SYMMETRIC DETERMINANTAL REPRESENTATIONS IN CHARACTERISTIC 2

BRUNO GRENET, THIERRY MONTEIL, AND STÉPHAN THOMASSÉ

Abstract. This paper studies Symmetric Determinantal Representations (SDR) in characteristic 2, that is the representation of a multivariate polynomial P by a symmetric matrix M such that $P = \det M$, and where each entry of M is either a constant or a variable.

We first give some sufficient conditions for a polynomial to have an SDR. We then give a non-trivial necessary condition, which implies that some polynomials have no SDR, answering a question of Grenet et al.

A large part of the paper is then devoted to the case of multilinear polynomials. We prove that the existence of an SDR for a multilinear polynomial is equivalent to the existence of a factorization of the polynomial in certain quotient rings. We develop some algorithms to test the factorizability in these rings and use them to find SDRs when they exist. Altogether, this gives us polynomial-time algorithms to factorize the polynomials in the quotient rings and to build SDRs. We conclude by describing the case of Alternating Determinantal Representations in any characteristic.

1. Introduction

Let $\mathbb{F}$ be some field of characteristic 2. A Symmetric Determinantal Representation (SDR) of a polynomial $P \in \mathbb{F}[x_1, \ldots, x_m]$ is a symmetric matrix M with entries in $\mathbb{F} \cup \{x_1, \ldots, x_m\}$ such that $\det M = P$. One can also find in the literature other definitions where for instance the symmetric matrix has linear (degree-1) polynomials as entries. The two definitions are essentially equivalent, and we shall see that for our purposes, taking one or the other does not make any difference.

Symmetric Determinantal Representations have been studied at least from the beginning of the twentieth century [6, 4] and apparently even from the nineteenth century [2]. Definite SDRs are SDRs with the additional requirement that the matrix obtained by setting all the variables to zero is positive semi-definite. Definite SDRs play an important role in convex optimization, leading to a renew of interest in these representations, definite or not, in the recent years [10, 9, 3, 13, 8, 14, 12, 15], see also [2] and the presentation [16] for more perspectives on this. Independently, symmetric determinants in characteristic two have also been a subject of studies [1, 19].

Symmetric Determinantal Representations for polynomials represented by weakly-skew circuits were given in [8] for any field of characteristic

Date: October 22, 2012.

different from 2. The authors conjectured that these representations do not always exist in characteristic 2. We prove this fact in this paper. To this end, we give a necessary condition for a polynomial to admit an SDR. We then focus on multilinear polynomials. For these polynomials, we show an equivalence between the existence of an SDR and the ability to factorize the polynomial in certain quotient rings. We develop algorithms to study the factorization in these quotient rings. Altogether, we obtain polynomial-time algorithms to factorize polynomials in the quotient rings and to compute SDRs of multilinear polynomials when they exist.

Definition 1.1. A polynomial $P \in \mathbb{F}[x_1, \dots, x_m]$ is said *representable* if it has an SDR, that is if there exists a symmetric matrix M with entries in $\mathbb{F} \cup \{x_1, \dots, x_m\}$ such that $P = \det M$. In this case, we say that M *represents* P.

For instance, the polynomial $xy + yz + zx$ is representable as the determinant of the 4×4 matrix

$$\begin{pmatrix} x & 0 & 0 & 1 \\ 0 & y & 0 & 1 \\ 0 & 0 & z & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

Note that we ask the matrix to have entries in $\mathbb{F}$. A natural relaxation would be to allow entries in an extension $\mathbb{G}$ of $\mathbb{F}$. Actually, we shall show along the way that at least for multilinear polynomials, and most certainly for any polynomial, this relaxation is irrelevant. In the case of multilinear polynomials, Corollary 5.6 shows that if a polynomial is representable, it has an SDR which only uses elements from the field generated by its coefficients.

Organization. We begin by introducing some relevant algebraic background in Section 2. Section 3 is devoted to prove that SDRs exist for a large class of polynomials. Then Section 4 proves the main results of this paper: Some polynomials are not representable, and we can characterize the multilinear representable polynomials. Some partial results towards a full characterization are also given. Section 5 is devoted to more algorithmic results. Using the equivalence between representability and factorizability in certain quotient rings, we develop algorithms for these two tasks. Section 6 is devoted to the case of Alternating Determinantal Representations in any characteristic. Finally, we conclude in Section 7 by some remaining open questions.

Experimentations were done using the free open-source mathematics software system *Sage* [17], they allowed in return to fix a bug in its determinant method (ticket #10063). The algorithms presented in this paper have been implemented and are available at `http://perso.ens-lyon.fr/bruno.grenet/publis/SymDetReprChar2.sage`.

2. Algebraic background

Let us introduce some useful notions and notations.

2.1. **Polynomials and determinants in characteristic 2.** Let $\mathbb{F}$ be any field of characteristic 2, and let $\mathbb{F}[x_1, \dots, x_m]$ be the ring of polynomials in m indeterminates over $\mathbb{F}$.

Let $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{N}^m$, then the *primitive monomial* x^α is defined by $x^\alpha = x_1^{\alpha_1} \cdots x_m^{\alpha_m}$. A *monomial* is a polynomial of the form $c.x^\alpha$ for some $c \in \mathbb{F}$ and some primitive monomial x^α. The constant c is its *coefficient*, and x^α is its *primitive part*. The value $\deg x^\alpha = \sum_i \alpha_i$ is its *total degree* and $\deg_i x^\alpha = \alpha_i$ is its degree *with respect to the variable* x_i.

Two primitive monomials x^α and x^β are compared as follows: $x^\alpha < x^\beta$ if either $\deg x^\alpha < \deg x^\beta$ or $\deg x^\alpha = \deg x^\beta$ and there exists i such that $\deg_i x^\alpha < \deg_i x^\beta$ and $\deg_j x^\alpha = \deg_j x^\beta$ for $j > i$. With this ordering, we define the *leading monomial* $\mathrm{lm}(P)$ of a polynomial P as its monomial with greatest primitive part. The *leading coefficient* $\mathrm{lc}(P)$ is the coefficient of its leading monomial.

A polynomial is said to be *multilinear* if its monomials $c.x_1^{\alpha_1} \cdots x_m^{\alpha_m}$ satisfy $\alpha_i \leq 1$ for all $i \leq m$.

Working in characteristic 2 causes some inconveniences, like the impossibility to halve. But, it also simplifies some computations. First, Frobenius endomorphism ensures that for any polynomials P_1 and P_2, we have $(P_1 + P_2)^2 = P_1^2 + P_2^2$. Second, the determinant can easily be computed:

Proposition 2.1. *Let M be a symmetric $(n \times n)$ matrix with entries in $\mathbb{F}[x_1, \dots, x_m]$. Then its determinant is*

$$\det M = \sum_\sigma \prod_{i=1}^n M_{i,\sigma(i)},$$

where σ ranges over all involutions from $\{1, \dots, n\}$ to itself, that is permutations such that $\sigma^{-1} = \sigma$.

Proof. The definition of the determinant is

$$\det M = \sum_\sigma \mathrm{sgn}(\sigma) \prod_{i=1}^n M_{i,\sigma(i)},$$

where σ ranges over all permutations of $\{1, \dots, n\}$. Actually, the signature of a permutation is either 1 or -1, and those two elements coincide in characteristic 2. This means that the signature can be removed from the definition.
Consider $P_\sigma = \prod_i M_{i,\sigma(i)}$ for some permutation such that $\sigma \neq \sigma^{-1}$. Then, $M_{i,\sigma^{-1}(i)} = M_{\sigma^{-1}(i),i}$ as M is symmetric, and $P_{\sigma^{-1}} = P_\sigma$. Thus the products for a permutation and its inverse cancel out in the sum. This shows that the sum can be restricted to involutions. □

2.2. **Quotient rings.** Given some polynomials $p_1, \dots, p_k$, we denote by $\langle p_1, \dots, p_k \rangle$ the ideal they generate. That is,

$$\langle p_1, \dots, p_k \rangle = \left\{ \sum_{i=1}^{k} p_i q_i : q_i \in \mathbb{F}[x_1, \dots, x_m] \right\}.$$

Given a tuple $\ell = (\ell_1, \dots, \ell_m) \in \mathbb{F}^m$, we define the ideal

$$\mathcal{I}(\ell) = \langle x_1^2 + \ell_1, \dots, x_m^2 + \ell_m \rangle.$$

We also define the quotient ring $\mathcal{R}(\ell)$ as $\mathbb{F}[x_1, \dots, x_m]/\mathcal{I}(\ell)$ and denote by π or π_ℓ the canonical projection $\mathbb{F}[x_1, \dots, x_m] \to \mathcal{R}(\ell)$. The restriction of this projection to $\mathbb{F}$ is one-to-one, hence $\mathbb{F}$ naturally embeds into $\mathcal{R}(\ell)$, and the elements of $\mathbb{F} \subseteq \mathcal{R}(\ell)$ are called *constants*. This morphism of rings can be extended to matrices by $\pi(A)_{ij} = \pi(A_{ij})$, and commutes with the determinant: $\pi \circ \det = \det \circ \pi$. An element of $\mathcal{R}(\ell)$ is said to be *linear* if it is the projection of a linear polynomial.

