr{H}$ is a $\mathbb{K}$-vector subspace of $\mathbb{K}^{n\times n}$. Its dimension is bounded from above by:*

$$\sum_{1\le i\le r}\sum_{1\le j\le d_i}(2d_i-2j+1)\,s_{i,j}.$$

## 2. Normalization - Canonical form of IP1S

In this section, we prove Theorem 2. In other words, we explain how to reduce any quadratic homogeneous instance $(\mathbf{f},\mathbf{g})\in\mathbb{K}[x_1,\ldots,x_n]^m\times\mathbb{K}[x_1,\ldots,x_n]^m$ of IP1S to a suitable canonical form, *i.e.* an instance of IP1S where all the Hessian matrices are invertible and the first two Hessian equal the identity. We emphasize that the reduction presented is randomized and requires to consider an algebraic extension of limited degree.

2.i. *Homogenization.* We show here that the equivalence problem over non homogeneous polynomials with affine transformation on the variables reduces to the equivalence problem over homogeneous polynomials with linear transformation on the variables. To do so, we simply homogenize the polynomials. Let $x_0$ be a new variable. For any polynomial $p\in\mathbb{K}[\mathbf{x}]$ of degree 2, we denote by $p^\star(x_0,x_1,\ldots,x_n)=x_0^2p(x_1/x_0,\ldots,x_n/x_0)$ its *homogenization*.

**Proposition 5.** IP1S *with quadratic polynomials and affine transformation on the variables many-one reduces to* IP1S *with homogeneous quadratic polynomials and linear transformation on the variables.*

*Proof.* Let $(\mathbf{f},\mathbf{g})\in\mathbb{K}[\mathbf{x}]^m\times\mathbb{K}[\mathbf{x}]^m$ be non homogeneous polynomials of degree 2. We consider the transformation which maps $(\mathbf{f},\mathbf{g})$ to $\big(\mathbf{f}^\star=(f_1^\star,\ldots,f_m^\star,x_0^2),\mathbf{g}^\star=(g_1^\star,\ldots,g_m^\star,x_0^2)\big)$. This clearly transforms polynomials of degree 2 to homogeneous quadratic polynomials. We can write $f_i(\mathbf{x})=\mathbf{x}^{\mathrm{T}}H_i\mathbf{x}+L_i\mathbf{x}+c_i$ with $H_i\in\mathbb{K}^{n\times n}$, $L_i\in\mathbb{K}^n$ and $c_i\in\mathbb{K}$, then $f_i(A\mathbf{x}+b)=(A\mathbf{x}+b)^{\mathrm{T}}H_i(A\mathbf{x}+b)+L_i(A\mathbf{x}+b)+c_i$ and its homogenization is $(A\mathbf{x}+bx_0)^{\mathrm{T}}H_i(A\mathbf{x}+bx_0)+L_i(A\mathbf{x}+bx_0)+c_ix_0^2=f_i^*(A'\mathbf{x}^\star)$, with $\mathbf{x}^\star=(x_1,\ldots,x_n,x_0)^{\mathrm{T}}$. If $(A,b)\in\mathrm{GL}_n(\mathbb{K})\times\mathbb{K}^n$ is an affine transformation solution on the non homogeneous instance then $A'=\left(\begin{smallmatrix}A & b\\ 0 & 1\end{smallmatrix}\right)$ is a solution for the homogenized instance. Conversely, a solution $A'\in\mathrm{GL}_{n+1}(\mathbb{K})$ of the homogeneous problem must stabilize the homogenization variable $x_0$ in order to be a solution of the non homogeneous problem. This is forced by adding $f_{m+1}=x_0^2$ and $g_{m+1}=x_0^2$ and setting $C'=A'/a'_{n+1,n+1}$. One can see that $C'$ is of the form $\left(\begin{smallmatrix}C & d\\ 0 & 1\end{smallmatrix}\right)$, and $(C,d)\in\mathrm{GL}_n(\mathbb{K})\times\mathbb{K}^n$ is a solution for $(\mathbf{f},\mathbf{g})$. □

2.ii. *Redundant Variables.* As a first preliminary natural manipulation, we first want to eliminate – if any – *redundant variables* from the instances considered. Thanks to E. Carlini [Car05] (and reformulated by Kayal in [Kay11]), this task can be done in randomized polynomial time:

**Proposition 6.** [Car05, Kay11] *Let $f \in \mathbb{K}[x_1 \dots, x_n]$ be a polynomial. $f$ has $s$* essential *variables if $\exists M \in \mathrm{GL}_n(\mathbb{K})$ such that $f(M\mathbf{x})$ depends only of the first $s$ variables $x_1, \dots, x_s$. The remaining $n-s$ variables $x_{s+1} \dots, x_n$ will be called* redundant *variables. The polynomial $f$ is said* regular *if its number of essential variables is $n$. If $\mathrm{char}\,\mathbb{K} = 0$ or $\mathrm{char}\,\mathbb{K} > \deg f$, and $f$ has $s$ essential variables, then we can compute in randomized polynomial time $M \in \mathrm{GL}_n(\mathbb{K})$ s.t. $f(M\mathbf{x})$ depends only of the first $s$ variables.*

For a set of equations, we extend the notion of essential variables as follows.

**Definition 4.** The number of essential variables of $\mathbf{f} = (f_1, \dots, f_m) \in \mathbb{K}[x_1, \dots, x_n]^m$ is the smallest $s$ such that $\mathbf{f}$ can be decomposed as:

$$\mathbf{f} = \tilde{\mathbf{f}}(\ell_1, \dots, \ell_s)$$

with $\ell_1, \dots, \ell_s$ linear forms in $x_1, \dots, x_n$ of rank $s$ and $\tilde{\mathbf{f}} \in \mathbb{K}[y_1, \dots, y_s]^m$. We shall say that $\mathbf{f}$ is regular if its number of essential variables is $n$.

For a quadratic form, $s$ is simply the rank of the associated Hessian matrix. The linear forms $\ell_1, \dots, \ell_s$ can be easily computed thanks to Proposition 6 when the characteristic of $\mathbb{K}$ is zero or greater than the degrees of $f_1, \dots, f_m$. In characteristic 2, when $\mathbb{K}$ is perfect (which is always true if $\mathbb{K}$ is finite for instance) the linear forms can also be recovered in polynomial time (see [BHM10, Gir72, Hir70] for instance). Below, we show that we can restrict our attention to only essential variables. Namely, solving `IP1S` on $(\mathbf{f}, \mathbf{g})$ reduces to solve `IP1S` on instances having only essential variables.

**Proposition 7.** *Let $(\mathbf{f}, \mathbf{g}) \in \mathbb{K}[x_1, \dots, x_n]^m \times \mathbb{K}[x_1, \dots, x_n]^m$. If $\mathbf{f} \sim \mathbf{g}$, then their numbers of essential variables must be the same. Let $s$ be the number of essential variables of $\mathbf{f}$. Finally, let $(\tilde{\mathbf{f}}, \tilde{\mathbf{g}}) \in \mathbb{K}[y_1, \dots, y_s]^m \times \mathbb{K}[y_1, \dots, y_s]^m$ be such that:*

$$\mathbf{f} = \tilde{\mathbf{f}}(\ell_1, \dots, \ell_s) \text{ and } \mathbf{g} = \tilde{\mathbf{g}}(\ell'_1, \dots, \ell'_s),$$

*with $\ell_1, \dots, \ell_s$ (resp. $\ell'_1, \dots, \ell'_s$) linear forms in $x_1, \dots, x_n$ of rank $s$ and $\tilde{\mathbf{f}}, \tilde{\mathbf{g}} \in \mathbb{K}[y_1, \dots, y_s]^m$. It holds that:*

$$\mathbf{f} \sim \mathbf{g} \iff \tilde{\mathbf{f}} \sim \tilde{\mathbf{g}}.$$

*Proof.* Let $H_1, \dots, H_m$ be the Hessian matrices associated of $f_1, \dots, f_m$ (resp. $H'_1, \dots, H'_m$ be the Hessian matrices of $g_1, \dots, g_m$). Similarly, we define the Hessian matrices $\tilde{H}_1, \dots, \tilde{H}_m$ (resp. $\tilde{H}'_1, \dots, \tilde{H}'_m$) associated to $\tilde{f}_1, \dots, \tilde{f}_m$ (resp. $\tilde{g}_1, \dots, \tilde{g}_m$). Let also $M$ and $N$ be matrices in $\mathbb{K}^{n \times n}$ such that $H_i = M^{\mathrm{T}} \left(\begin{smallmatrix} \tilde{H}_i & 0 \\ 0 & 0 \end{smallmatrix}\right) M$ and $H'_i = N^{\mathrm{T}} \left(\begin{smallmatrix} \tilde{H}'_i & 0 \\ 0 & 0 \end{smallmatrix}\right) N$ for all $i, 1 \le i \le m$. There exist such $M$ and $N$, as $\mathbf{f}$ and $\mathbf{g}$ have essentially $s$ variables. Up to re-indexing the rows of $M$ and $N$, one can always choose $M$ and $N$ such that $M = \left(\begin{smallmatrix} M_1 & M_2 \\ 0 & \mathrm{Id} \end{smallmatrix}\right)$ and $N = \left(\begin{smallmatrix} N_1 & N_2 \\ 0 & \mathrm{Id} \end{smallmatrix}\right)$, with $M_1, N_1 \in \mathrm{GL}_s(\mathbb{K})$.

If $\tilde{\mathbf{f}} \sim \tilde{\mathbf{g}}$, $\exists \tilde{A} \in \mathrm{GL}_s(\mathbb{K})$ such that $\tilde{A}^{\mathrm{T}} \tilde{H}_i \tilde{A} = \tilde{H}'_i$, for all $i, 1 \le i \le m$. Then, for all $B \in \mathrm{GL}_{n-s}(\mathbb{K})$:

$$\left(\begin{smallmatrix} \tilde{A}^{\mathrm{T}} & 0 \\ 0 & B^{\mathrm{T}} \end{smallmatrix}\right) \left(\begin{smallmatrix} \tilde{H}_i & 0 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} \tilde{A} & 0 \\ 0 & B \end{smallmatrix}\right) = \left(\begin{smallmatrix} \tilde{H}'_i & 0 \\ 0 & 0 \end{smallmatrix}\right),$$

$$N^{\mathrm{T}} \left(\begin{smallmatrix} \tilde{A}^{\mathrm{T}} & 0 \\ 0 & B^{\mathrm{T}} \end{smallmatrix}\right) M^{-\mathrm{T}} H_i M^{-1} \left(\begin{smallmatrix} \tilde{A} & 0 \\ 0 & B \end{smallmatrix}\right) N = H'_i.$$

Therefore, $\mathbf{f}$ and $\mathbf{g}$ are equivalent.

Conversely, we assume now that $\mathbf{f} \sim \mathbf{g}$, *i.e.* there exists $A \in \mathrm{GL}_n(\mathbb{K})$ such that $A^{\mathrm{T}} \cdot H_i \cdot A = H'_i$, for all $i, 1 \le i \le m$. This implies that:

$$N^{-\mathrm{T}} A^{\mathrm{T}} M^{\mathrm{T}} \left(\begin{smallmatrix} \tilde{H}_i & 0 \\ 0 & 0 \end{smallmatrix}\right) M A N^{-1} = \left(\begin{smallmatrix} \tilde{H}'_i & 0 \\ 0 & 0 \end{smallmatrix}\right), \forall i, 1 \le i \le m.$$

We then define $\tilde{A} = (MAN^{-1}_{i,j})_{1 \le i,j \le s}$, so that $\tilde{f}(\tilde{A}\mathbf{x}) = \tilde{g}(\mathbf{x})$. As $\mathbf{g}$ has $s$ essential variables, then $\mathrm{rank}(\tilde{A})$ cannot be smaller than $s$, hence $\tilde{A} \in \mathrm{GL}_s(\mathbb{K})$. We then get $\tilde{A}^{\mathrm{T}} \tilde{H}_i \tilde{A} = \tilde{H}'_i$ for all $i, 1 \le i \le m$, *i.e.* $\tilde{\mathbf{f}} \sim \tilde{\mathbf{g}}$. □

According to Proposition 7, we can the consider w.l.o.g. that the number of essential variables of both $\mathbf{f}$ and $\mathbf{g}$ are $n$. There is an efficient reduction mapping an instance $(\mathbf{f},\mathbf{g})$ of IP1S to an instance $(\tilde{\mathbf{f}},\tilde{\mathbf{g}})$ of IP1S having only essential variables. From now on, we will then always assume that we consider instances of IP1S with $n$ essential variables.