Since the quotient identifies the squares of variables with constants, any element of $r \in \mathcal{R}(\ell)$ has a unique multilinear representative in $P \in \mathbb{F}[x_1, \dots, x_m]$: we denote it by $\rho(r)$ or $\rho_\ell(r)$. We have $\pi \circ \rho = Id_{\mathcal{R}(\ell)}$. We denote by $\textsc{Mult}_\ell$ or $\textsc{Mult}$ the map $\rho_\ell \circ \pi_\ell$ that sends a polynomial to the multilinear polynomial obtained by replacing each factor x_i^2 by ℓ_i. For instance, let $P(x, y, z) = x^2 y + z^3 + xz + y$ then $\textsc{Mult}_{(0,0,0)}(P) = xz + y$ and $\textsc{Mult}_{(1,1,1)}(P) = y + z + xz + y = z + xz$.

The square of any element of $\mathcal{R}(\ell)$ belongs to $\mathbb{F}$. In particular, an element of $\mathcal{R}(\ell)$ is invertible if, and only, if its square is not zero. For example, $\pi(x_1 x_2 + 1)$ is invertible if, and only if, $\ell_1 \ell_2 \neq 1$.

Given a tuple $\ell = (\ell_1, \dots, \ell_m) \in \mathbb{F}^m$, we denote by ℓ^2 the tuple $(\ell_1^2, \dots, \ell_m^2) \in \mathbb{F}^m$, and say that ℓ^2 is a *tuple of squares*. If ℓ^2 is a tuple of squares, the square of an element r of $\mathcal{R}(\ell^2)$ is the square of a unique element c of $\mathbb{F}$: we denote it by $|r|$ or $|r|_{\ell^2}$, and call it the *absolute value* of r. We remark that $|r_1 r_2| = |r_1| + |r_2|$ and $|r_1 + r_2| = |r_1| + |r_2|$ for all $r_1, r_2 \in \mathcal{R}(\ell^2)$. Furthermore, r is inversible if and only if $|r| \neq 0$.

3. Some representable polynomials

We deal with some positive results. Even though the main part of this paper is focused on negative results, we need to be able to represent some class of polynomials in order to give a characterization.

In order to clarify some proofs, we will use the correspondence between permanents and cycle covers in graphs. We refer the reader to [5] for the definitions concerning graphs. Let G be a weighted digraph and M its adjacency matrix. We assume that the weights of G are elements of $\mathbb{F}[x_1, \dots, x_m]$. A *cycle cover* of G is a set of disjoint cycles such that each vertex of the digraph belongs to exactly one cycle. The *weight* of a cycle cover is the product of the weights of all the arcs it uses. It is easily seen from the definition that the permanent of M equals the sum of the weights

of all the cycle covers of G. Since the characteristic of $\mathbb{F}$ is two, then the permanent of M equals its determinant.

Suppose now that G is symmetric (that is M is symmetric). Proposition 2.1 shows that only some special cases of cycle covers can be considered. More precisely, the determinant of M equals the sum of the weights of the cycle covers of G corresponding to an involution. These cycle covers are made of length-1 and length-2 cycles, and are called *partial matchings*.

As G is symmetric, it can actually be considered as an undirected graph. Length-1 cycles are *loops*, and length-2 cycles are *edges*. The weight of a length-2 cycle is the product of the weights of its arcs, that is the square of the weight of the edge. Thus consider a partial matching of a graph G with (symmetric) adjacency matrix M. It can be viewed as a set μ of edges such that no vertex belongs to two distinct edges. The discussion is summarized by the identity

$$\det M = \sum_{\mu} \Big(\prod_{e \in \mu} w(e)^2 \times \prod_{v \notin \mu} w(v) \Big),$$

where $w(e)$ and $w(v)$ represent the weights of an edge e and of a loop on a vertex v respectively, $v \notin \mu$ means that the vertex v is not covered by μ, and μ ranges over all partial matchings of G. An example is given by Figure 1. The adjacency matrix of the graph is given is the introduction. The only partial matchings are made of one of the three edges, to cover the central vertex, and two loops. By convention, an edge with no indicated weight has weight 1.

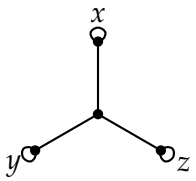

FIGURE 1. Graph representing $xy + xz + yz$.

In the following, if M is a symmetric matrix, we denote by $G(M)$ the graph whose adjacency matrix is M. Conversely, given a graph G, we denote by $M(G)$ its adjacency matrix. By a slight abuse of language, we shall say that a graph *represents* a polynomial when its adjacency matrix is an SDR of the polynomial. In the same way, we write $\det G$ instead of $\det M(G)$ to simplify the notations.

Lemma 3.1. *Let P and Q be two representable polynomials. Then $(P \times Q)$ is representable.*

Proof. Let M and N be two symmetric matrices representing P and Q respectively. To represent the product by a graph, it is enough to consider the disjoint union of $G(M)$ and $G(N)$. This means that the SDR of $(P \times Q)$ is a block-diagonal matrix with two blocks being M and N. □

The first part of the next lemma was proved in [8]. We give here another proof which is suitable for the second part.

Lemma 3.2. *Let $P \in \mathbb{F}[x_1, \dots, x_m]$. Then P^2 is representable.*

Moreover, there exists a graph G that represents P^2 with two distinguished vertices s and t and such that $\det(G \setminus \{s,t\}) = 1$ *and* $\det(G \setminus \{s\}) = \det(G \setminus \{t\}) = 0$.

Proof. Let $P = \sum_{\alpha \in \mathbb{N}^m} c_\alpha x^\alpha$ where $x^\alpha = x_1^{\alpha_1} \cdots x_m^{\alpha_m}$. The square of a monomial $c_\alpha x^\alpha$ can be represented by a graph G_α of size $2 \deg x^\alpha + 2$. For a variable x_i with exponent α_i, we build α_i graphs with two vertices and an edge of weight x_i inbetween. We also build a graph with two vertices and an edge of weight c_α inbetween. These $(\deg(x^\alpha) + 1)$ size-2 graphs are arranged in a line to build G_α: The graphs are arranged in some arbitrary order and an edge of weight 1 links two consecutive graphs (Figure 2. The

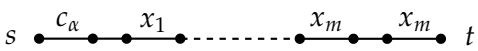

FIGURE 2. Graph G_α corresponding to some monomial $c_\alpha x^\alpha$ with $\alpha_1 \geq 1$ and $\alpha_m \geq 2$.

extremities of G_α are named s and t. There is no loop in G_α, therefore partial matchings are perfect matchings. The only perfect matching of G_α is made of all the edges of weight different from 1. The weight of such a matching is $c_\alpha^2 (x^\alpha)^2$. The only matching of $G_\alpha \setminus \{s,t\}$ is made of the edges of weight 1, and has weight 1. Since G_α has an even number of vertices, $G_\alpha \setminus \{s\}$ and $G_\alpha \setminus \{t\}$ have no perfect matching.

Given a graph G_α for each monomial of P, the graph G the union of these graphs in which all the vertices with name s on the one hand, and all vertices with name t on the other hand, are merged. The perfect matchings of G are then made of a perfect matching of some G_α, and perfect matchings of weight 1 of $G_\beta \setminus \{s,t\}$ for all $\beta \neq \alpha$. The sum of the weights of the matchings of G is $\det G = \sum_\alpha c_\alpha^2 (x^\alpha)^2 = P^2$. Furthermore, the only perfect matching $G \setminus \{s,t\}$ is made of perfect matchings of $G_\alpha \setminus \{s,t\}$ for all α, thus $\det(G \setminus \{s,t\}) = 1$. By the same parity argument as before, $\det(G \setminus \{s\}) = \det(G \setminus \{t\}) = 0$. □

This allows us to represent in a quite simple way a large class of polynomials.