2.iii. *Canonical Form.* We now assume that $\operatorname{char}\mathbb{K} > 2$. In this part, we want to show that it is always possible to assume that at least one Hessian matrix associated to a quadratic homogeneous instance is non-singular. More precisely:

**Proposition 8.** *Let $\mathbf{f} = (f_1,\dots,f_m) \in \mathbb{K}[x_1,\dots,x_n]$ be quadratic homogeneous forms. If $\mathbf{f}$ is regular and $|\mathbb{K}| > n$, then there exists a non-degenerate quadratic form $f$ in $\operatorname{Span}_{\mathbb{K}}(\mathbf{f})$ (i.e. the $\mathbb{K}$-vector space spanned by the polynomials of $\mathbf{f}$). Moreover, there exists a randomized polynomial-time algorithm recovering $\lambda_1,\dots,\lambda_m \in \mathbb{K}$ such that $\sum_{i=1}^m \lambda_i \cdot f_i$ is non-degenerate with success probability at least $1 - n/|\mathbb{K}|$.*

*Proof.* We shall prove this by induction on $(m,n) \in \mathbb{N}^* \times \mathbb{N}^*$.

First, the affirmation holds clearly whenever $m = 1$ and $n \neq 0$ is any. Then let us prove it by induction on $n > 0$ whenever $m = 2$. The affirmation clearly holds whenever $n = 1$. Let us assume it holds for all $1 \leq q \leq n$ and let us prove that it still holds for $n+1$. Let $\mathbf{f} = (f_1, f_2)$ be such that its essential number of variables is $n+1$. Assuming the minimal number of variables of $f_1$ is $q$, w.l.o.g., one can assume that these variables are $x_1,\dots,x_q$, hence its Hessian matrix is

$$H_1 = \begin{pmatrix} H_{11} & 0 \\ 0 & 0 \end{pmatrix}$$

with $H_{11}$ diagonal and regular. As $\mathbf{f}$ is regular, a set of essential variables of $f_2$ contains at least $x_{q+1} + \ell_{q+1}(x_1,\dots,x_q),\dots,x_{n+1} + \ell_{n+1}(x_1,\dots,x_q)$, where $\ell_{q+1},\dots,\ell_{n+1}$ are linear forms. Applying a partial Gauß reduction algorithm on $f_2$ from $x_{n+1}$ to $x_{q+1}$, one can assume that the Hessian matrix of $f_2$ is

$$H_2 = \begin{pmatrix} H_{21} & 0 \\ 0 & H_{24} \end{pmatrix}$$

with $H_{24}$ diagonal and regular. As a consequence, if $H_2$ is invertible, then $f_2$ suits. Otherwise,

$$\det(H_1 + \lambda H_2) = \begin{vmatrix} H_{11} + \lambda H_{21} & 0 \\ 0 & H_{24} \end{vmatrix} = \det(H_{11} + \lambda H_{21}) \det H_{24} = \det H_{11} \det(\mathrm{Id} + \lambda H_{11}^{-1} H_{21}) \det H_{24}.$$

Hence this determinant is non zero if, and only if, $-\lambda$ is not an eigenvalue of $H_{11}^{-1}H_{21}$. There are at most $q \leq n+1$ such $\lambda$'s.

Now assume that the affirmation holds for all $2 \leq p \leq m$ and $1 \leq q \leq n$. Let us prove that the affirmation still holds for $(m+1,n)$. Let $\mathbf{f} = (f_1,\dots,f_{m+1})$ be such that its essential number of variables is $n$. Assuming the minimal number of variables of $\tilde{\mathbf{f}} = (f_1,\dots,f_m)$ is $q$, w.l.o.g., one can assume that these variables are $x_1,\dots,x_q$, then by assumption there exists $\varphi \in \operatorname{Span}_{\mathbb{K}}(\tilde{\mathbf{f}})$ that is regular in $x_1,\dots,x_q$. As $\mathbf{f}$ is regular, a set of essential variables of $f_{m+1}$ contains at least $x_{q+1} + \ell_{q+1}(x_1,\dots,x_q),\dots,x_n + \ell_n(x_1,\dots,x_q)$, where $\ell_{q+1},\dots,\ell_n$ are linear forms. Thus $(\varphi, f_m)$ is regular in $x_1,\dots,x_n$. By assumption, there exists a linear combination of both which is non-degenerate.

Now, let $H_1,\dots,H_m$ be the Hessian matrices associated to the quadratic forms of $\mathbf{f}$. We consider now the task to find $\lambda_1,\dots,\lambda_m \in \mathbb{K}$ such that $\operatorname{rank}(\sum_{i=1}^m \lambda_i \cdot f_i) = n$. Once again, we have to solve a particular instance of Edmonds' problem (also known as *maximum matrix completion* problem in the literature, *e.g.* [HKM05, HKY06]). In [Lov79], Lovász shows that a solution maximizing the rank can be found by simply randomly assigning values to the variables. We know that there exists an invertible matrix in the linear space of the Hessian matrices. Then, Schwartz-Zippel-DeMillo-Lipton Lemma [DL78, Zip79] guarantees that a random assignment of the variables will provide an invertible matrix with success probability at least $1 - n/|\mathbb{K}|$. □

We are now in position to reduce quadratic homogeneous instances of IP1S to a first simplified form.

**Proposition 9.** *Let $(\mathbf{f},\mathbf{g}) \in \mathbb{K}[x_1,\dots,x_n]^m \times \mathbb{K}[x_1,\dots,x_n]^m$ be quadratic homogeneous polynomials. There is a randomized polynomial-time algorithm which returns "*NoSolution*" only if $\mathbf{f} \not\sim \mathbf{g}$, or a new instance $(\tilde{\mathbf{f}},\tilde{\mathbf{g}}) = \big((\sum_{i=1}^n x_i^2, \tilde{f}_2,\dots,\tilde{f}_m), (\sum_{i=1}^n x_i^2, \tilde{g}_2,\dots,\tilde{g}_m)\big) \in \mathbb{L}[x_1,\dots,x_n]^m \times \mathbb{L}[x_1,\dots,x_n]^m$, where $\mathbb{L}$ is an algebraic extension of $\mathbb{K}$ of degree 2, such that $\mathbf{f} \sim \mathbf{g} \iff \tilde{\mathbf{f}} \sim \tilde{\mathbf{g}}$. In the latter case, the output*

*of this algorithm is correct with probability at least* $1-n/|\mathbb{K}|$. *If* $\mathbf{f}\sim\mathbf{g}$, *invertible matrices* $P,Q$ *and* $A'\in \mathrm{GL}_n(\mathbb{L})$ *are returned such that* $\mathbf{f}(P\mathbf{x})=\tilde{\mathbf{f}}(\mathbf{x})$, $\mathbf{g}(P\mathbf{x})=\tilde{\mathbf{g}}(\mathbf{x}), \tilde{\mathbf{g}}(Q\mathbf{x})=\bar{\mathbf{g}}$ *and* $\tilde{\mathbf{f}}(A'\mathbf{x})=\bar{\mathbf{g}}(\mathbf{x})$. *It then holds that* $\mathbf{f}(PA'Q^{-1}P^{-1}\mathbf{x})=\mathbf{g}(\mathbf{x})$.

*Proof.* According to Proposition 8, we can can compute in randomized polynomial time $\lambda_1,\ldots,\lambda_m\in\mathbb{K}$ such that $f=\sum_{i=1}^m \lambda_i\cdot f_i$ is regular. We define $g=\sum_{i=1}^m \lambda_i\cdot g_i$. Should one reorder the equations, we can assume w.lo.g. that $\lambda_1\neq 0$. We have then:

$$\mathbf{f}\sim\mathbf{g} \iff (f,f_2,\ldots,f_m)\sim(g,g_2,\ldots,g_m).$$

Now, applying Gauß reduction algorithm to $f$, there exist $k\in\{1,\ldots,n\}$ and $a\in\mathbb{K}^2\setminus\mathbb{K}$ such that $f=\sum_{i=1}^k \ell_i^2+a\sum_{i=k+1}^n \ell_i^2$, where $\ell_1,\ldots,\ell_n$ are independent linear forms in $x_1,\ldots,x_n$ (for instance see [LN97, Theorem 6.21]). If $k<n$, over $\mathbb{L}=\mathbb{K}(\sqrt{a})$, which is the quadratic extension of $\mathbb{K}$, one can write $f_1=\sum_{i=1}^n \ell_i{}^2$. This gives a $P\in\mathrm{GL}_n(\mathbb{L})$ such that $\tilde{\mathbf{f}}=(\tilde{f}=\sum_{i=1}^n x_i^2,\tilde{f}_2,\ldots,\tilde{f}_m)=(f(P\mathbf{x}),f_2(P\mathbf{x}),\ldots,f_m(P\mathbf{x}))$ $\big($resp. $\tilde{\mathbf{g}}=(\tilde{g},\tilde{g_2},\ldots,\tilde{g_m})=\big(g(P\mathbf{x}),g_2(P\mathbf{x}),\ldots,g_m(P\mathbf{x})\big)\big)$. Clearly, $\mathbf{f}\sim\tilde{\mathbf{f}}$ and $\mathbf{g}\sim\tilde{\mathbf{g}}$. Hence, $\tilde{\mathbf{f}}\sim\tilde{\mathbf{g}}$.

After that, we can apply once again Gauß reduction to $\tilde{g}$. If the reduced polynomial is different from $\sum_{i=1}^n x_i^2$, then $\mathbf{f}\not\sim\mathbf{g}$ and we return "NoSolution". Otherwise, the reduction is given by a matrix $Q\in\mathrm{GL}_n(\mathbb{L})$ such that $\bar{\mathbf{g}}=(\bar{g}=\sum_{i=1}^n x_i^2,\bar{g}_2,\ldots\bar{g}_m)=(\tilde{g}(Q\mathbf{x}),\tilde{g}_2(Q\mathbf{x}),\ldots,\tilde{g}_m(Q\mathbf{x}))$ and $\mathbf{g}\sim\tilde{\mathbf{g}}\sim\bar{\mathbf{g}}$. Thus, $\tilde{\mathbf{f}}\sim\bar{\mathbf{g}}$ if, and only, if $\mathbf{f}\sim\mathbf{g}$. Now, assume that $\exists A'\in\mathrm{GL}_n(\mathbb{L})$ such that $\tilde{f}(A'\mathbf{x})=\bar{\mathbf{g}}(\mathbf{x})$. Then, $\mathbf{f}(PA'\mathbf{x})=\mathbf{g}(PQ\mathbf{x})$ and $\mathbf{f}(PA'Q^{-1}P^{-1}\mathbf{x})=\mathbf{g}(\mathbf{x})$. □

2.iv. *Invertible Hessian Matrices.* We are now in position to reduce any homogeneous quadratic instances $(\mathbf{f},\mathbf{g})$ of `IP1S` to a new form of the instances where all the polynomials are regular. From Proposition 9, this is already the case – under randomized reduction – for $f_1$ and thus $g_1$. For the others polynomials, we proceed as follows. For $i, 2\leq i\leq m$, if the Hessian matrix $H_i$ of $f_i$ is invertible, then we do nothing. Otherwise, we change $H_i$ into $H_i+\lambda\mathrm{Id}=H_i+\lambda H_1$, for $\lambda$ in a suitable extension. Indeed, we must have a $\lambda$ which is not the opposite of an eigenvalue of $H_i$. To this end, we consider the smallest $\mathbb{L}$ extension of $\mathbb{K}$ with at least $n+1$ elements. There exists such a $\lambda$ in $\mathbb{L}$. This gives the following result:

**Theorem 10.** *Let* $(\mathbf{f},\mathbf{g})\in\mathbb{K}[x_1,\ldots,x_n]^m\times\mathbb{K}[x_1,\ldots,x_n]^m$ *be quadratic homogeneous polynomials. There is a randomized polynomial-time algorithm which returns "*NoSolution*" only if* $\mathbf{f}\not\sim\mathbf{g}$. *Otherwise, the algorithm returns two sets of* $n\times n$ *invertible symmetric matrices* $\{\mathrm{Id},\tilde{H}_2\ldots,\tilde{H}_m\}$ *and* $\{\mathrm{Id},\tilde{H}'_m,\ldots,\tilde{H}'_m\}$ *defined over algebraic extension* $\mathbb{L}$ *of* $\mathbb{K}$ *of degree* $O(\log n)$ *such that:*

$$\mathbf{g}(\mathbf{x})=f(A\mathbf{x}),\ \textit{for some}\ A\in\mathrm{GL}_n(\mathbb{K}) \iff A'^{-1}\tilde{H}_iA'=\tilde{H}'_i,\forall i,1\leq i\leq m,\ \textit{for some}\ A'\in\mathscr{O}_n(\mathbb{L}),$$

*with* $\mathscr{O}_n(\mathbb{L})$ *denoting the set of* $n\times n$ *orthogonal matrices over* $\mathbb{L}$.