Proposition 3.3. *Let $P(x_1, \dots, x_m) = L_1 \times L_2 \times \cdots \times L_k$, where for $1 \leq i \leq k$,*

$$L_i(x_1, \dots, x_m) = P_{i0}^2 + x_1 P_{i1}^2 + \cdots + x_m P_{im}^2$$

for some $P_{ij} \in \mathbb{F}[x_1, \dots, x_m]$. Then P is representable.

Proof. By Lemma 3.1, it is sufficient to show how to represent each L_i. We first prove how to represent a polynomial of the form

$$L(x_1, \dots, x_m) = \lambda_0^2 + \lambda_1^2 x_1 + \cdots + \lambda_m^2 x_m,$$

where the λ_j's are constants from $\mathbb{F}$.

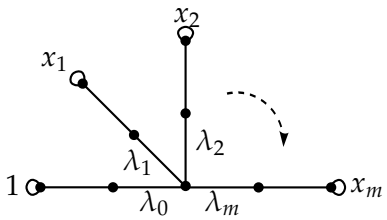

FIGURE 3. Graph representing $L = \lambda_0^2 + \lambda_1^2 x_1 + \cdots + \lambda_m^2 x_m$.

The linear polynomial L is represented by the graph G_L given on Figure 3. We prove that this effectively represents L: A partial matching has to match the central vertex with some of its neighbors. Once a neighbor is chosen, say in the direction of x_i, the loop with weight x_i has to be chosen. Then, there is only one choice to have a partial matching which consists in covering the remaining vertices by the outside edges. Thus the weight of such a partial matching is $\lambda_i^2 x_i$, and the sum over all partial matchings equals L.

Now, let G_{P_i} be the graph representing the polynomial P_i^2 given by Lemma 3.2. By a slight abuse of language, we call λ_i the edge that has weight λ_i in G_L, and denote by s and t its extremities. Let $G_L \setminus \lambda_i$ the graph obtained from G_L by removing the edge λ_i. We build a new graph G'_L in which G_{P_i} *replaces* the edge λ_i: Both G_L and G_{P_i} have two vertices called s and t. The graph G'_L is the union of $G_L \setminus \lambda_i$ and G_{P_i}, where the two s (respectively the two t) are merged.

A partial matching of G_L either is a partial matching of $G_L \setminus \lambda_i$, or is made of λ_i and a partial matching of $G_L \setminus \{s,t\}$. Thus $\det G_L = \det(G_L \setminus \lambda_i) + \lambda_i^2 \det(G_L \setminus \{s,t\})$. In G'_L, a partial matching can also be of two sorts: Either it is made of partial matchings of $G_{P_i} \setminus \{s,t\}$ and $G_L \setminus \lambda_i$, or of partial matchings of G_{P_i} and $G_L \setminus \{s,t\}$. Indeed, no partial matching exists covering $G_{P_i} \setminus \{s\}$ (respectively $G_{P_i} \setminus \{t\}$). Thus

$$\begin{aligned}\det G'_L &= \det(G_{P_i} \setminus \{s,t\}) \times \det(G_L \setminus \lambda_i) + \det G_{P_i} \times \det(G_L \setminus \{s,t\}) \\ &= 1 \times \det(G \setminus \lambda_i) + P_i^2 \times \det(G_L \setminus \{s,t\}).\end{aligned}$$

This shows that we can replace in G_L each λ_i by the G_{P_i} to obtain an SDR of $P_0^2 + x_1 P_1^2 + \cdots + x_m P_m^2$. □

In particular, this theorem shows that if $\mathbb{F}$ is a finite field of characteristic 2, every linear polynomial is representable since every element in such a field is a quadratic residue.

Definition 3.4. Let $P \in \mathbb{F}[x_1, \ldots, x_m]$. A *generalized Symmetric Determinantal Representation* (gSDR) of P is a symmetric matrix M such that $\det M = P$ and whose entries are polynomials of $\mathbb{F}[x_1, \ldots, x_m]$ such that each diagonal entry is of the form $P_0^2 + x_1 P_1^2 + \cdots + x_m P_m^2$ where $P_1, \ldots, P_m \in \mathbb{F}[x_1, \ldots, x_m]$.

Theorem 3.5. *A polynomial $P \in \mathbb{F}[x_1, \dots, x_m]$ is representable if, and only if, it admits a gSDR.*

Proof. An SDR is already a gSDR. We once again work with the graph representation instead of the matrix representation. Suppose we have a graph G where the weights of the edges are any polynomials, and the weights of the loops are of the form $P_0^2 + x_1 P_1^2 + \cdots + x_m P_m^2$. We show how we can turn this graph into an SDR.

We use the same technique as in the proof of Proposition 3.3 to replace each edge with weight P in G by the graph G_P which is an SDR of P^2. It remains to show how to deal with the loops.

Suppose some vertex v of G has a loop of weight $L = P_0^2 + x_1 P_1^2 + \cdots + x_m P_m^2$. Consider the graph G_L obtained in Proposition 3.3, and let G_0 be the graph obtained from G by removing the loop on v. Then G is replaced by $G_0 \cup G_L$, where the central vertex of G_L is merged with v. Let G' be this new graph. Note that $\det(G_L \setminus \{v\}) = 1$. Then

$$\begin{aligned} \det G' &= \det G_L \times \det(G \setminus \{v\}) + \det(G_L \setminus \{v\}) \times \det G_0 \\ &= L \times \det(G \setminus \{v\}) + 1 \times \det G_0 = \det G. \end{aligned}$$

Repeating this operation for all the loops of the graph yields the result. □

4. Obstructions to SDR

This section deals with negative results, showing that some polynomials have no SDR. Section 4.1 is devoted to a necessary condition that holds for any polynomial. It is followed by a simple example of a polynomial with no SDR. We prove in Section 4.3 that this necessary condition is actually a characterization when applied to multilinear polynomials. Finally, Section 4.4 gives some partial results towards a full characterization.

4.1. A necessary condition.

We aim to prove in this section a necessary condition for a polynomial to be representable. We introduce a notion of factorization *modulo* some ideal $\mathcal{I}(\ell)$ to express this condition.

Definition 4.1. Let $P \in \mathbb{F}[x_1, \dots, x_m]$. Then P is said *factorizable modulo* $\mathcal{I}(\ell)$ if there exist some linear elements $L_1, \dots, L_k$ of $\mathcal{R}(\ell)$ such that

$$\pi_\ell(P) = L_1 \times \cdots \times L_k.$$

This definition can be restated as follows. A polynomial P is factorizable *modulo* $\mathcal{I}(\ell)$ if there exists some linear polynomials $L_1, \dots, L_k$ of $\mathbb{F}[x_1, \dots, x_m]$ such that $\pi_\ell(P) = \pi_\ell(L_1 \cdots L_k)$.

Theorem 4.2. *Let $P \in \mathbb{F}[x_1, \dots, x_m]$ be a representable polynomial. Then for every tuple of squares $\ell^2 \in \mathbb{F}^m$, P is factorizable* modulo $\mathcal{I}(\ell^2)$.

For instance, one can recall the representable polynomial $P(x,y,z) = xy + yz + xz$ from the introduction. Then $\pi_{(0,0,0)}(P) = \pi_{(0,0,0)}((x+y)(x+z))$ and $\pi_{(1,1,1)}(P) = \pi_{(1,1,1)}(xyz(x+y+z))$.

The proof of this theorem is of algorithmic nature. We give an algorithm that takes as inputs an SDR M of some polynomial P and a tuple of squares ℓ^2, and returns a factorization of P *modulo* $\mathcal{I}(\ell^2)$. The general idea is to build the projection $A = \pi(M)$ of M to get a representation of $\pi(P)$, and then to perform row and column operations to *isolate* some diagonal entry A_{ii}, that is to cancel out each entry A_{ij} for $j \neq i$, keeping A diagonal. We then show that A_{ii} is a linear element of $\mathcal{R}(\ell^2)$. Thus we can write $\pi(P) = A_{ii}\det(A')$ where A' is obtained from A by removing its row and column of index i. By induction on the dimensions of A, we can conclude that $\pi(P)$ can be factorized as a product of linear elements. In what follows, we prove some lemmas that justify this approach.