*Proof.* Combining Proposition 9 and paragraph 2.iv any quadratic homogeneous instance of `IP1S` can be reduced in randomized polynomial time to "NoSolution" only if the two systems are not equivalent or to a $(\tilde{f},\tilde{g})=\big((\sum_{i=1}^n x_i^2,\tilde{f}_2,\ldots,\tilde{f}_m),(\sum_{i=1}^n x_i^2,\tilde{g}_2,\ldots,\tilde{g}_m)\big)$, where all the polynomials are *non degenerate* homogeneous quadratic polynomials in $\mathbb{L}[x_1,\ldots,x_n]$ where $\mathbb{L}$ is an algebraic extension of $\mathbb{K}$ of degree $2\left\lceil\frac{\log_q(n+1)}{2}\right\rceil$. It follows that $\tilde{\mathbf{f}}\sim\tilde{\mathbf{g}} \iff \exists A'\in\mathrm{GL}_n(\mathbb{L})$ such that $\forall i,1\leq i\leq m$, $A'^{\mathrm{T}}\tilde{H}_iA'=\tilde{H}'_i$. In particular $A'^{\mathrm{T}}\mathrm{Id}A'=\mathrm{Id}$ and $A'$ is orthogonal. Hence, $A'^{\mathrm{T}}\tilde{H}_iA'=A'^{-1}\tilde{H}_iA'=H'_i,\forall i,1\leq i\leq m$. □

The proof of this result implies Theorem 2.

2.v. *Field Extensions and Jordan Normal Form.* To amplify the success probability of our results, it will be convenient to embed $\mathbb{K}$ in some finite extension $\mathbb{L}$ of $\mathbb{K}$. This is motivated by the fact that matrices in $\mathbb{K}^{n\times n}$ are similar if, and only if, they are similar in $\mathbb{L}^{n\times n}$, see [dSP10]. In this paper, we will need to compute the *Jordan normal form* $J$ of some matrix $H$ in several situations. The computation of the Jordan normal form is done in two steps. First, we factor the characteristic polynomial, using for instance Berlekamp's algorithm [vzGG99, Theorem 14.14] over $\mathbb{K}=\mathbb{F}_q$ in $O(n\mathsf{M}(n)\log(qn))$ operations in $\mathbb{K}$. Then, we use Storjohann's algorithm [Sto98] to compute the generalized eigenvectors in $O(n^\omega)$ operations in $\mathbb{K}$, with $2<\omega\leq 3$.

## 3. QUADRATIC IP1S

In this section, we present efficient algorithms for solving quadratic-IP1S. According to Proposition 5, we can w.l.o.g. restrict our attention on linear change of variables and homogeneous quadratic instances. Let $\mathbb{L}$ be an algebraic extension of $\mathbb{K}$ of degree $O(\log(n))$. Let $\mathscr{H} = \{\mathrm{Id}, H_2, \ldots, H_m\}$ and $\mathscr{H}' = \{\mathrm{Id}, H'_2, \ldots, H'_m\}$ be two families of invertible symmetric matrices in $\mathbb{L}^{n\times n}$. As explained in Theorem 10, our task reduces – under a randomized process – to finding an orthogonal matrix $A' \in \mathscr{O}_n(\mathbb{L})$ such that:

$$A'^{-1} H_i A' = H'_i, \forall i, 1 \leq i \leq m. \tag{4}$$

In [CIK97, Theorem 4], the authors prove that there is an orthogonal solution $A$ such that $H_i A = A H'_i$ if, and only if, there is a regular matrix $Y$ such that $H_i Y = Y H'_i$ and $H_i^{\mathrm{T}} Y = Y H_i^{\mathrm{T}}$. In our case, the matrices are symmetric. So, the added conditions – with the transpose – are automatically fulfilled. The authors of [CIK97] suggest then to use the polar decomposition of $Y = AW$, with $W$ symmetric and $A$ orthogonal. Then, $A$ is an orthogonal solution of (4). Remark that whenever we just want to test if $\mathbf{f} \sim \mathbf{g}$, it is enough to find such a regular $Y$.

The main idea to compute $A$ is to compute $W$ as the square root of $Z = Y^{\mathrm{T}} Y$ as stated in [CIK97, Section 3]. However, in general $W$ and $A$ are not defined over $\mathbb{L}$ but over $\mathbb{L}(\zeta_1, \ldots, \zeta_r)$, where $\zeta_1, \ldots, \zeta_r$ are the eigenvalues of $Z$. Assuming $\zeta_1$ is the root of an irreducible polynomial $P$ of degree $d$, then $\zeta_2, \ldots, \zeta_d$ are also roots of the same polynomial. However, there is no reason for them to be in $\mathbb{L}[x]/(P) = \mathbb{L}(\zeta_1)$. But they will be the roots of a polynomial of degree $d-1$, in general, over the field $\mathbb{L}(\zeta_1)$. Then, doing another extension might only add one eigenvalue in the field. Repeating this process yields a field of degree $d!$ over $\mathbb{L}$. As a consequence, in the worst case, we can have to work over an extension field of degree $n!$. Therefore, computing $W$ could be the bottleneck of the method.

In [CIK97], Chistov *et al.* emphasize that constructing such a square root $W$ in polynomial time is the only serious algorithmic problem. As presented, it is not completely clear that the method proposed is efficient. From $Z' = YY^{\mathrm{T}}$, they propose to compute the eigenspaces $V_1, \ldots, V_r$ of $Z'$ and then express the restriction $Y_i$ of $Y$ to $V_i$. Let us remark that one cannot use Cai's work [Cai94] to compute it as $Y$ does not commute with $Z$, hence $Y_i$ is a map from $V_i$ to the whole space $V$. The obtained matrix, *i.e* $YT$ with $T$ such that $T^{-1} Z' T = \mathrm{Diag}(\zeta_1, \ldots, \zeta_n)$, has each column defined over one extension $\mathbb{L}(\zeta_i)$. Then, setting $W'^2 = Z'$, as a map from $V_i$ to itself, $T^{-1} W'^{-1} T$ is just a multiplication by $\sqrt{\zeta_i}^{-1}$. Finally, $X' = W'^{-1} Y$ makes them set $X_i = \sqrt{\zeta_i}^{-1} Y_i$. However, the image of $Y_i$ need not be included in $V_i$, hence the multiplication by $W'^{-1}$ is not just a multiplication by $\sqrt{\zeta}^{-1}$. Even if it were, the concatenation of matrices $X_i$ would be $XT$ and not $X$. Then, multiplying by $T^{-1}$ would yield $X$ but might be only computed in exponential time [Cai94].

Let us mention that our motivation to set $Z = Y^{\mathrm{T}} Y$ and take $A = Y W^{-1}$ is coming from this issue about $W^{-1} Y_i$, since, in this case, their argument is valid. However, this does not resolve the problem of computing $XT$ and not $X$. For the sake of completeness, we present several efficient algorithms for performing the square root computation.

### 3.1. Computing of the Orthogonal Solution.

The goal of this part is to "orthogonalize" a regular solution $Y \in \mathrm{GL}_n(\mathbb{L})$ of equation 4. Instead of computing exactly $A \in \mathscr{O}_n(\mathbb{L})$, we compute in polynomial-time two matrices whose product is $A$. These matrices allow to verify in polynomial-time that $H_i$ and $H'_i$ are conjugate for all $i, 1 \leq i \leq m$. To be more precise, we prove the following proposition.

**Proposition 11.** *Let $\mathscr{H} = \{H_1, \ldots, H_m\}$ and $\mathscr{H}' = \{H'_1, \ldots, H'_m\}$ be two sets of regular matrices in $\mathbb{L}^{n\times n}$. We can compute in polynomial time two matrices $P$ and $Q$ defined over an algebraic extension $\mathbb{L}'$ such that $PQ^{-1}$ is orthogonal and for all $1 \leq i \leq m$, $H_i(PQ^{-1}) = (PQ^{-1})H'_i$. in the worst case, product $PQ^{-1}$ cannot be computable in polynomial time over $\mathbb{L}'$. However, the matrices $P^{\mathrm{T}} H_i P$ and $Q^{\mathrm{T}} H'_i Q$ can be computed and tested for equality in polynomial time.*

*Proof.* Let $Y \in \mathrm{GL}_n(\mathbb{L})$ such that $H_i Y = Y H'_i, \forall i, 1 \leq i \leq m$. We set $Z = Y^{\mathrm{T}} Y$. Let us denote by $T$, the change of basis matrix such that $J = T^{-1} Z T$ is the Jordan normal form of $Z$. According to Cai [Cai94], $T$, $T^{-1}$ and $J$ can be computed in polynomial time. Because of the issue of mixing all the eigenvalues of $Z$, we cannot compute efficiently $A$ in one piece. We will then compute $AT$ and $T^{-1}$ separately. Indeed,

$AT$ (resp. $T^{-1}$) is such that each of its columns (resp. each of its rows) is defined over an extension field $\mathbb{L}(\zeta_i)$, where $\zeta_1, \ldots, \zeta_r$ are the eigenvalues of $Z$.

We shall say that a matrix is *block-wise* (resp. *columnblock-wise*, *rowblock-wise*) *defined over* $\mathbb{L}(\zeta)$ if for all $1 \leq i \leq r$, its $i$th block (resp. block of columns, block of rows) is defined over $\mathbb{L}(\zeta_i)$. The size of the $i$th block being the size of the $i$th Jordan block of $J$.

As $J = T^{-1}ZT$ is a Jordan normal form, it is block-wise defined over $\mathbb{L}(\zeta)$. Using the closed formula of Appendix A.1, one can compute in polynomial time a square root $G$ of $J$. This matrix is a block diagonal matrix, block-wise defined over $\mathbb{L}(\sqrt{\zeta})$, hence can be inverted in polynomial time. If one would want $W$, one would have to compute $W = TGT^{-1}$. Let us recall that matrices $T$ and $T^{-1}$ are respectively columnblock-wise and rowblock-wise defined over $\mathbb{L}(\zeta)$, see [Cai94, Section 4]. Since $Y$ is defined over $\mathbb{L}$, then $YT$ is blockcolumn-wise defined over $\mathbb{L}(\zeta)$. Thus $AT = YW^{-1}T = YTG^{-1}$ is a blockcolumn-wise defined over $\mathbb{L}(\sqrt{\zeta})$. We recall that product $AT \cdot T^{-1}$ mangles the eigenvalues and make each coefficients defined over $\mathbb{L}\left(\sqrt{\zeta_1}, \ldots, \sqrt{\zeta_r}\right)$ and thus must be avoided.

Now, to verify that $A^{\mathrm{T}}HA = H'$, for any $H \in \mathscr{H}$ and the corresponding $H' \in \mathscr{H}'$, we compute separately $T^{\mathrm{T}}A^{\mathrm{T}}HAT$ and $T^{\mathrm{T}}H'T$. For the former, $AT$ (resp. $(AT)^{\mathrm{T}}$) is columnblock-wise (resp. rowblock-wise) defined over $\mathbb{L}(\sqrt{\zeta})$ and $H$ is defined over $\mathbb{L}$. Therefore, the product matrix has its coefficients which are on both the $i$th block of rows and the $j$th block of columns defined over $\mathbb{L}\left(\sqrt{\zeta_i}, \sqrt{\zeta_j}\right)$ and so can be computed in polynomial time. For the latter, the same behaviour occurs on the resulting matrix as $T$ is blockcolumn-wise defined over $\mathbb{L}(\zeta)$.

Let us assume that the characteristic polynomial of $Z$ has degree $n$ and can be factored as $P_1^{m_1} \cdots P_s^{m_s}$ with $P_i$ and $P_j$ coprime whenever $i \neq j$, $\deg P_i = d_i$ and $m_i \geq 1$. From a computation point of view, one needs to introduce a variable $\alpha_{i,j}$ for each root of $P_i$ and then a variable $\beta_{i,j}$ for the square root of $\alpha_{i,j}$. This yields a total number of $2\sum_{i=1}^{s} d_i$ variables. In Appendix A.3, we present another method which manages to introduce only $2s$ variables. □

3.2. **Probabilistic and Deterministic Algorithms.** We first describe a simple probabilistic algorithm summarizing the method of Section 3.1.

**Algorithm 1.** Probabilistic algorithm.

**Input:** Two sets of regular symmetric matrices $\mathscr{H} = \{H_1 = \mathrm{Id}, \ldots, H_m\} \subseteq \mathbb{L}^{n\times n}$ and $\mathscr{H}' = \{H'_1 = \mathrm{Id}, \ldots, H_m\} \subseteq \mathbb{L}^{n\times n}$.

**Output:** A description of the matrix $A \in \mathrm{GL}_n(\mathbb{L})$ such that $H'_i = A^{\mathrm{T}}H_iA$ for all $1 \leq i \leq m$ or "NoSolution".

Compute the vector subspace $\mathscr{Y} = \{Y \mid \quad H_iY = YH'_i,\ \forall 1 \leq i \leq m\} \subseteq \mathbb{L}^{n\times n}$.
**If** $\mathscr{Y}$ is reduced to the null matrix **then return** "NoSolution"
Pick at random $Y \in \mathscr{Y}$.
Compute $Z = Y^{\mathrm{T}}Y$ and $J = T^{-1}ZT \in \mathbb{L}^{n\times n}$, the Jordan normal form of $Z$ together with $T$.
Compute $G^{-1}$ the inverse of a square root of $J$.
**Return** $YTG^{-1}$ and $T$.

**Theorem 12.** *Algorithm 1 is correct with probability at least* $1 - n/|\mathbb{L}|$ *and runs in polynomial-time.*

*Proof.* The correctness and the polynomial-time complexity of the algorithm come from Section 3.1. After computing $\mathscr{Y}$ and putting the equations defining its matrices in triangular form, one has to pick at random one matrix $Y \in \mathscr{Y}$. By sampling the whole field $\mathbb{L}$ on these free variables, the probability that $\det Y = 0$ is upper bounded by $n/|\mathbb{L}|$ thanks to Schwartz-Zippel-DeMillo-Lipton Lemma [DL78, Zip79]. □

**Remark 13.** Let us recall that the conjugacy problem does not depend on the ground field [dSP10], *i.e.* if there exists $Y \in \mathrm{GL}_n(\mathbb{L}')$, such that $H_iY = YH'_i$, then there exists $Y' \in \mathrm{GL}_n(\mathbb{L})$ such that $H_iY' = Y'H'_i$. This allows us to extend $\mathbb{L}$ to a finite extension in order to decrease the probability of getting a singular matrix $Y$. Thus the success probability of the Algorithm 1 can be amplified to $1 - n/|\mathbb{L}'|$ for any extension $\mathbb{L}' \supseteq \mathbb{L}$. The probability can be then made overwhelming by considering extension of degree $O(n)$. In this case, the algorithm returns the description of a solution on $\mathbb{L}'$. Notice also that

this algorithm can be turned into a deterministic algorithm using Chistov *et al.*'s [CIK97, Theorems 2]. That's is, there is a poly-time algorithm allowing to compute a regular element in $\mathscr{Y}$. Furthermore, if one of the original Hessian matrices is already invertible, the computations of the essential variables of paragraph 2.ii and the search of regular equation of paragraph 2.iii can be done in a deterministic way. Whence, the whole algorithm is deterministic.

The main Theorem 3 summarizes this remark together with Theorem 12.

3.3. **Rational Case.** In this section, we consider the case $\operatorname{char}\mathbb{K} = 0$. The field $\mathbb{K}$ can be thought as $\mathbb{Q}$, a number field $\mathbb{Q}(\alpha_1,\ldots,\alpha_e)$ or even $\mathbb{R}$. In such fields, some of the normalizations proposed in Section 2 cannot be done. We adapt here the normalization process for such fields and then rewrite Proposition 9 according to this situation.

*Reduction to canonical representations.* Let $f_1 = \sum_{i=1}^n \lambda_i \ell_i^2$ be the Gauß reduction of the first polynomial of the instance considered. Unlike paragraph 2.iii, one may not expect to embed $\mathbb{K}$ into $\mathbb{K}\left(\sqrt{\lambda_1},\ldots,\sqrt{\lambda_n}\right)$ for obtaining $f_1 = \sum_{i=1}^n \ell_i'^2$. Indeed, if $\mathbb{K} = \mathbb{Q}$ and if $\lambda_i$ is the $i$th prime integer, this extension has degree $2^n$. Therefore, we only apply Gauß reduction to have $H_1$ non degenerate and diagonal. On the other hand, the process of transforming the Hessian matrices in regular Hessian matrices (paragraph 2.iv) is easier since $\mathbb{K}$ infinite. Indeed, if an Hessian matrix $H_i$ is not invertible, then picking up at random $\lambda \in \mathbb{K}$ will yield an invertible matrix $H_i + \lambda H_1$ with probability 1. All in all, we to find a solution of the `OSMC` problem preserving the quadratic form induced by $H_1$, i.e. a matrix $A$ which verifies the matricial equation $A^{\mathrm{T}} H_1 A = H_1$. Such a matrix $A$ will be called $H_1$-*orthogonal* following [Hig03]. The set of $H_1$-orthogonal matrices is a group denoted by $\mathscr{O}_n(\mathbb{K}, H_1)$. Proposition 9 and Theorem 10 are rephrased as follows:

**Proposition 14.** *Let $(\mathbf{f},\mathbf{g}) \in \mathbb{K}[x_1,\ldots,x_n]^m \times \mathbb{K}[x_1,\ldots,x_n]^m$ be quadratic homogeneous polynomials. We can compute in randomized polynomial time $(\tilde{\mathbf{f}},\tilde{\mathbf{g}}) = \left(\sum_{i=1}^n \lambda_i x_i^2, \tilde{f}_2,\ldots,\tilde{f}_m,\tilde{g}_1,\tilde{g}_2,\ldots,\tilde{g}_m\right) \in \mathbb{K}[\mathbf{x}]^{2m}$, such that $\mathbf{f} \sim \mathbf{g} \iff \tilde{\mathbf{f}} \sim \tilde{\mathbf{g}}$ and the Hessian matrices are all invertible. Furthermore, we can reduce $\tilde{\mathbf{g}}$ to $\bar{\mathbf{g}} = \left(\sum_{i=1}^n \lambda_i x_i^2, \bar{g}_2,\ldots,\bar{g}_m\right) \in \mathbb{K}[x_1,\ldots,x_n]^m$ such that $\mathbf{f} \sim \mathbf{g}$ if, and only if $\tilde{\mathbf{f}} \sim \bar{\mathbf{g}}$ or we cannot and we return "*NoSolution*", $\mathbf{f} \not\sim \mathbf{g}$. Finally, denoting $H_1$ the Hessian matrix of $\tilde{f}_1 = \bar{g}_1$,* `IP1S` *comes down to a $H_1$-Orthogonal Simultaneous Matrix Conjugacy problem,* i.e. *conjugacy by an $H_1$-orthogonal matrix.*

*Proof.* Polynomial $f_1$ being regular, its Gauß reduction must be $\sum_{i=1}^n \lambda_i \ell_i^2$ and we apply the same change of variables on $f_2,\ldots,f_m,g_1,\ldots,g_m$. Then, either $\tilde{g}_1$ has the same reduction as $f_1$ and we apply this change of variables on $\tilde{g}_1,\ldots,\tilde{g}_m$ and obtain $\bar{\mathbf{g}} = (\bar{g}_1 = \tilde{f}_1,\ldots,\bar{g}_m)$ such that $\mathbf{f} \sim \mathbf{g} \iff \tilde{\mathbf{f}} \sim \bar{\mathbf{g}}$. Otherwise, $\tilde{g}_1 \not\sim \tilde{f}_1$, hence $\tilde{\mathbf{f}} \not\sim \tilde{\mathbf{g}}$ and $\mathbf{f} \not\sim \mathbf{g}$.

If $\tilde{\mathbf{f}} \sim \tilde{\mathbf{g}}$, then $A^{\mathrm{T}} H_1 A = H_1$, hence $A$ is $H_1$-orthogonal. Then $A^{\mathrm{T}} H_i A = H_i'$ yields $A^{-1} H_1^{-1} H_i A = H_1^{-1} H_i'$, hence we have an `OSMC` problem by a $H_1$-orthogonal matrix between the two sets $H_1^{-1}\mathscr{H}$ and $H_1^{-1}\mathscr{H}'$ with $\mathscr{H} = \{H_1,\ldots,H_m\}$ and $\mathscr{H}' = \{H_1',\ldots,H_m'\}$. As in the finite field case, it is quite clear that there is a one-to-one correspondence between solutions of `IP1S` and $H_1$-orthogonal solutions of the `OSMC` problem for $H_1^{-1}\mathscr{H}$ and $H_1^{-1}\mathscr{H}'$. □

The classical polar decomposition is used in [CIK97, Theorem 4] to determine an orthogonal solution. Using the analogous decomposition, the so-called Generalized Polar Decomposition (GPD), which depends on $H_1$, yields an $H_1$-orthogonal solution, see [MMT05]. The GPD of a regular matrix $Y$ is the factorization $Y = AW$, with $A$ $H_1$-orthogonal and $W$ in the associated Jordan algebra, *i.e.* $W^{\mathrm{T}} = H_1 W H_1^{-1}$. Let us notice that $A$ and $W$ might be defined only over $\mathbb{L}$ an algebraic extension of $\mathbb{K}$ of some degree.

**Proposition 15.** *Let $\mathscr{K}$ and $\mathscr{K}'$ be two subsets of $m$ matrices in $\mathbb{K}^{n\times n}$. Let $S$ be a regular symmetric matrix. There is a $S$-orthogonal solution $A$ to the conjugacy problem $K_i A = A K_i'$ for all $1 \le i \le m$, if, and only if, there is a regular solution $Y$ to the conjugacy problem $K_i Y = Y K_i'$ and $K_i^{\mathrm{T}} S Y S^{-1} = S Y S^{-1} K_i'^{\mathrm{T}}$ for all $1 \le i \le m$. Furthermore, if $Y = AW$ is the* GPD *of $Y$ with respect to $S$, then $A$ suits.*

*Proof.* This proof is a generalization of [CIK97, Section 3]. If $A$ is an $S$-orthogonal solution to the first problem, then as $A^{\mathrm{T}} = S A^{-1} S^{-1}$, it is clear that $A$ is a solution to the second problem. Conversely, let $Y$ be a solution to the second problem, then $Z = S^{-1} Y^{\mathrm{T}} S Y$ commutes with $K_i'$. As $Y$ is invertible, so is $Z$, therefore, given a determination of the square roots of the eigenvalues of $Z$, there is a unique

matrix $W$ with these eigenvalues such that $W^2 = Z$ and $W$ is in the Jordan algebra associated to $S$, that is $W^{\mathrm{T}} = SWS^{-1}$ (see [MMT05, Theorem 6.2]). As such, $W$ is a polynomial in $Z$ as proven in Appendix A.1 and commutes with $K'_i$.

Finally, $A = YW^{-1}$ is an $S$-orthogonal solution of the first problem for $A^{-1}K_iA = WY^{-1}K_iYW^{-1} = WK'_iW^{-1} = K'_i$, as $W$ commutes with $K'_i$, and

$$A^{\mathrm{T}}SA = W^{-\mathrm{T}}Y^{\mathrm{T}}SYW^{-1} = SW^{-1}S^{-1}Y^{\mathrm{T}}SYW^{-1} = SW^{-\mathrm{T}}ZW^{-1} = S. \qquad \square$$

As one can remark, the equations that one needs to add in Proposition 15 are in fact automatically verified in our case with $S = H_1$, $K_i = H_1^{-1}H_i$ and $K'_i = H_1^{-1}H'_i$ for all $1 \le i \le m$. Indeed, as $H_i$ and $H'_i$ are symmetric, then one has $K_i^{\mathrm{T}}SYS^{-1} = H_iH_1^{-1}H_1YH_1^{-1} = H_iYH_1^{-1}$ and $SYS^{-1}K_i'^{\mathrm{T}} = H_1YH_1^{-1}H'_iH_1^{-1}$. Thus, an equation of the second set reduces to the equation $H_1^{-1}H_iY = YH_1^{-1}H'_i$, and thus $K_iY = YK'_i$.

3.4. **The binary case.** In this section, we investigate fields of characteristic 2. Let $\mathbb{K} = \mathbb{F}_q$ and $(\mathbf{f},\mathbf{g}) \in \mathbb{K}[\mathbf{x}]^m \times \mathbb{K}[\mathbf{x}]^m$. Instead of Hessian matrices, we consider equivalently non symmetric matrices $H_1,\dots,H_m$ and $H'_1,\dots,H'_m$ such that:

$$f_i(\mathbf{x}) = \mathbf{x}^{\mathrm{T}}H_i\mathbf{x},\ g_i(\mathbf{x}) = \mathbf{x}^{\mathrm{T}}H'_i\mathbf{x}, \quad \forall\, 1 \le i \le m.$$

Clearly, if it exists $A \in \mathrm{GL}_n(\mathbb{K})$ such that $\mathbf{g}(\mathbf{x}) = \mathbf{f}(A\cdot\mathbf{x})$, then we also have $H'_i = A^{\mathrm{T}}H_iA$, for all $1 \le i \le m$.

*Reduction to canonical representations.* As in paragraph 2.ii, w.l.o.g. we can assume that $\mathbf{f}$ and $\mathbf{g}$ are regular, that is, $x_1,\dots,x_n$ are the essential variables of both systems. Let us assume there exists a polynomial, let's say $f_1$, in $\mathrm{Span}_{\mathbb{K}}(\mathbf{f})$ which is non-degenerate. As a consequence, we can find linear forms $\ell_1,\dots,\ell_n$ in $\mathbf{x}$ such that (see [LN97, Theorem 6.30]):

(i) if $n$ is odd, $f_1(\mathbf{x}) = \ell_1\ell_2 + \cdots + \ell_{n-2}\ell_{n-1} + \ell_n^2$;
(ii) if $n$ is even, $f_1(\mathbf{x}) = \ell_1\ell_2 + \cdots + \ell_{n-1}\ell_n$ or $f_1(\mathbf{x}) = \ell_1\ell_2 + \cdots + \ell_{n-1}\ell_n + \ell_{n-1}^2 + a\ell_n^2$, where $\mathrm{Tr}_{\mathbb{K}}(a) = a + a^2 + \cdots + a^{q/2} = 1$.