Let us fix some tuple of squares ℓ^2. In the next definition, we extend the notion of gSDR, originally defined for polynomials, to elements of $\mathcal{R}(\ell^2)$.

Definition 4.3. Let $r \in \mathcal{R}(\ell^2)$. A *generalized Symmetric Determinantal Representation* (gSDR) of r is a symmetric matrix A such that A has linear diagonal entries and $\det(A) = r$.

In a gSDR for a polynomial, the diagonal entries are of the form $P_0^2 + x_1P_1^2 + \cdots + x_mP_m^2$. The projection of such a polynomial is a linear element of $\mathcal{R}(\ell^2)$. Indeed, for all i, $\pi(P_i^2) = \pi(P_i)^2$ belongs to $\mathbb{F}$. Therefore, if we let $\lambda_i = \pi(P_i)^2$ for all i, $\pi(P_0^2 + x_1P_1^2 + \cdots + x_mP_m^2)$ is also the projection of the linear polynomial $\lambda_0 + x_1\lambda_1 + \cdots + x_m\lambda_m$.

The previous remark implies in particular the following lemma:

Lemma 4.4. *Let M be a gSDR of some polynomial $P \in \mathbb{F}[x_1, \ldots, x_m]$. Then the matrix $\pi(M)$ is a gSDR of $\pi(P)$.*

Lemma 4.5. *Let A be a gSDR of some $r \in \mathcal{R}(\ell^2)$. Then there exists a gSDR B of r whose non-diagonal entries are constant.*

Proof. Suppose that $A_{ij} = A_{ji} = \pi(P)$, $i \neq j$, for some polynomial P. Since the determinant of A equals $\sum_\sigma \prod_i A_{i,\sigma(i)}$ where σ ranges over the involutions (by Proposition 2.1), if A_{ij} divides a monomial in $\det A$, then so does A_{ij}^2. Thus, if $\pi(P)$ divides a monomial, so does $\pi(P)^2$. If we replace A_{ij} and A_{ji} by the absolute value $|\pi(P)| \in \mathbb{F}$, the determinant of A is unchanged as $\pi(P)^2 = |\pi(P)|^2$ by definition. This proves the lemma, as B can be obtained by replacing each non-diagonal entry by its absolute value. □

We now define the main tools we use to prove the theorem. These are simple algorithms that we apply on the symmetric matrix representing an element $r \in \mathcal{R}(\ell^2)$ such that the determinant remains unchanged and the

matrix becomes diagonal. All of these depend on the tuple ℓ^2, even though it is not explicitly given as an argument to simplify the notations.

Let CLEAN be the algorithm that replaces each non diagonal entry A_{ij} by its absolute value $|A_{ij}|$ as in Lemma 4.5. We define two other algorithms, $\text{ADD}_{i,j,\alpha}$ (Algorithm 1) and ISOLATE_i (Algorithm 2).

Algorithm 1: $\text{ADD}_{i,j,\alpha}(A)$

$n \leftarrow$ dimension of A
for $k = 1$ *to* n **do** $A_{j,k} \leftarrow A_{j,k} + \alpha A_{i,k}$ // $R_j \leftarrow R_j + \alpha R_i$
for $k = 1$ *to* n **do** $A_{k,j} \leftarrow A_{k,j} + \alpha A_{k,i}$ // $C_j \leftarrow C_j + \alpha C_i$
return $\text{CLEAN}(A)$

Algorithm 2: $\text{ISOLATE}_i(A)$

$n \leftarrow$ dimension of A
for $j = 1$ *to* n **do**
    if $j \neq i$ **then**
        $\alpha \leftarrow A_{ij} \times |A_{ii}|^{-1}$
        $A \leftarrow \text{ADD}_{i,j,\alpha}(A)$
return A

Lemma 4.6. *Let A be a gSDR of some $r \in \mathcal{R}(\ell^2)$. Then $\text{ADD}_{i,j,\alpha}(A)$ is a gSDR of r whose non-diagonal entries are constants.*

Proof. The algorithm adds α times the i^{th} row to the j^{th} one, and then α times the i^{th} column to the j^{th} one. These two operations do not change the determinant. Furthermore, only entries of the j^{th} row and column are changed. But with those two operations, A_{jk} is replaced by $A_{jk} + \alpha A_{ik}$ while A_{kj} is replaced by $A_{kj} + \alpha A_{ki}$ for $j \neq k$. As initially $A_{ik} = A_{ki}$ and $A_{jk} = A_{kj}$, A remains symmetric. Furthermore, A_{jj} is first replaced by $A_{jj} + \alpha A_{ij}$, and finally by $(A_{jj} + \alpha A_{ij}) + \alpha(A_{ij} + \alpha A_{ii}) = A_{jj} + \alpha^2 A_{ii}$. Thus A_{jj} remains linear. This shows that A remains a gSDR of r after the first two operations. Eventually, CLEAN is applied to a gSDR and we obtain the second property. □

Lemma 4.7. *Let A be a gSDR of some $r \in \mathcal{R}(\ell^2)$. If there exists an index i such that $|A_{ii}| \neq 0$, then $\text{ISOLATE}_i(A)$ is a gSDR of r. Furthermore the i^{th} row and column have the entry (i, i) as their only nonzero entry.*

Proof. The matrix $\text{ISOLATE}_i(A)$ is a gSDR of r since $\text{ADD}_{i,j,\alpha}(A)$ is a gSDR of r (for all j and α). Now, let $\alpha = A_{ij} \times |A_{ii}|^{-1}$ for some j such that $A_{ij} \neq 0$ and consider the action of $\text{ADD}_{i,j,\alpha}$ on the i^{th} row of A. The only altered entry

is A_{ij}, when the i^{th} column multiplied by $\alpha = A_{ij}|A_{ii}|^{-1}$ is added to the j^{th} one, and then by $\textsc{Clean}(A)$. So A_{ij} is replaced by $A_{ij}(1 + |A_{ii}|^{-1} \times A_{ii})$. Since $|A_{ii}|^2 = A_{ii}^2$ by definition, A_{ij} is replaced by 0 during $\textsc{Clean}(A)$. The same is true on the i^{th} column. Thus, if $A' = \textsc{Isolate}_i(A)$, A'_{ii} is the only nonzero entry in the i^{th} row and column of A'. □

Lemma 4.8. *Let A be a gSDR of some $r \in \mathcal{R}(\ell^2)$ such that the square of each diagonal entry is zero. If there exists a nonzero diagonal entry, say $A_{1,1}$, and a nonzero entry $A_{1,j}$ for $j > 1$, then one can build a new gSDR of the same dimensions $\tilde{A}$, representing some $\tilde{r} \in \mathcal{R}(\ell^2)$ such that $r = (A_{1,1} + 1) \times \tilde{r}$, where moreover $\tilde{A}$ contains diagonal entries whose square is nonzero.*

Proof. Let us write $A_{1,1}$ as $1 + (A_{1,1} + 1)$. Let

$$B = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 1 & A_{1,1}+1 & A_{1,2} & \dots & A_{1,n} \\ 0 & A_{2,1} & & & \\ \vdots & \vdots & & A' & \\ 0 & A_{n,1} & & & \end{pmatrix}$$

where A' is obtained from A by removing its first row and column. Then $\det B = \det A$. Indeed, adding the first row of B to the second one, and the first column to the second one yields the matrix

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & A_{1,1} & A_{1,2} & \dots & A_{1,n} \\ 0 & A_{2,1} & & & \\ \vdots & \vdots & & A' & \\ 0 & A_{n,1} & & & \end{pmatrix}$$

whose determinant equals $\det A$.

Now

$$\textsc{Isolate}_2(B) = \begin{pmatrix} A_{1,1} & 0 & A_{1,2} & \dots & A_{1,n} \\ 0 & A_{1,1}+1 & 0 & \dots & 0 \\ A_{2,1} & 0 & & & \\ \vdots & \vdots & & A'' & \\ A_{n,1} & 0 & & & \end{pmatrix}$$

still has the same determinant. For each $j > 1$, A_{jj} is replaced by $A_{jj} + A_{1j}^2(A_{1,1}+1)$ in A''. Since $A_{jj}^2 = 0$ for all j by hypothesis and $(A_{1,1}+1)^2 = 1$, A'' contains some diagonal entries whose square is nonzero. Actually, this holds since we supposed that some $A_{1,j}$ is nonzero. Now, the determinant

of this matrix equals

$$(A_{1,1}+1)\cdot\det\begin{pmatrix} A_{1,1} & A_{1,2} & \dots & A_{1,n} \\ A_{2,1} & & & \\ \vdots & & A'' & \\ A_{n,1} & & & \end{pmatrix}.$$

Therefore, A can be replaced by this new matrix $\tilde{A}$, of the same dimensions, with some diagonal entries having a nonzero square. Then $\tilde{A}$ is a gSDR for some $\tilde{r} \in \mathcal{R}(\ell^2)$ such that $r = (A_{1,1}+1) \times \tilde{r}$. □

We now have all the ingredients to prove the theorem.