But this yields to $H_1$ non invertible.

We propose a classical change of basis in order to have $H_1$ invertible as in paragraph 2.iii. Let us recall that if $i, i+1 \ne n$, then $x_ix_{i+1} + x_n^2 = x_i^2 + x_ix_{i+1} + x_n^2 + (x_i + x_{i+1} + x_n)^2$, thus by induction, if $n$ is odd, then there exist $\ell_1,\dots,\ell_{n-1},\ell'_n$ such that $f_1(\mathbf{x}) = \ell_1^2 + \ell_1\ell_2 + \ell_2^2 + \cdots + \ell_{n-2}^2 + \ell_{n-2}\ell_{n-1} + \ell_{n-1}^2 + \ell_n^2$ and $H_1$ is invertible. Likewise, for $1 \le i < i+1 < i+2 < i+3 \le n$, $x_i^2 + x_ix_{i+1} + x_{i+1}^2 + x_{i+2}^2 + x_{i+2}x_{i+3} + x_{i+3}^2 = (x_i + x_{i+3})^2(x_i + x_{i+1} + x_{i+3})^2 + (x_{i+1} + x_{i+2})(x_{i+1} + x_{i+2} + x_{i+3})^2$. Thus, if $n$ is even, there exist $\ell'_1,\dots,\ell'_n$ such that

(i) whenever $n/2$ is even, $f_1(\mathbf{x}) = \ell_1^2 + \ell_1\ell_2 + \ell_2^2 + \cdots + \ell_{n-1}^2 + \ell_{n-1}\ell_n + \ell_n^2$ or $f_1(\mathbf{x}) = \ell_1^2 + \ell_1\ell_2 + \ell_2^2 + \cdots + \ell_{n-1}^2 + \ell_{n-1}\ell_n + \ell_{n-1}^2 + a\ell_n^2$, and $H_1$ is invertible;
(ii) whenever $n/2$ is odd, $f_1(\mathbf{x}) = \ell_1^2 + \ell_1\ell_2 + \ell_2^2 + \cdots + \ell_{n-3}^2 + \ell_{n-3}\ell_{n-2} + \ell_{n-2}^2 + \ell_{n-1}\ell_n$ and $H_1$ is not invertible or $f_1(\mathbf{x}) = \ell_1^2 + \ell_1\ell_2 + \ell_2^2 + \cdots + \ell_{n-3}^2 + \ell_{n-3}\ell_{n-2} + \ell_{n-2}^2 + \ell_{n-1}^2 + a\,\ell_n^2$ and $H_1$ is invertible.

We restrict ourselves to the case when $H_1$ is invertible. Following paragraph 2.iv, if $H_i$, $2 \le i \le m$ is singular, we replace it by $H_i + \zeta H_1$. As $\det(H_i + \zeta H_1)$ is a nonzero polynomial of degree $n$ in $\zeta$, should we embed $\mathbb{K}$ into its extension $\mathbb{L}$ of degree $\lceil \log_q(n+1) \rceil$, we can also restrict ourselves to the case wherein $H_1,\dots,H_m$ and $H'_1,\dots,H'_m$ are invertible. Under this conditions, Proposition 9 and Theorem 10 become:

**Proposition 16.** *Let $(\mathbf{f},\mathbf{g}) \in \mathbb{K}[x_1,\dots,x_n]^m \times \mathbb{K}[x_1,\dots,x_n]^m$ be quadratic homogeneous polynomials. We can compute in randomized polynomial time $(\tilde{\mathbf{f}},\tilde{\mathbf{g}}) = (\tilde f, \tilde f_2,\dots,\tilde f_m, \tilde g, \tilde g_2,\dots,\tilde g_m) \in \mathbb{L}[x_1,\dots,x_n]^m \times \mathbb{L}[x_1,\dots,x_n]^m$, where $\mathbb{L}$ is an algebraic extension of $\mathbb{K}$ of degree $O(\log n)$, such that $\mathbf{f} \sim \mathbf{g} \iff \tilde{\mathbf{f}} \sim \tilde{\mathbf{g}}$ and the matrices of the quadratic forms are all invertible. Either we can furthermore reduce $\tilde{\mathbf{g}}$ to $\bar{\mathbf{g}} = (\bar g = \tilde f, \bar g_2,\dots,\bar g_m) \in \mathbb{L}[x_1,\dots,x_n]^m$ such that $\mathbf{f} \sim \mathbf{g}$ if, and only if $\tilde{\mathbf{f}} \sim \bar{\mathbf{g}}$ or we cannot and we return "*NoSolution*", $\mathbf{f} \not\sim \mathbf{g}$. Furthermore, denoting $H_1$ the Hessian matrix of $\tilde f_1 = \tilde g_1$,* `IP1S` *comes down to a $H_1$-Orthogonal Simultaneous Matrix Conjugacy problem,* i.e. *conjugacy by an $H_1$-orthogonal matrix.*

*Proof.* As for the rational case, Proposition 14 in Section 3.3, if the reduction $\tilde f$ of $f_1$ is not also the reduction of $g_1$, then $\mathbf{f} \not\sim \mathbf{g}$. Assuming it is, if $\tilde{\mathbf{f}} \sim \bar{\mathbf{g}}$ by a matrix $A$, then $A^{\mathrm{T}}H_1A = H'_1 = H_1$, hence

$A$ is $H_1$-orthogonal. Likewise, denoting $\mathscr{H} = \{H_1, \ldots, H_m\}$ and $\mathscr{H}' = \{H'_1, \ldots, H'_m\}$, we then have a conjugacy problem between sets $H_1^{-1}\mathscr{H}$ and $H_1^{-1}\mathscr{H}'$. □

Let us notice that, here, matrices $H_i$'s and $H'_i$'s are never symmetric. Therefore, to apply Chistov *et al.*'s Theorem 4 [CIK97, ], one really has to double the set of equations by adding $H_i^{\mathrm{T}}A = AH_i'^{\mathrm{T}}$ for all $i$, $1 \leq i \leq m$. The remaining part is the same as in Section 3.3, except for the computation of the square root of the Jordan normal form $J = T^{-1}ZT$ where $Z = H_1^{-1}Y^{\mathrm{T}}H_1Y$. To the contrary of other characteristics, even if $Z$ is invertible, it might not have any square roots. Even worse, should $Z$ have a square root $W$, $W$ would not need to be a polynomial in $Z$, unless $Z$ is diagonalizable. We give a proof of these results in Appendix A.2. As a consequence, from an algorithmic point a view, one may have to test multiple solutions $Y$ of the conjugacy problem between $H_1^{-1}\mathscr{H}$ and $H_1^{-1}\mathscr{H}'$ before finding one which would yield an orthogonal solution.

## 4. Counting the Solutions: #IP1S

In this part, we present a method for enumerating all the solutions to quadratic-IP1S. According to Proposition 5, this is equivalent to enumerating all the invertible linear transformations on the variables between two sets of quadratic homogeneous polynomials. This allows to provide an upper bound on the number of solutions. We consider in this part quadratic homogeneous instances $(\mathbf{f}, \mathbf{g}) \in \mathbb{K}[\mathbf{x}]^m \times \mathbb{K}[\mathbf{x}]^m$ whose number of essential variables is $n$. If this number is $s < n$, then one can expand the solution matrix with any matrix in $\mathrm{GL}_{n-s}(\mathbb{K})$ (see the proof of Proposition 7).

Let $\mathscr{H} = \{H_1, \ldots, H_m\}$ and $\mathscr{H}' = \{H'_1, \ldots, H'_m\}$ be Hessian matrices in $\mathbb{K}^{n\times n}$ of $\mathbf{f}$ and $\mathbf{g}$ respectively. Our counting problem is equivalent to enumerating the orthogonal matrices $X$ verifying:

$$X^{-1}H_iX = H'_i, \quad \forall i, 1 \leq i \leq m. \tag{5}$$

Let us notice that if $M$ and $N$ are both orthogonal solutions of (5), then $MN^{-1}$ commutes with $\mathscr{H}$ (resp. $MN^{-1}$ commutes with $\mathscr{H}'$). Therefore, computing the cardinal of the set of solutions is equivalent to computing the number of regular elements in the centralizer $\mathscr{C}(\mathscr{H})$ of $\mathscr{H}$.

Let $\alpha$ be an algebraic element of degree $m$ over $\mathbb{K}$ and let $\mathbb{K}' = \mathbb{K}(\alpha)$. We consider the matrix $H = H_1 + \cdots + \alpha^{m-1}H_m \in \mathbb{K}'^{n\times n}$. It is clear that a matrix $X \in \mathbb{K}^{n\times n}$ is such that $X^{-1}H_iX = H_i$ for all $i, 1 \leq i \leq m$ if, and only if, $X^{-1}HX = H$. Hence, the problem again reduces itself to the computation of the centralizer $\mathscr{C}(H)$ of $H$ intersected with $\mathrm{GL}_n(\mathbb{K})$. To ease the analysis, we consider the subspace $\mathscr{V} = \mathscr{C}(H) \cap \mathbb{K}^{n\times n}$ of matrices in $\mathbb{K}^{n\times n}$ commuting with $H$. This provides an upper bound on the number of solutions. The dimension of $\mathscr{V}$ as a $\mathbb{K}$-vector space is upper bounded by the dimension of $\mathscr{C}(H)$ as a $\mathbb{K}'$-vector space. Indeed, $\mathscr{V} \otimes \mathbb{K}' \subseteq \mathscr{C}(H)$, hence $\dim_{\mathbb{K}} \mathscr{V} = \dim_{\mathbb{K}'}(\mathscr{V} \otimes \mathbb{K}') \leq \dim_{\mathbb{K}'} \mathscr{C}(H)$. Since we only want the cardinal of the centralizer of $H$, we can restrict our attention to the centralizer of the normal Jordan form $D$ of $H$ defined over a field $\mathbb{L}$. This means that $D$ is a block diagonal matrix wherein each block is a Jordan matrix $J_{\lambda,s}$ (*i.e.* an upper triangular matrix of size $s \times s$ whose diagonal elements are $\lambda$ and the elements just above the diagonal are 1).

We recall that a matrix $X$ which commutes with a Jordan matrix $J$ of size $s$ is an upper triangular Toeplitz matrix of size $s \times s$. Indeed, $XJ - JX$ is as such

$$XJ - JX = \begin{pmatrix} -x_{2,1} & x_{1,1}-x_{2,2} & \cdots & x_{1,n-1}-x_{2,n} \\ \vdots & \vdots & & \vdots \\ -x_{n,1} & x_{n-1,1}-x_{n,2} & \cdots & x_{n-1,n-1}-x_{n,n} \\ 0 & x_{n,1} & \cdots & x_{n,n-1} \end{pmatrix} = 0.$$

This is used in the following theorem to compute the centralizer of a Jordan normal form.

**Theorem 17.** *Let $D$ be a Jordan normal form. Let us denote $J_{\lambda_i,s_i} = D_i$ the $i$th block of $D$ for $1 \leq i \leq r$. Let $X = (X_{i,j})_{1\leq i,j\leq r}$ be a block-matrix, with $X_{i,j} \in \mathbb{L}(\lambda_1, \ldots, \lambda_r)^{s_i \times s_j}$, that commutes with $D$. If $\lambda_i = \lambda_j$, then $X_{i,j}$ is an upper triangular Toeplitz matrix whose non necessary zero coefficients are the one on the last $\min(s_i, s_j)$ diagonals starting from to the top-right corner. Otherwise, $X_{i,j} = 0$.*

*Proof.* We assume that $r = 2$. If $XD - DX = \begin{pmatrix} X_{1,1}D_1 - D_1X_{1,1} & X_{1,2}D_2 - D_1X_{1,2} \\ X_{2,1}D_1 - D_2X_{2,1} & X_{2,2}D_1 - D_1X_{2,2} \end{pmatrix} = 0$, then $X_{1,1}$ commutes with $D_1 = J_{\lambda_1,s_1}$ and $X_{2,2}$ with $D_2 = J_{\lambda_2,s_2}$. Thus they are upper triangular Toeplitz matrices.