Proof of Theorem 4.2. Let us first restate the theorem. We aim to prove that if $P \in \mathbb{F}[x_1, \dots, x_m]$ has a gSDR, then its projection $r = \pi(P)$ can be written as $L_1 \times \cdots \times L_k$ where $L_1, \dots, L_k \in \mathcal{R}(\ell^2)$ are linear. Suppose we are given a gSDR M of some polynomial P. Then we have a gSDR $A = \pi(M)$ of $r = \pi(P)$ by Lemma 4.4. Thus we have to prove that given a gSDR A of some $r \in \mathcal{R}(\ell^2)$, we can find some linear elements $L_1, \dots, L_k$ of $\mathcal{R}(\ell^2)$ such that $r = L_1 \times \cdots \times L_k$.

First note that if A does not satisfy the conditions of Lemma 4.8, then we can already conclude. Indeed, this means that each diagonal entry is either zero, or is the only nonzero entry in its row and column. By reordering the rows and columns, we can get a block-diagonal matrix with two blocks: The first one has zero diagonal entries and the second one is diagonal. Therefore, since the determinant of A is the product of the determinants of these two blocks, we get a constant times a product of linear elements. In other words, the factorization is found.

So let A be a gSDR of some $r \in \mathcal{R}(\ell^2)$ satisfying the hypotheses of Lemma 4.8. We build a gSDR $\tilde{A}$ of some $\tilde{r} \in \mathcal{R}(\ell^2)$ such that $r = L \times \tilde{r}$ for some linear element $L \in \mathcal{R}(\ell^2)$, and such that $\tilde{A}$ has at least one diagonal entry $\tilde{A}_{ii}$ whose square is nonzero. If A already satisfied the property, then $\tilde{A} = A$ and $L = 1$. Now, the i^{th} row and column of $A' = \textsc{Isolate}_i(\tilde{A})$ have as only nonzero entry A'_{ii} by Lemma 4.7. Thus, removing the i^{th} row and column to A' yields a gSDR B of some polynomial $Q \in \mathcal{R}(\ell^2)$ such that $\tilde{P} = A'_{ii} \times Q$.

This shows that from a gSDR of dimensions $(n \times n)$ of some $r \in \mathcal{R}(\ell^2)$, we can build a gSDR of dimensions $(n-1) \times (n-1)$ of some polynomial $s \in \mathcal{R}(\ell^2)$ such that $r = L \times L' \times s$ where L and L' are linear.

We can now use induction to prove that if $r \in \mathcal{R}(\ell^2)$ has a gSDR, then it can be written as $L_1 \times \cdots \times L_k$ for some linear elements $L_1, \dots, L_k \in \mathcal{R}(\ell^2)$. Indeed, if A is a (1×1) gSDR of r, then r is linear. □

The proof of Theorem 4.2 is of algorithmic nature. It is easily seen that the underlying algorithm runs in time polynomial in the dimensions of the input gSDR. (More precisely, the complexity of the algorithm is $\mathcal{O}(n^3)$).

4.2. **An example.** Let us consider the polynomials in $\mathbb{F}_2[x, y, z]$, where $\mathbb{F}_2$ denotes the field with two elements. The ring $\mathcal{R}(1, 1, 1)$ has 256 elements, 136 of which can be written as the product of linear polynomials, 120 of which can not. The polynomial $\pi(xy + z)$ is one of those. Therefore, Theorem 4.2 tells us that the polynomial $xy + z$ can *not* be represented as the determinant of a symmetric matrix with entries in $\mathbb{F}_2 \cup \{x, y, z\}$.

4.3. **Multilinear polynomials.** In this section, we show that the necessary condition of Theorem 4.2 is actually a characterization when applied to multilinear polynomials. This relies on the following structural lemma. It is valid for any polynomial, even non-multilinear.

Lemma 4.9. *Let $P \in \mathbb{F}[x_1, \dots, x_m]$ be a representable polynomial. Then there exists an SDR M of P such that each variable appears at most once on the diagonal.*

Proof. Let M be any SDR for P, that is $\det M = P$, and M has entries in $\mathbb{F} \cup \{x_1, \dots, x_m\}$. Suppose that for some other i, x_i appears (at least) twice on the diagonal, as entries $M_{i_1 i_1}$ and $M_{i_2 i_2}$. Consider the matrix obtained after adding the row of index i_1 to the row of index i_2, and the column of index i_1 to the column of index i_2. As already mentioned, the only altered diagonal entry is $M_{i_2 i_2}$ and it is now equal to $M_{i_2 i_2} + M_{i_1 i_1} = 2x_i = 0$. Therefore, we obtain a new SDR with one occurrence of x_i on the diagonal replaced by zero. We can repeat this for each variable until each variable appears exactly once on the diagonal. □

We can use this lemma to obtain the desired characterization, when $\mathbb{F}$ is a finite field of characteristic 2.

Theorem 4.10. *Let $P \in \mathbb{F}[x_1, \dots, x_m]$ be a multilinear polynomial where $\mathbb{F}$ is a finite field of characteristic 2. Then the three following statements are equivalent:*

- (i) *P is representable;*
- (ii) *For every tuple of squares $\ell^2 \in \mathbb{F}^m$, P is factorizable* modulo $\mathcal{I}(\ell^2)$*;*
- (iii) *There exists a tuple of squares $\ell^2 \in \mathbb{F}^m$ such that P is factorizable* modulo $\mathcal{I}(\ell^2)$*;*

Proof. The implication $(i) \implies (ii)$ is a special case of Theorem 4.2, and $(ii) \implies (iii)$ is evident. Let us prove that $(iii) \implies (i)$.

Let $\ell^2 \in \mathbb{F}^m$ such that $\pi_{\ell^2}(P) = L_1 \times \cdots \times L_k$, where each L_i is a linear element of $\mathcal{R}(\ell^2)$. For $i \leq k$, $\rho_{\ell^2}(L_i)$ is a linear polynomial, hence by Proposition 3.3, we know that $Q = \rho_{\ell^2}(L_1) \times \cdots \times \rho_{\ell^2}(L_k)$ has an SDR M. By Lemma 4.9, there exists an SDR N of Q such that each variable appears at most once on the diagonal. Hence, Lemma 4.4 and Lemma 4.5 ensure that $\pi_{\ell^2}(P) = \pi_{\ell^2}(Q)$ has a gSDR A such that each $A_{i,i}$ is linear and each $A_{i,j}$ is constant for $i \neq j$. Let O be the matrix defined by $O_{i,j} = \rho_{\ell^2}(A_{i,j})$. Since each variable appears once on the diagonal, $\det O$ is a multilinear polynomial. We have $\pi_{\ell^2}(P) = \pi_{\ell^2}(Q) = \det A = \pi_{\ell^2}(\det O)$. Since both P and $\det O$ are multilinear, we have $P = \det O$, hence P is representable. □

If $\mathbb{F}$ is infinite, a similar characterization can be obtained. To this end, the conclusion of Theorem 4.2 can be reinforced as follows: If P is representable, then there exist linear polynomials $L_1, \dots, L_k$ *whose coefficients are quadratic residue in* $\mathbb{F}$ such that $\pi_{\ell^2}(P) = \pi_{\ell^2}(L_1 \cdots L_k)$. One can check that the proof of Theorem 4.2 actually is a proof of this stronger statement. The converse is proved using Proposition 3.3.

4.4. **Towards a full characterization.** Theorem 4.2 is valid for any polynomial. Thus we have a necessary condition for all polynomials. The characterization for multilinear polynomials relies on the fact that $\rho(\pi(P)) = P$ in this case. If we are working with a non-multilinear polynomial P, the projection of P *modulo* some ideal $\mathcal{I}(\ell)$ can dramatically change the structure of the polynomial. In particular, if we have a polynomial $P = x_1^2 \times Q$ for some multilinear polynomial Q, then $\textsc{Mult}_{(1,\dots)}P = Q$ but $\textsc{Mult}_{(0,\dots)}P = 0$. Thus, it is certainly impossible to go back from the projection *modulo* $\mathcal{I}(0,\dots)$ to P. To come up with this issue, we look at some new specific ideal for the projection. In this section, the field $\mathbb{F}$ is supposed to be finite. With the same arguments as for Theorem 4.10, the results of this section can be extended to any field of characteristic 2.