From $X_{2,1}D_2 - D_1X_{2,2}$, one deduces that $(\lambda_1 - \lambda_2)x_{s_1+s_2,1} = 0$, hence either $\lambda_1 = \lambda_2$ or $x_{s_1+s_2,1} = 0$. If $\lambda_1 \neq \lambda_2$, then step by step, one has $X_{1,2} = 0$. Assuming $\lambda_1 = \lambda_2$, then step by step, one has $x_{s_1+i,1} = 0$ for $i > 1$ and since $x_{s_1+i+1,j+1} - x_{s_1+i,j} = 0$ for all $i, j$, one has in fact that $X_{1,2}$ is a upper triangular Toeplitz matrix with potential nonzero coefficients on the last $\min(s_1, s_2)$ diagonals starting from the top-right corner. The same argument applies to $X_{2,1}$.

The case $r > 2$ is an easy generalization of this result. □

Since the centralizer of a matrix is a vector subspace, this characterization of the centralizer allows us to determine an upper bound for its dimension.

**Proposition 18** (Proposition 4)**.** *Let $H \in \mathbb{K}'^{n\times n}$ be a matrix and let $D$ be its normal Jordan form. Assuming the blocks of $D$ are $J_{\lambda_1,s_{1,1}}, \ldots, J_{\lambda_1,s_{1,d_1}}, \ldots, J_{\lambda_r,s_{r,1}}, \ldots, J_{\lambda_r,s_{r,d_r}}$, then the centralizer of $H$ is a $\mathbb{K}'$-vector subspace of $\mathbb{K}'^{n\times n}$ of dimension no more than $\sum_{1\leq i\leq r}\sum_{1\leq j\leq d_i}(2d_i - 2j + 1)s_{i,j}$.*

*Proof.* Let $\mathbb{L}$ be the smallest field over which $D$ is defined. It is clear that the centralizer of $H$ over $\mathbb{L}$, denoted $\mathscr{W}$, contains $\mathscr{C}(H) \otimes \mathbb{L}$. Hence, $\dim_{\mathbb{K}'} \mathscr{C}(H) = \dim_{\mathbb{L}}(\mathscr{C}(H) \otimes \mathbb{L}) \leq \dim_{\mathbb{L}} \mathscr{W}$.

Now, let $X = (X_{i,j})_{1\leq i,j\leq d_1+\cdots+d_r} \in \mathscr{V}$ and let us assume that for all $i$, the sequences $(s_{i,1}, \ldots, s_{i,d_i})$ are increasing. From Theorem 17, there are $\sum_{1\leq i\leq r}\sum_{1\leq j\leq d_i} s_{i,j}$ free parameters for the diagonal blocks of $X$ and $2\sum_{1\leq i\leq r}\sum_{1\leq j<k\leq d_i}\min(s_{i,j}, s_{i,k}) = 2\sum_{1\leq i\leq r}\sum_{1\leq j\leq d_i}(d_i - j)s_{i,j}$ free parameters for the off-diagonal blocks of $X$. This concludes the proof. □

As a consequence, if $q$ is an odd prime power, then the number of solutions of quadratic-IP1S in $\mathbb{F}_q^{n\times n}$ is bounded from above by:

$$q^{\left(\sum_{1\leq i\leq r}\sum_{1\leq j\leq d_i}(2d_i-2j+1)s_{i,j}\right)} - 1.$$

As mentioned in the introduction, the counting problem considered here is related to cryptographic concerns. It corresponds to evaluating the number of equivalent secret-keys in MPKC [FLPW12, WP05, WP11]. In particular, [FLPW12] proposes an "ad-hoc" method for solving a particular instance of #IP1S. An interesting open question would be to revisit the results from [FLPW12] with our approach.

## 5. Special Case of the general IP Problem

In this part, we present a randomized polynomial-time algorithm for solving the following task:
**Input:** $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{K}[x_1, \ldots, x_n]^n$, and $\mathbf{POW}_{n,d} = (x_1^d, \ldots, x_n^d) \in \mathbb{K}[x_1, \ldots, x_n]^m$ for some $d > 0$.
**Question:** find – if any – $(A, B) \in \mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_m(\mathbb{K})$ such that:

$$\mathbf{g} = B \cdot \mathbf{POW}_{n,d}(A \cdot \mathbf{x}), \text{ with } \mathbf{x} = (x_1, \ldots, x_n)^{\mathrm{T}}.$$

In [Kay11], Kayal proposed a randomized polynomial-time algorithm for solving the problem below when $B$ is the identity matrix and $m = 1$. We generalize this result to $m = n$ with an additional transformation on the polynomials. As in [Kay11, Per05], we use partial derivatives to extract the matrices $A$ and $B$. The idea is to factorize the Jacobian (whereas [Kay11] uses the Hessian matrix) matrix of $\mathbf{g}$ at $\mathbf{x}$ which is defined as follows:

$$\mathrm{J}_{\mathbf{g}}(\mathbf{x}) = \left\{\partial_j g_i = \frac{\partial g_i}{\partial x_j}\right\}_{1\leq i\leq m}^{1\leq j\leq n}.$$

According to the following lemma, the Jacobian matrix is especially useful in our context:

**Lemma 19.** *Let $\big(\mathbf{f} = (f_1, \ldots, f_m), \mathbf{g} = (g_1, \ldots, g_m)\big) \in \mathbb{K}[x_1, \ldots, x_n]^m \times \mathbb{K}[x_1, \ldots, x_n]^m$. If there exists $(A, B) \in \mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_n(\mathbb{K})$ such that $\mathbf{g} = B \cdot \mathbf{f}(A \cdot \mathbf{x})$, then:*

$$\mathrm{J}_{\mathbf{g}}(\mathbf{x}) = B \cdot \mathrm{J}_{\mathbf{f}}(A \cdot x) \cdot A.$$

*As a consequence,* $\det\big(\mathrm{J}_{\mathbf{g}}(\mathbf{x})\big) = \det(A) \cdot \det(B) \cdot \det\big(\mathrm{J}_{\mathbf{f}}(A \cdot x)\big)$.

The Jacobian matrix of $\mathbf{f} = \mathbf{POW}_{n,d}(\mathbf{x})$ is a diagonal matrix whose diagonal elements are $\big(\mathrm{J}_{\mathbf{f}}(\mathbf{x})\big)_{i,i} = d \cdot x_i^{d-1}, \forall\, i \leq i \leq n$. Thus:

$$\det\big(\mathrm{J}_{\mathbf{POW}_{n,d}}(\mathbf{x})\big) = d^n \prod_{i=1}^{n} x_i^{d-1}.$$

This gives:

**Lemma 20.** *Let* $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{K}[x_1, \ldots, x_n]^n$. *Let* $d > 0$ *be an integer, and define* $\mathbf{POW}_{n,d} = (x_1^d, \ldots, x_n^d) \in \mathbb{K}[x_1, \ldots, x_n]^m$. *If there exists* $(A, B) \in \mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_n(\mathbb{K})$ *such that* $\mathbf{g}(\mathbf{x}) = B \cdot \mathbf{POW}_{n,d}(A \cdot \mathbf{x})$, *then:*

$$\mathrm{J}_{\mathbf{g}}(\mathbf{x}) = c \cdot \prod_{i=1}^{n} \ell_i(\mathbf{x})^{d-1},$$

*with* $c \in \mathbb{K} \setminus \{0\}$, *and where the* $\ell_i$*'s are linear forms whose coefficients are the ith rows of* $A$.

*Proof.* According to Lemma 19, $\det\big(\mathrm{J}_{\mathbf{g}}(\mathbf{x})\big) = \det(A) \cdot \det(B) \cdot d^n \cdot \prod_{i=1}^{n} \ell_i(\mathbf{x})^{d-1}$. □

From this lemma, we can derive a randomized polynomial-time algorithm for solving IP on $(f = \mathbf{POW}_{n,d}, \mathbf{g}) \in \mathbb{K}[x_1, \ldots, x_n]^n \times \mathbb{K}[x_1, \ldots, x_n]^n$. It suffices to use Kaltofen's algorithm [Kal89] for factoring $\det\big(\mathrm{J}_{\mathbf{g}}(\mathbf{x})\big)$ in randomized polynomial time. This allows us to recover – if any – the change of variable $A$. The matrix $B$ can be then recovered by linear algebra, *i.e.* solving a linear system of equations. This proves the result announced in the introduction for IP, that is Theorem 1.

## REFERENCES


[AS06] 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.

[Ba11] Alessandra Bernardi and Monica and, Alessandro Gimigliano Idà. Computing symmetric rank for symmetric tensors. *J. Symb. Comput.*, 46(1):34–53, 2011.

[BFL13] Arnab Bhattacharyya, Eldar Fischer, and Shachar Lovett. Testing low complexity affine-invariant properties. In Khanna [Kha13], pages 1337–1355.

[BFV13] 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.

[BHM10] Jérémy Berthomieu, Pascal Hivert, and Hussein Mourtada. Computing Hironaka's invariants: Ridge and Directrix. In *Arithmetic, Geometry, Cryptography and Coding Theory 2009*, volume 521 of *Contemp. Math.*, pages 9–20. Amer. Math. Soc., Providence, RI, 2010.

[BI11] Peter Bürgisser and Christian Ikenmeyer. Geometric complexity theory and tensor rank. In Lance Fortnow and Salil P. Vadhan, editors, *STOC*, pages 509–518. ACM, 2011.

[BI13] Peter Bürgisser and Christian Ikenmeyer. Explicit lower bounds via geometric complexity theory. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *STOC*, pages 141–150. ACM, 2013.

[Bür12] Peter Bürgisser. Prospects for geometric complexity theory. In *IEEE Conference on Computational Complexity*, page 235. IEEE, 2012.

[Cai94] Jin-yi Cai. Computing Jordan Normal forms Exactly for Commuting Matrices in Polynomial Ttime. *International Journal of Foundations of Computer Science*, 05(03n04):293–302, 1994.

[Car05] Enrico Carlini. Reducing the number of variables of a polynomial. In *Algebraic geometry and geometric modeling*, pages 237–247. Springer, 2005.

[CGLM08] Pierre Comon, Gene H. Golub, Lek-Heng Lim, and Bernard Mourrain. Symmetric tensors and symmetric tensor rank. *SIAM J. Matrix Analysis Applications*, 30(3):1254–1279, 2008.

[CIK97] Alexander L. Chistov, Gábor Ivanyos, and Marek Karpinski. Polynomial time algorithms for modules over finite dimensional algebras. In Bruce W. Char, Paul S. Wang, and Wolfgang Küchlin, editors, *ISSAC*, pages 68–74. ACM, 1997.

[CKW11] Xi Chen, Neeraj Kayal, and Avi Wigderson. Partial derivatives in arithmetic complexity and beyond. *Foundations and Trends in Theoretical Computer Science*, 6(1-2):1–138, 2011.

[CU13] Henry Cohn and Christopher Umans. Fast matrix multiplication using coherent configurations. In Khanna [Kha13], pages 1074–1087.

[DL78] Richard DeMillo and Richard Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):192–194, 1978.

[dSP10] Clément de Seguins Pazzis. Invariance of simultaneous similarity and equivalence of matrices under extension of the ground field. *Linear Algebra and its Applications*, 433(3):618 – 624, 2010.

[Edm67] Jack Edmonds. Systems of distinct representatives and linear algebra. *Journal of Research of the National Bureau of Standards*, 718(4):242 – 245, 1967.

[FLPW12] Jean-Charles Faugère, Dongdai Lin, Ludovic Perret, and Tianze Wang. On enumeration of polynomial equivalence classes and their application to MPKC. *Finite Fields and Their Applications*, 18(2):283 – 302, 2012.

[FP06] 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.

[Gan59] F.R. Gantmacher. *The Theory of Matrices, Vol. 1*. Chelsea, 1959.

[Gir72] Jean Giraud. *Étude locale des singularités*. U.E.R. Mathématique, Université Paris XI, Orsay, 1972. Cours de 3ème cycle, 1971–1972, Publications Mathématiques d'Orsay, No. 26.

[GT09] Ben Joseph Green and Terence Tao. The distribution of polynomials over finite fields, with applications to the gowers norms. *Contributions to Discrete Mathematics*, 4(2), 2009.

[GWX13] Elena Grigorescu, Karl Wimmer, and Ning Xie. Tight lower bounds for testing linear isomorphism. *Electronic Colloquium on Computational Complexity (ECCC)*, page 17, 2013.

[Hig03] Nicholas J. Higham. *J*-orthogonal matrices: properties and generation. *SIAM Rev.*, 45(3):504–519 (electronic), 2003.

[Hir70] Heisuke Hironaka. Additive groups associated with points of a projective space. *Ann. of Math. (2)*, 92:327–334, 1970.

[HKM05] Nicholas J. A. Harvey, David R. Karger, and Kazuo Murota. Deterministic network coding by matrix completion. In *SODA*, pages 489–498. SIAM, 2005.

[HKY06] Nicholas J. A. Harvey, David R. Karger, and Sergey Yekhanin. The complexity of matrix completion. In *SODA*, pages 1103–1111. ACM Press, 2006.

[Kal89] Erich Kaltofen. Factorization of polynomials given by straight-line programs. In *Randomness and Computation*, pages 375–412. JAI Press, 1989.

[Kay11] Neeraj Kayal. Efficient algorithms for some special cases of the polynomial equivalence problem. In *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1409–1421, Philadelphia, PA, 2011. SIAM.

[Kay12] Neeraj Kayal. Affine projections of polynomials: extended abstract. In Howard J. Karloff and Toniann Pitassi, editors, *STOC*, pages 643–662. ACM, 2012.

[Kha13] Sanjeev Khanna, editor. *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2013, New Orleans, Louisiana, USA, January 6-8, 2013*. SIAM, 2013.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[LN97] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[Lov79] László Lovász. On determinants, matchings, and random algorithms. In *FCT*, pages 565–574, 1979.

[Mat02] K. R. Matthews. A rational canonical form algorithm, 2002.

[MI88] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Advances in Cryptology – EUROCRYPT 1988*, volume 330 of *LNCS*, pages 419–453. Springer–Verlag, 1988.

[MMT05] D. Steven Mackey, Niloufer Mackey, and Françoise Tisseur. Structured factorizations in scalar product spaces. *SIAM J. Matrix Anal. Appl.*, 27(3):821–850, 2005.

[MS01] Ketan Mulmuley and Milind A. Sohoni. Geometric complexity theory i: An approach to the p vs. np and related problems. *SIAM J. Comput.*, 31(2):496–526, 2001.

[Mul12] Ketan Mulmuley. The gct program toward the *p* vs. *np* problem. *Commun. ACM*, 55(6):98–107, 2012.

[New67] Morris Newman. Two classical theorems on commuting matrices. *J. Res. Nat. Bur. Standards Sect. B*, 71B:69–71, 1967.

[Pat96a] 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.

[Pat96b] Jacques Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In *EUROCRYPT*, pages 33–48, 1996. Extended version available on `http://www.minrank.org/hfe.pdf`.

[Per04] Ludovic Perret. On the computational complexity of some equivalence problems of polynomial systems of equations over finite fields. *Electronic Colloquium on Computational Complexity (ECCC)*, 116, 2004.

[Per05] 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.

[PGC98] 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.

[Sax06] Nitin Saxena. *Morphisms of Rings and Applications to Complexity*. PhD thesis, INDIAN INSTITUTE OF TECHNOLOGY KANPUR, June 2006.

[Sto98] Arne Storjohann. An $O(n^3)$ algorithm for the Frobenius normal form. In *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, ISSAC '98, pages 101–105, New York, NY, USA, 1998. ACM.

[TX12] Shaohua Tang and Lingling Xu. Proxy signature scheme based on isomorphisms of polynomials. In Li Xu, Elisa Bertino, and Yi Mu, editors, *NSS*, volume 7645 of *Lecture Notes in Computer Science*, pages 113–125. Springer, 2012.

[TX13] Shaohua Tang and Lingling Xu. Towards provably secure proxy signature scheme based on isomorphisms of polynomials. *Future Generation Computer Systems*, (0):–, 2013.

[Val79] Leslie G. Valiant. The complexity of computing the permanent. *Theor. Comput. Sci.*, 8:189–201, 1979.

[vzGG99] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 1999.

[WP05] Christopher Wolf and Bart Preneel. Large superfluous keys in multivariate quadratic asymmetric systems. In *Public Key Cryptography – PKC 2005*, volume 3386 of *LNCS*, pages 275–287. Springer, 2005.

[WP11] Christopher Wolf and Bart Preneel. Equivalent keys in multivariate quadratic public key systems. *Journal of Mathematical Cryptology*, 4(4):375–415, 2011.

[YTY11] Guangdong Yang, Shaohua Tang, and Li Yang. A novel group signature scheme based on mpkc. In Feng Bao and Jian Weng, editors, *ISPEC*, volume 6672 of *Lecture Notes in Computer Science*, pages 181–195. Springer, 2011.

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation (EUROSAM'79), Internat. Sympos.*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer Verlag, 1979.

## APPENDIX A. SQUARE ROOT OF A MATRIX

In this appendix, we present further algorithms for computing the square root of a matrix. We use the same notation as in Section 3. A square root of a regular matrix $Z$ is a matrix whose square is $Z$. In the first subsection, we deal with some properties of the square root of a matrix in characteristic not 2. In particular, we show that a regular matrix $Z$ always has a square root which is a polynomial in $Z$. In the second subsection, we consider the case of characteristic 2. Let us recall that whenever $Z$ is not diagonalizable, then $Z$ might have a square root but it is never a polynomial in $Z$. We give some examples of such matrices $Z$. Lastly, we propose an alternative to the method of Section 3 for computing the square root of a matrix in polynomial time for any field of characteristic $p \geq 2$.

### A.1. The square root as a polynomial in characteristic not 2.

In this section, we prove that a regular matrix always has a square root which is a polynomial in considered matrix. More specifically, we shall prove the following result.

**Proposition 21.** *Let $Z \in \mathbb{K}^{n\times n}$ be a regular matrix whose eigenvalues are $\zeta_1, \ldots, \zeta_r$. There exists $W$ a square root of $Z$ whose eigenvalues $\omega_1, \ldots, \omega_r$ verify $\omega_i^2 = \zeta_i$ for all $1 \leq i \leq r$. Furthermore, $W$ is a polynomial in $Z$ with coefficients in $\mathbb{K}(\omega_1, \ldots, \omega_r)$.*

*Proof.* We shall prove this proposition incrementally. First, we shall assume that $Z$ only has simple eigenvalues, then that it is diagonalizable and finally that it is any regular matrix.

Whenever $Z \in \mathbb{K}^{n\times n}$ only has simple eigenvalues $\zeta_1, \ldots, \zeta_n$, then it is similar to the diagonal matrix $D$ whose entries are the $\zeta_i$'s. Let $C$ be a diagonal matrix whose coefficients are the $\omega_i$'s. Matrix $C$ is a polynomial $P(D)$ if, and only if, there exists $p_0, \ldots, p_{n-1}$ such that

$$\begin{pmatrix} \omega_1 & & 0 \\ & \ddots & \\ 0 & & \omega_n \end{pmatrix} = \begin{pmatrix} p_0 + p_1\zeta_1 + \cdots + p_{n-1}\zeta_1^{n-1} & & 0 \\ & \ddots & \\ 0 & & p_0 + p_1\zeta_n + \cdots + p_{n-1}\zeta_n^{n-1} \end{pmatrix}.$$

Since $\zeta_1, \ldots, \zeta_n$ are pairwise distinct, then this Vandermonde system is invertible over $\mathbb{K}(\omega_1, \ldots, \omega_n)$ and thus has a solution. Let us remark that no choice of the determination of the square root is needed.

Whenever $Z$ has eigenvalues with multiplicity but is diagonalizable, then one must be careful for the choices of the square roots. For instance, although $W = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ is a square root of $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, it is not a polynomial in $Z$ over $\mathbb{K}$. One must choose by advance a determination of the square roots and must stick to it for each eigenvalue. This means, that if $\zeta_1 = \zeta_2$, then $\omega_1 = \omega_2$. In this case, considering only the eigenvalues that are different, the computation of $W$ comes down naturally to the simple eigenvalues case.

Let us assume that $Z$ is similar to a single Jordan block $J$ for eigenvalue $\zeta \neq 0$ and let $\omega$ be a square root of $\zeta$. Remarking that $J - \zeta\mathrm{Id}$ is a upper triangular nilpotent matrix and that $\binom{1/2}{k}$ is well-defined in $\mathbb{K}$ for $\mathrm{char}\,\mathbb{K} \neq 2$ and $k \geq 0$, then a square root $G$ of $J$ can be computed as follows:

$$G = \sqrt{J} = \omega\sqrt{\mathrm{Id} + \frac{1}{\omega^2}(J - \zeta\mathrm{Id})} = \omega\left(\mathrm{Id} + \frac{1}{2}\frac{1}{\omega^2}(J - \zeta\mathrm{Id}) - \frac{3}{8}\frac{1}{\omega^4}(J - \zeta\mathrm{Id})^2 + \cdots\right),$$

where this Taylor expansion is in fact a polynomial in $J$. As such, $G$ is the upper triangular matrix such that for all $1 \le i \le n$, $i \le j \le n$, the element at row $i$ and column $j$ is $\binom{1/2}{j-i}\omega^{1-2(j-i)}$. Let us remark that if $J$ is a Jordan block of size at least 2 for eigenvalue $\zeta = 0$, then $J$ has no square roots.

Let $Z$ be any regular matrix whose Jordan normal form $J$ is made of blocks $J_1 \ldots, J_r$ for eigenvalues $\zeta_1, \ldots, \zeta_r$. Let $G$ be a block diagonal matrix with blocks $G_1, \ldots, G_r$ being square roots of $J_1, \ldots, J_r$ with eigenvalues $\omega_1, \ldots, \omega_r$ such that $\zeta_i = \zeta_j \Rightarrow \omega_i = \omega_j$. Obviously $G$ is a square root of $J$ and it remains to prove that $G$ is a polynomial $P(J)$. Assuming $J_1$ has size $d_1 + 1, \ldots, J_r$ has size $d_r + 1$, then finding $P$ comes down to interpolate $P$ knowing that $P(\zeta_1) = \omega_1, \ldots, P^{(d_1)}(\zeta_1) = \binom{1/2}{d_1}\omega^{1-2d_1}, \ldots, P(\zeta_r) = \omega_r, \ldots, P^{(d_r)}(\zeta_r) = \binom{1/2}{d_r}\omega^{1-2d_r}$ and such a $P$ can always be found. For instance, if $\zeta_1$ is an eigenvalue with *algebraic* multiplicity 2 but *geometric* multiplicity 1 and if $\zeta_2$ has multiplicity 1, then one would have to interpolate a polynomial $P(z) = p_0 + p_1 z + p_2 z^2$ such that

$$\begin{pmatrix} \omega_1 & \frac{1}{2\omega_1} & 0 \\ 0 & \omega_1 & 0 \\ 0 & 0 & \omega_2 \end{pmatrix} = \begin{pmatrix} p_0 + p_1\zeta_1 + p_2\zeta_1^2 & p_1 + 2p_2\zeta_1 & 0 \\ 0 & p_0 + p_1\zeta_1 + p_2\zeta_1^2 & 0 \\ 0 & 0 & p_0 + p_1\zeta_2 + p_2\zeta_2^2 \end{pmatrix}$$
$$= \begin{pmatrix} P(\zeta_1) & P'(\zeta_1) & 0 \\ 0 & P(\zeta_1) & 0 \\ 0 & 0 & P(\zeta_2) \end{pmatrix},$$

and this system has a unique solution since $\zeta_1 \neq \zeta_2$. Remark that if $\omega_1 = \omega_2$, then there is also a unique $P$ of degree 1 verifying the equation above.

Finally, once one has $P$ such that $P(J) = G$, then it is clear that $P(Z) = W$ with $W^2 = Z$. □

A.2. **Matrices with square roots in characteristic** 2**.** In this section, we consider the trickier case of computing the square root of a matrix over a field $\mathbb{K}$ with $\operatorname{char}\mathbb{K} = 2$. Unfortunately, unlike other characteristics, a regular matrix has not necessarily a square root over $\bar{\mathbb{K}}$. In fact, any Jordan block of size at least 2 does not have any square root. This is mainly coming from the fact that generalized binomial coefficients $\binom{1/2}{k}$ are meaningless in characteristic 2.

**Proposition 22.** *Let $Z \in \mathbb{K}^{n\times n}$ be a Jordan normal form with blocks $J_1, \ldots, J_r$ of sizes $d_1, \ldots, d_r \ge 2$, associated to eigenvalues $\zeta_1, \ldots, \zeta_r$ and blocks of sizes 1 with eigenvalues $\upsilon_1, \ldots, \upsilon_s$. We assume that $J_1, \ldots, J_r$ are ordered by decreasing sizes and then eigenvalues. Matrix $Z$ has a square root $W$ if, and only if, $d_1 - d_2 \le 1$ and $\zeta_1 = \zeta_2$, $d_3 - d_4 \le 1$ and $\zeta_3 = \zeta_4$,* etc. *and if for each $J_i$ of size 2 that is not paired with $J_{i-1}$ or $J_{i+1}$, then there exists a $j$ such that $\upsilon_j = \zeta_i$.*

Before, proving this result, we give some example of matrices with or without square root. Following matrices $J$ and $J'$ have square roots $K$ and $K'$, while $J''$ and $J'''$ do not have any:

$$J = \begin{pmatrix} \zeta & 0 & 0 \\ 0 & \zeta & 1 \\ 0 & 0 & \zeta \end{pmatrix}, \quad K = \begin{pmatrix} \zeta & 0 & x \\ \frac{1}{x} & \zeta & y \\ 0 & 0 & \zeta \end{pmatrix},$$
$$J' = \begin{pmatrix} \zeta & 1 & 0 & 0 \\ 0 & \zeta & 0 & 0 \\ 0 & 0 & \zeta & 1 \\ 0 & 0 & 0 & \zeta \end{pmatrix}, \quad K'_1 = \begin{pmatrix} \zeta & x & 0 & y \\ 0 & \zeta & 0 & 0 \\ \frac{1}{y} & z & \zeta & x \\ 0 & \frac{1}{y} & 0 & \zeta \end{pmatrix}, \quad K'_2 = \begin{pmatrix} \zeta & x & y & z \\ 0 & \zeta & 0 & y \\ 0 & \frac{1}{y} & \zeta & x \\ 0 & 0 & 0 & \zeta \end{pmatrix},$$
$$J'' = \begin{pmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta & 1 & 0 \\ 0 & 0 & \zeta & 1 \\ 0 & 0 & 0 & \zeta \end{pmatrix}, \quad J''' = \begin{pmatrix} \zeta & 1 & 0 & 0 & 0 & 0 \\ 0 & \zeta & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta & 1 & 0 & 0 \\ 0 & 0 & 0 & \zeta & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta & 1 \\ 0 & 0 & 0 & 0 & 0 & \zeta \end{pmatrix}.$$

As one can see, none of $K$, $K'_1$ and $K'_2$ are polynomials in $J$ or $J'$ because of the non zero subdiagonal elements $1/x$ and $1/y$.