Let $\mathbb{F}(\xi_1, \dots, \xi_m)$ be the field of fractions in m indeterminates over $\mathbb{F}$, and $\mathcal{I}(\xi^2) = \langle x_1^2 + \xi_1^2, \dots, x_m^2 + \xi_m^2 \rangle$. For $P \in \mathbb{F}[x_1, \dots, x_m]$, we can consider the multilinear polynomial $\textsc{Mult}_{\xi^2}P = \rho_{\xi^2}(\pi_{\xi^2}(P))$ and apply Theorem 4.10 about multilinear polynomials. In particular, $\textsc{Mult}_{\xi^2}P$ is representable if, and only if, it is factorizable.

The problem we face is that our constructions use inverse of elements in the base field. This means that we have an equivalence between factorization and SDR for multilinear polynomials in $\mathbb{F}(\xi_1, \dots, \xi_m)[x_1, \dots, x_m]$ but the factorization or the SDR we build can use rational fractions in the ξ_i's. To partly avoid this problem, we have to restrict the ideals we are working with to ideals of the form $\mathcal{I}(\ell^2)$ for $\ell \in \mathbb{F}^m$. Unfortunately, it is not sufficient. Nevertheless, we are able to prove some partial results.

Lemma 4.11. *Let $P \in \mathbb{F}[x_1, \dots, x_m]$. Then P is representable if, and only if, $\textsc{Mult}_{\xi^2}P$ has an SDR with non-diagonal entries in $\mathbb{F}[\xi_1, \dots, \xi_m]$.*

Proof. Let us remark at first that $\textsc{Mult}_{\xi^2}$ is a bijection from $\mathbb{F}[x_1, \dots, x_m]$ to the set of multilinear polynomials with coefficients in $\mathbb{F}[\xi_1, \dots, \xi_m]$. Indeed, its inverse $\textsc{Mult}_{\xi^2}^{-1}$ simply consists in mapping each ξ_i to x_i.

Using Lemma 4.9, we can transform any (g)SDR to an SDR such that each variable appears exactly once on the diagonal.

Let M be an SDR of P. We can apply the procedure Clean to M (with respect to the tuple $(\xi_1^2, \dots, \xi_m^2)$). This yields an SDR of $\textsc{Mult}_{\xi^2}P$ as proved by Lemma 4.4. Conversely, if we have an SDR M' of $\textsc{Mult}_{\xi^2}P$, we can replace each ξ_i by x_i to get an SDR of P. This corresponds to applying $\textsc{Mult}_{\xi^2}^{-1}$ to each entry. As this function is compatible with the

addition and multiplication, the new matrix M we obtain satisfy $\det M = \textsc{Mult}^{-1}_{\xi^2}(\det M') = P$. □

Theorem 4.12. *Let $P \in \mathbb{F}[x_1, \ldots, x_m]$.*

- *If P is representable, then for every tuple of squares $\ell^2 \in \mathbb{F}^m$, $\textsc{Mult}_{\xi^2} P$ can be factorized as a product of linear polynomials* modulo $\mathcal{I}(\ell^2)$*, and the linear polynomials have coefficients in $\mathbb{F}(\xi_1, \ldots, \xi_m)$.*
- *If $\textsc{Mult}_{\xi^2} P$ can be factorized as a product of linear polynomials* modulo $\mathcal{I}(\ell^2)$ *for some tuple of squares ℓ^2, and if the linear polynomials have coefficients in $\mathbb{F}[\xi_1, \ldots, \xi_m]$, then P is representable.*

To obtain a full characterization, we would need to prove that in the first statement, we can obtain linear factors with coefficients in $\mathbb{F}[\xi_1, \ldots, \xi_m]$.

Proof. The first statement only consists in applying Theorem 4.2 to $P \in \mathbb{F}(\xi_1, \ldots, \xi_m)$.

For the second statement, suppose $\textsc{Mult}_{\xi^2} P \equiv L_1 \times \cdots \times L_k \mod \mathcal{I}(\ell^2)$ for some ℓ^2, and each L_i has coefficients in $\mathbb{F}[\xi_1, \ldots, \xi_m]$. Using Theorem 4.10, we can build a matrix representing $\textsc{Mult}_{\xi^2} P$. Since the L_j's have as coefficients some polynomials in the ξ_i's, and since the transformations of Lemma 4.9 used in the proof of Theorem 4.10 use no inverse of any of the coefficients, we get an SDR of $\textsc{Mult}_{\xi^2} P$ the non-diagonal entries of which are polynomials in the ξ_i's. Using Lemma 4.11, we conclude that P is representable. □

5. Factorization

Section 4.3 gives a characterization of representable multilinear polynomials in terms of the factorization of the polynomials into linear polynomials *modulo* an ideal $\mathcal{I}(\ell)$. We give in this section an algorithm to decide this problem. Its running time is polynomial in the lacunary representation of the polynomial. In this section, $\mathbb{F}$ is a finite field of characteristic 2.

5.1. Preliminary results.

In the previous section, we worked with elements of the quotient ring $\mathcal{R}(\ell)$ for some tuple ℓ. The algorithms presented in this section deal with multilinear polynomials $P \in \mathbb{F}[x_1, \ldots, x_m]$. Theorem 4.10 is the basic tool. Since $P = \textsc{Mult}_\ell(P)$ for any ℓ, it can be reformulated as follows: A multilinear polynomial is representable if and only if for every tuple of squares ℓ^2, there exist linear polynomials $L_1, \ldots, L_k$ such that $P = \textsc{Mult}_{\ell^2}(L_1 \cdots L_k)$. It is equivalent to say that $\pi_{\ell^2}(P) = \pi_{\ell^2}(L_1 \cdots L_k)$. Moreover, as seen before this existence does not depend on the tuple ℓ^2. This motivates the following definition.

Definition 5.1. We say that a multilinear polynomial P is *factorizable* if there exist a tuple of squares ℓ^2 and linear polynomials $L_1, \ldots, L_k$ such that

$$P = \textsc{Mult}_{\ell^2}(L_1 \times \cdots \times L_k).$$

The algorithm heavily relies on the fact that the possibility to factorize a polynomial *modulo* $\mathcal{I}(\ell^2)$ does not depend on ℓ^2. Actually two tuples are used, $\bar{0} = (0, \dots, 0)$ and $\bar{1} = (1, \dots, 1)$. To simplify the notations, this tuples are respectively denoted by 0 and 1, and π_0, ρ_0 and $\textsc{Mult}_0$ on the one hand and π_1, ρ_1 and $\textsc{Mult}_1$ on the other hand are the functions defined in Section 2.2. In the same way, let

$$\mathcal{I}_0 = \mathcal{I}(\bar{0}) = \langle x_1^2, \dots, x_m^2 \rangle \quad \text{and} \quad \mathcal{I}_1 = \mathcal{I}(\bar{1}) = \langle x_1^2 + 1, \dots, x_m^2 + 1 \rangle$$

and $\mathcal{R}_0$ and $\mathcal{R}_1$ be defined by analogy.

We shall sometimes write that P is *factorizable modulo* $\mathcal{I}$ for $\mathcal{I} = \mathcal{I}_0$ or $\mathcal{I}_1$ instead of simply factorizable to emphasize the fact that we are working specifically with the ideal $\mathcal{I}$. Let P be a multilinear polynomial. We define its *linear part* $\mathrm{Lin}(P)$ as the sum of all its monomials of degree at most 1. For instance $\mathrm{Lin}(xyz + xy + x + z + 1) = x + z + 1$. Furthermore, we write $\partial P/\partial x_i$ the partial derivative of P with respect to the variable x_i. For a multilinear polynomial, this equals the quotient in the euclidean division of P by x_i.