*Proof.* Let $J$ be a Jordan block of size $d$ associated to eigenvalue $\zeta$. Then $J^2-\zeta^2\mathrm{Id} = \begin{pmatrix} 0 & \mathrm{Id}_{d-2} \\ 0_2 & 0 \end{pmatrix}$ and one can deduce that $\zeta^2$ is the sole eigenvalue of $J^2$ but that its geometric multiplicity is 2. Hence the Jordan normal form of $J^2$ is made of two Jordan blocks.

As $(J-\zeta\mathrm{Id})^d = 0$ and $(J-\zeta\mathrm{Id})^e \neq 0$ for all $e < d$, then $\left(J^2-\zeta^2\mathrm{Id}\right)^{\lceil d/2\rceil} = 0$ and $\left(J^2-\zeta^2\mathrm{Id}\right)^e \neq 0$ for $e < \lceil d/2\rceil$, *i.e.* $e < d/2$ if $d$ is even and $e < (d+1)/2$ if $d$ is odd. Thus the Jordan normal form of $J^2$ has a block of size exactly $\lceil d/2\rceil$. That is, if $d$ is even, both blocks have size $d/2$ and if $d$ is odd, one block has size $(d+1)/2$ and the other block has size $(d-1)/2$.

By this result, if $Z$ is a square, then one must be able to pair up its Jordan blocks with same eigenvalue $\zeta$ so that the sizes differ by at most 1. The blocks that need not being paired being the blocks of size 1.

Conversely, assuming one can pair up the Jordan blocks of $Z$ with same eigenvalue $\zeta$ so that the sizes differ by at most 1 and the remaining blocks have sizes 1. Then, each pair of blocks is the Jordan normal form of the square of a Jordan block of size the sum of the sizes and eigenvalue $\sqrt{\zeta}$. Furthermore, each alone block of size 1 associated with $\zeta$ is the square of the block of size 1 associated with $\sqrt{\zeta}$.

Finally, let us prove that if $W^2 = Z$ and $Z$ is not diagonalizable, then $W$ is not a polynomial in $Z$. Let $J$ be the normal Jordan form of $Z$ blocks $J_1,\dots,J_r$, a polynomial $P(J)$ is also block diagonal with blocks $P(J_1),\dots,P(J_r)$. Thus, if $P(J)^2 = J$, then $P(J_i)^2 = J_i$ for all $1 \leq i \leq r$, which is false, unless $J_i$ has size 1. □

A.3. **Computation in characteristic $p \geq 2$.** In this part, we present an alternative method to the one presented in Section 3.1. We aim at diminishing the number of variables needed in the expression of the square root. However, this method does not work in characteristic 0. For the time being, we consider $\mathrm{char}\,\mathbb{K} > 2$. However, we shall see below how to adapt this method to the characteristic 2.

The idea is still to perform a change of basis $T$ over $\mathbb{K}$ so that $C = T^{-1}ZT$ has an easily computable square root. This matrix $C$ is the *generalized Jordan normal form*, also known as the *primary rational canonical form* of $Z$. As the classical Jordan normal form, if $Z$ is diagonalizable over $\bar{\mathbb{K}}$, then $C$ is block diagonal, otherwise it is a block lower triangular matrix. Its diagonal blocks are companion matrices $C(P_1),\dots,C(P_r)$ of irreducible polynomials $P_1,\dots,P_r$. Subdiagonal blocks are zero matrices with eventually a 1 on the top-right corner, if the geometric multiplicity associated to roots of one the $P_i$ is not large enough. In other words, it gathers $d$ conjugated eigenvalues in one block of size $d$ which is the companion matrix of their shared minimal polynomial. Let us remark that computing such a normal form can be done in polynomial time [Mat02, Sto98] and that the change of basis matrix $T$ is defined over $\mathbb{K}$. Thus, after computing a square root of $C'$ of $C$, one can retrieve $W$ and $M$ in $O(n^\omega)$ operations in the field of coefficients of $C'$. Furthermore, computing a square root of $C$ is equivalent to computing the square root of each companion matrix. Finally, using the same argument as for the more classical Jordan normal form in Appendix A.1, $C'$ is a polynomial in $C$. In the following, we only show how to determine the square root of a companion matrix $C(P)$, for an irreducible $P$.

Let $P = x^d + p_{d-1}x^{d-1} + \cdots + p_0$, let us recall that the companion matrix of $P$ is

$$C(P) = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ -p_0 & -p_1 & \cdots & -p_{d-1} \end{pmatrix}.$$

If polynomial $P$ can be decomposed as $P(z) = (z-\alpha_0)\cdots(z-\alpha_{d-1})$, then we want to find a polynomial $Q$ such that $Q(z) = (z-\beta_0)\cdots(z-\beta_{d-1})$, where $\beta_i^2 = \alpha_i$ for all $0 \leq i \leq d-1$. Let us notice that

$$P(z^2) = (z^2-\beta_0)\cdots(z^2-\beta_{d-1}) = Q(z)(z+\beta_0)\cdots(z+\beta_{d-1}) = (-1)^d Q(z)Q(-z).$$

As a consequence, the characteristic polynomial of $C(Q)^2$ is

$$\det(\lambda\mathrm{Id} - C(Q)^2) = \det(\sqrt{\lambda}-C(Q))\det(\sqrt{\lambda}+C(Q)) = (-1)^d Q(\sqrt{\lambda})Q(-\sqrt{\lambda}) = P(\lambda).$$

But since $P$ is irreducible over $\mathbb{K}$, by the invariant factors theory, then $C(Q)^2$ must be similar to the companion matrix $C(P)$.

As $P$ is irreducible over $\mathbb{K} = \mathbb{F}_q$, up to reindexing the roots of $P$, the conjugates $\alpha_1,\dots,\alpha_{d-1}$ of $\alpha_0$ are just its iterated $q$th powers. Denoting $\mathbb{L} = \mathbb{K}[x]/(P(x)) = \mathbb{F}_{q^d}$, let us assume that $S(y)$ is reducible in

$\mathbb{L}[y]$, then $\beta_0 \in \mathbb{L}$. As such, one can chose $\beta_i = \beta_0^{q^i}$, the iterated $q$th powers. In that case, the previous equations can be rewritten

$$P(z) = (z-\alpha_0)\left(z-\alpha_0^q\right)\cdots\left(z-\alpha_0^{q^{d-1}}\right) = (z-x)\left(z-x^q\right)\cdots\left(z-x^{q^{d-1}}\right),$$
$$Q(z) = (z-\beta_0)\left(z-\beta_0^q\right)\cdots\left(z-\beta_0^{q^{d-1}}\right) = (z-y)\left(z-y^q\right)\cdots\left(z-y^{q^{d-1}}\right).$$

As a consequence, $Q(z) \in \mathbb{K}[z]$ and to compute $Q(z)$, we need to compute $y^{q^i}$ effectively. This is done by computing the following values in $O(d\log q)$ operations in $\mathbb{L}$:

$$u_0 = x, u_1 = x^q \bmod P(x), \ldots, u_{d-1} = u_{d-2}^q = x^{q^{d-1}} \bmod P(x).$$

Then, we simply compute in $d$ operations $Q(z) = (z-u_0)(z-u_1)\cdots(z-u_{d-1})$ and we know that the resulting polynomial is in $\mathbb{K}[z]$.

Whenever $\alpha_0$ is not a square in $\mathbb{L}$, that is whenever $S(y)$ is irreducible, then $\beta_0^{q^d}$ is square root of $\alpha_0$ different from $\beta_0$, thus it is $-\beta_0$. As a consequence, setting $Q(z) = (z-\beta_0)(z-\beta_0^q)\cdots(z-\beta_0^{q^{d-1}})$ would yield a polynomial that is not stable by the Frobenius endomorphism.

As such, we introduce a new variable $y$ to represent the field $\mathbb{L}' = \mathbb{L}[y]/(y^2-x)$ and to compute $Q(z)$, we need to compute $y^{q^{i(d+1)}}$ effectively. Since $y^{q^i} = yy^{q^i-1} = yx^{\frac{q^i-1}{2}}$, we can compute the following values in $O(d\log q)$ field operations in $\mathbb{L}$:

$$u_0 = 1, u_1 = x^{\frac{q-1}{2}} \bmod P(x), \ldots, u_{d-1} = u_1 u_{d-2}^q = x^{\frac{q^{d-1}-1}{2}} \bmod P(x).$$

Consequently, $Q(z) = (z-yu_0)(z-yu_1)\cdots(z-yu_{d-1})$.

As a first step, we compute in $d$ operations, the dehomogenized polynomial in $y$,

$$\tilde{Q}(z) = (z-u_0)(z-u_1)\cdots(z-u_{d-1}) = z^d + h_1 z^{d-1} + \cdots + h_{d-1}z + h_d.$$

Then, $Q(z) = z^d + yh_1z^{d-1} + \cdots + y^{d-1}h_{d-1}z + y^d h_d$. But, denoting by $i_0 = i \bmod 2$, we have $y^i = y^{i_0}y^{i-i_0} = y^{i_0}x^{\frac{i-i_0}{2}}$ Hence we deduce:

$$\begin{aligned} Q(z) &= z^d + yh_1z^{d-1} + xh_2z^{d-2} + yxh_3z^{d-3} + \cdots + y^{d_0}x^{\frac{d-d_0}{2}}h_d \\ &= z^d + y\sum_{i=0}^{\lfloor\frac{d-1}{2}\rfloor} h_{2i+1}x^i z^{d-2i-1} + \sum_{i=1}^{\lfloor\frac{d}{2}\rfloor} h_{2i}x^i z^{d-2i} \end{aligned}$$

*Complexity analysis.* Since the number of operations for computing the square root of a block of size $d$ is bounded by $O(d\log q)$ operations in $\mathbb{L} = \mathbb{F}_{q^d}$, this is also bounded by $O(d\mathsf{M}(d)\log q)$ operations in $\mathbb{K} = \mathbb{F}_q$. As a consequence, the computation of $W$ can be done in no more than $O(n^\omega + n\mathsf{M}(n)\log q)$ operations in $\mathbb{K}$. Let us assume that the characteristic polynomial of $Z$ has degree $n$ and can be factored as $P_1^{m_1}\cdots P_s^{m_s}$ with $P_i$ and $P_j$ coprime whenever $i \neq j$, $\deg P_i = d_i$ and $m_i \geq 1$. From a computation point of view, in the worst case, one needs to introduce a variable $\alpha_i$ for one root of $P_i$ and a variable $\beta_i$ for the square root of $\alpha_i$, assuming $\alpha_i$ is not a square. This yields a total number of $2s$ variables.

*Computation in characteristic* 2. The case of characteristic 2 is almost the same. From a polynomial $P(z) = z^d + p_{d-1}z^{d-1} + \cdots + p_0 = (z-\zeta_1)\cdots(z-\zeta_d)$, we want to compute $Q(z) = z^d + q_{d-1}z^{d-1} + \cdots + q_0 = (z-\omega_1)\cdots(z-\omega_d)$, with $\omega_i^2 = \zeta_i$ for all $1 \leq i \leq d$. As $P(z^2) = Q(z)^2$, this yields $q_i = \sqrt{p_i} = p_i^{q/2}$, for all $1 \leq i \leq d-1$. Thus, $Q$ can be computed in $O(d\log q)$ operations in $\mathbb{K}$ and as a consequence, $W$ in $O(n^\omega + n\log q)$ operations in $\mathbb{K}$.

However, let us recall that $C$ is block diagonal if, and only if, the Jordan normal form is block diagonal. As such, a square root of $C$ is a polynomial in $C$ if, and only if, $C$ is block diagonal, see Appendix A.2.