To show how to test the factorizability of a multilinear polynomial, we proceed into two steps. We first show how to test the factorizability of a polynomial P whose monomial of lowest degree has degree exactly 1 (we say that P has *valuation* 1). To this end, we show that P is factorizable if, and only if, $P = \textsc{Mult}_0(\mathrm{Lin}(P) \times \frac{1}{\alpha_i}\frac{\partial P}{\partial x_i})$ where $\alpha_i x_i$ is a nonzero monomial of $\mathrm{Lin}(P)$ (Lemmas 5.2 and 5.3). The second step proves that given any multilinear polynomial P, we can compute a polynomial Q of the same degree whose valuation is 1 such that P is factorizable if, and only if, Q also. There are two cases, covered by Lemmas 5.4 and 5.5. This will allow us to describe an algorithm using alternatively those two steps to test factorizability.

Lemma 5.2. *Let P be a multilinear polynomial of valuation 1. If there exists some linear polynomials $L_1, \dots, L_k$ such that*

$$P = \textsc{Mult}_0(L_1 \times \cdots \times L_k),$$

then there exist an index j and a constant α such that $\mathrm{Lin}(P) = \alpha L_j$.

Proof. Suppose that $P = \textsc{Mult}_0(L_1 \cdots L_k)$ and let $Q = L_1 \cdots L_k$. In particular, $Q(0) = 0$ and $\mathrm{Lin}(P) = \mathrm{Lin}(Q)$. Thus there exists j such that $L_j(0) = 0$. In other words, L_j is a sum of degree-1 monomials. The linear part of P being nonzero, the polynomial Q/L_j has a constant coefficient $\alpha \in \mathbb{F}$. A degree-1 monomial of Q is the product of a monomial of L_j by α. This means that $\mathrm{Lin}(P) = \mathrm{Lin}(Q) = \alpha L_j$. □

We now prove that we can efficiently test if some linear polynomial L can appear in the factorization of P *modulo* $\mathcal{I}_0$.

Lemma 5.3. *Let P be a multilinear polynomial and L be a linear polynomial with no constant coefficient, having a nonzero monomial $\alpha_i x_i$. If there exists a*

multilinear polynomial Q such that $P = \textsc{Mult}_0(L \times Q)$, then

$$P = \textsc{Mult}_0\left(L \times \frac{1}{\alpha_i}\frac{\partial P}{\partial x_i}\right).$$

Proof. Suppose that $P = \textsc{Mult}_0(L \times Q)$. This means that there exist polynomials $p_1, \dots, p_m$ such that

$$P = L \times Q + x_1^2 p_1 + \cdots + x_m^2 p_m.$$

Moreover, $\partial(x_j^2 p_j)/\partial x_i = x_j^2 \partial p_j/\partial x_i$ for all j. For $j = i$, this comes from the fact that $\partial x_i^2/\partial x_i = 2x_i = 0$. Since L contains the monomial $\alpha_i x_i$, $\partial L/\partial x_i = \alpha_i$. Therefore,

$$\frac{\partial P}{\partial x_i} = \alpha_i Q + L\frac{\partial Q}{\partial x_i} + \frac{\partial p_1}{\partial x_i}x_1^2 + \cdots + \frac{\partial p_m}{\partial x_i}x_m^2.$$

Since $\alpha_i \neq 0$, the previous equality can be multiplied by L/α_i to obtain

$$L \times \frac{1}{\alpha_i}\frac{\partial P}{\partial x_i} = L \times Q + \frac{L^2}{\alpha_i}\frac{\partial Q}{\partial x_i} + \frac{L}{\alpha_i}\left(\frac{\partial p_1}{\partial x_i}x_1^2 + \cdots + \frac{\partial p_m}{\partial x_i}x_m^2\right).$$

Since L^2 is a sum of squares,

$$\textsc{Mult}_0\left(L \times \frac{1}{\alpha_i}\frac{\partial P}{\partial x_i}\right) = \textsc{Mult}_0(L \times Q) = P.$$

□

In the second step we prove that given any multilinear polynomial P, we can find a polynomial Q of valuation 1 such that P is factorizable if, and only if, Q also. There are two distinct cases. At first, we focus on *full* polynomials, that is without zero coefficient. An m-variate multilinear polynomial is full if it has 2^m nonzero monomials. In particular, if every coefficient equals 1, then the polynomial can be factorized as $\prod_i(1 + x_i)$. In the general case, such a factorization does not necessarily exist.

In the following lemma, given a full polynomial, a new polynomial is produced that is either not full, or has less variables. In any case, the number of monomials decreases.

Lemma 5.4. *Let P be a multilinear polynomial over m variables with exactly 2^m monomials. Then there exists a linear polynomial L such that $Q \stackrel{def}{=} \textsc{Mult}_0(P \times L)$ is nonzero and has less than 2^m monomials. Moreover, P is factorizable if, and only if, Q is factorizable.*

Proof. Let x_i be any variable of P and $L = p_i x_i + p_0$ where p_i is the coefficient of x_i in P and p_0 is its constant coefficient. Then the constant coefficient of Q is p_0^2 and thus Q is nonzero, and the coefficient of x_i in Q is $p_0 p_i + p_i p_0 = 0$. Thus Q has less monomials than P.

By definition, Q is factorizable if P also. Moreover, $\textsc{Mult}_0(L \times Q) = \textsc{Mult}_0(L^2 \times P) = \textsc{Mult}_0(p_0^2 P) = p_0^2 P$ since P is multilinear. Thus if Q is factorizable, then so is P. □

It remains to deal with the case where P does not possess all the possible monomials. In this lemma, we consider the ideal $\mathcal{I}_1$ instead of $\mathcal{I}_0$ as before.

Lemma 5.5. *Let P be a multilinear polynomial over m variables with at most $(2^m - 1)$ monomials. Then there exists a primitive monomial x^α such that $Q \stackrel{def}{=} \textsc{Mult}_1(x^\alpha \times P)$ has valuation 1. Moreover, P is factorizable if, and only if, Q is factorizable.*

Proof. If P already has valuation 1, we can take $\alpha = (0, \dots, 0)$.

If P has valuation greater than 1, let x^β be a nonzero primitive monomial of P of minimal degree. Let i be some index such that $\beta_i \neq 0$ and define $x^\alpha = x^\beta / x_i$. Then $\textsc{Mult}_1(x^\alpha x^\beta) = x_i$. Moreover, $\textsc{Mult}_1(x^\alpha x^\gamma) = 1$ if, and only if, $\alpha = \gamma$. Since $\deg x^\alpha < \deg x^\beta$, the coefficient of x^α in P is zero. Thus x^α satisfies the lemma.

If P has valuation 0, let x^α be a primitive monomial of minimal degree whose coefficient in P is zero. Such a monomial exists since P has at most $(2^m - 1)$ monomials. Then $\textsc{Mult}_1(x^\alpha \times P)$ has no constant coefficient. Furthermore, by the minimality of x^α, every monomial of smaller degree has a nonzero coefficient in P. This is in particular the case of the monomials x^α / x_i for every variable x_i that divides x^α. Since $\textsc{Mult}_1(x^\alpha (x^\alpha / x_i)) = x_i$, x^α satisfies the lemma.

To finish the proof, we remark that $\textsc{Mult}_1(x^\alpha Q) = \textsc{Mult}_1((x^\alpha)^2 P) = P$. Therefore, P is factorizable if and only if Q is factorizable. □

For the proof of the next corollary, one need to remark a simple fact. If a multilinear polynomial P is representable, then $\partial P / \partial x_i$ is also representable for any variable x_i. Indeed, suppose that M is an SDR of P with each variable appearing at most once on the diagonal. Suppose that $M_{jj} = x_i$. Then the determinant of the matrix obtained by removing the row and column j from M equals $\partial P / \partial x_i$.

Corollary 5.6. *Let $P \in \mathbb{F}[x_1, \dots, x_m]$ be a multilinear polynomial and $\mathbb{G}/\mathbb{F}$ a field extension. If P has an SDR with entries in $\mathbb{G} \cup \{x_1, \dots, x_m\}$, then it has an SDR with entries in $\mathbb{F} \cup \{x_1, \dots, x_m\}$.*

Proof. Let us first consider $\mathbb{G}$ as the base field. By Theorem 4.10, P is representable if, and only if, it is factorizable. Using Lemmas 5.4 and 5.5, one can suppose that P has valuation 1. Moreover, using Lemmas 5.2 and 5.3 and the remark before the corollary, one can deduce that P is representable if, and only if, $P = \textsc{Mult}_0(\operatorname{Lin} P \times \frac{1}{\alpha_i} \frac{\partial P}{\partial x_i})$ and $\partial P / \partial x_i$ is representable.

Now, $\partial P / \partial x_i$ is a polynomial with coefficients in $\mathbb{F}$, which has an SDR with entries in $\mathbb{G} \cup \{x_1, \dots, x_m\}$. Moreover, it has one variable less than P. Therefore, we can prove the corollary by induction on the number of variables. □

5.2. **An algorithm for factorizability.** The previous lemmas yield a polynomial time algorithm to decide whether some polynomial P is factorizable.

We first give an algorithm PREPARATION (Algorithm 3) corresponding to Lemmas 5.4 and 5.5.

Algorithm 3: PREPARATION(P)

Input: A multilinear polynomial P
Output: A multilinear polynomial Q of valuation 1 or linear

if P *is linear* **then return** P
// Lemma 5.4
else if P *is full* **then**
  $x_i \leftarrow$ some variable of P
  $p_i \leftarrow$ coefficient of x_i in P
  $p_0 \leftarrow$ constant coefficient of P
  $P \leftarrow \text{MULT}_0(P \times (p_i x_i + p_0))$
  return PREPARATION(P)
// Lemma 5.5
else if P *has valuation* 0 **then**
  $x^\alpha \leftarrow$ minimal monomial with a zero coefficient in P
  return $\text{MULT}_1(x^\alpha P)$
else if P *has valuation* > 1 **then**
  $x^\alpha \leftarrow$ minimal monomial of P, divided by one of its variables
  return $\text{MULT}_1(x^\alpha P)$
else return P

Lemma 5.7. *Let $P \in \mathbb{F}[x_1, \dots, x_m]$ be a multilinear polynomial. Then $Q =$ PREPARATION(P) is either linear, or has valuation 1. Moreover, P is factorizable if and only if Q also.*

The algorithm runs in time polynomial in the number of variables and the number of monomials of P.

Proof. The correctness is ensured by Lemmas 5.4 and 5.5. We only have to prove its termination and the running time estimate. There is a recursive call when P is full. From Lemma 5.4, $\text{MULT}_0(P \times (p_0 x_i + p_i))$ then has at most $(2^m - 1)$ monomials. Either this new polynomial is full, but the number of variables decreased, or the condition "f is full" is not satisfied anymore and there is no new recursive call. Therefore, the number of recursive calls is bounded by the number of variables. This proves both the termination and the complexity analysis. □

Let us now describe the algorithm ISFACTORIZABLE (Algorithm 4) corresponding to Lemmas 5.2 and 5.3.

Theorem 5.8. *Let $P \in \mathbb{F}[x_1, \dots, x_m]$ be a multilinear polynomial. Then* ISFACTORIZABLE(P) *answers **True** if, and only if, P is factorizable.*

The algorithm runs in time polynomial in the number m of variables and the number of monomials of P.

Algorithm 4: IsFactorizable(P)

Input: A multilinear polynomial P
Output: Is P factorizable?

```
1 P ← Preparation(P)
2 if P is linear then return true
3 else
      // Lemma 5.2 & 5.3:
4     α_i x_i ← some nonzero monomial of Lin(P)
5     P_0 ← ∂P/∂x_i
6     if P = Mult_0(1/α_i Lin(P) × P_0) then
7         return IsFactorizable(P_0)
8     else
9         return False
```

Proof. The correctness follows from Lemmas 5.2 and 5.3. The termination is ensured by the fact that $\partial P/\partial x_i$ has less variables than P. This bounds the number of iterations by m. □

5.3. **An algorithm for the representation.** Algorithm 4 only tells us if a polynomial is factorizable, but does not give us a factorization. The reason for this is that we change several times the ideal we are working with. Nevertheless, we proved in Section 4.3 that given the factorization of a multilinear polynomial *modulo* some ideal $\mathcal{I}$, we can find a symmetric matrix representing the polynomial. We use this in the following to show how to modify Algorithm 4 in order to get a Symmetric Determinantal Representation. Using the results of Section 4.1, we are then able to factorize any factorizable multilinear polynomial *modulo* any ideal $\mathcal{I}$.

Lemma 5.9. *Given two SDRs M_P and M_Q of two multilinear polynomials P and Q respectively, one can build an SDR* $\textsc{Merge}_b(M_P, M_Q)$ *of* $\textsc{Mult}_b(P \times Q)$ *($b \in \{0,1\}$) in time polynomial in the dimensions of M_P and M_Q.*

Proof. The algorithm is based on Lemma 4.9. Let N be the block-diagonal matrix made of M_P and M_Q. Clearly, this matrix represents $P \times Q$. Using Lemma 4.9, a matrix N' is built such that each variable appears at most once on the diagonal and such that $\det N' = P \times Q$. Then $\textsc{Merge}_b(M_P, M_Q) = \textsc{Mult}_b(N')$ represents $\textsc{Mult}_b(P \times Q)$. □

Theorem 5.10. *There is an algorithm* SymDet *that given as input a multilinear polynomial $P \in \mathbb{F}[x_1, \dots, x_m]$ in sparse representation returns an SDR of P if one exists. This algorithm runs in time polynomial in m and the number of monomials.*

Proof. The algorithm SymDet is made of two steps. The first one is a modification of the algorithm IsFactorizable such that it returns a list

of factors instead of **True** when P is factorizable. The second one is the construction of an SDR of P from this list of factors, using the algorithm Merge of Lemma 5.9.

In algorithms Preparation and IsFactorizable, to test if P is factorizable, it is written as $P = \text{Mult}_b(L \times Q)$ where L is either linear or a monomial and $b \in \{0, 1\}$, and then one tests whether Q is factorizable. These algorithms are modified to retain the couples (L, b) each time such an operation is performed. More precisely, we add a global variable $\mathcal{L}$ of the form (L, b). Let us now describe how Preparation and IsFactorizable modify this variable.

In Preparation, Line 7, the couple $((p_0x_i + p_i)/p_i^2, 0)$ is added to $\mathcal{L}$. Indeed, a recursive call is performed with the polynomial $Q = \text{Mult}_0(P \times (p_0x_i + p_i))$. But $\text{Mult}_0(Q \times (p_0x_i + p_i)/p_i^2) = \text{Mult}_0(P \times (p_0^2x_i^2 + p_i)^2/p_i^2) = P$. In the same way, the couple $(x^\alpha, 1)$ is added to $\mathcal{L}$ at Lines 11 and 14. To finish, the couple $(\text{Lin}(f)/\alpha_i, 0)$ is added to $\mathcal{L}$ at Line 7 of IsFactorizable.

When IsFactorizable answers **True**, then P is linear. Instead of this answer, the new algorithm adds the couple $(P, 0)$ to $\mathcal{L}$ (the bit 0 is arbitrary and unused) and returns $\mathcal{L}$. At this stage, we have a list $\mathcal{L}$ of couples $(L_1, b_1), \ldots, (L_k, b_k)$. Let $P_k = L_k$ and for i from $(k-1)$ down to 1, $P_i = \text{Mult}_{b_i}(L_i \times P_{i+1})$. From the construction of $\mathcal{L}$, $P = P_1$. An SDR for P is built as follows: For all i, an SDR N_i of L_i is built using Proposition 3.3. Then, let $M_k = N_k$ and for i from $(k-1)$ down to 1, let $M_i = \text{Merge}_{b_i}(N_i, M_{i+1})$. If $\det(M_{i+1}) = P_{i+1}$ and $\det(N_i) = L_i$, Lemma 5.9 shows that $\det(M_i) = P_i$. To conclude, the algorithm returns $M = M_1$.

The running time of the algorithm is controlled by the running times of Preparation, IsFactorizable, and Merge. □

6. A characteristic-free result: Alternating Determinantal Representations

Symmetric matrices correspond to symmetric bilinear forms. We saw that in this context, there is a big difference depending on whether the characteristic of the underlying field is 2 or not. As explained to us by Mathieu Florence [7], the related notion of alternating forms is known to be *characteristic-free*. An *alternating form* is a bilinear form $\varphi : V \times V \to \mathbb{F}$ such that such that $\varphi(v, v) = 0$ for any v in the vector space V. The matrix associated to alternating forms are the anti-symmetric matrix with zero diagonal entries. Hence, we should expect an homogeneous result concerning Alternating Determinantal Representations. It turns out to be the case:

Theorem 6.1. *Let $\mathbb{F}$ be some field and $P \in \mathbb{F}[x_1, \ldots, x_m]$ be a polynomial. Then, P can be written as the determinant of an alternating matrix with entries in $\mathbb{F} \cup \{x_1, \ldots, x_m\}$ if, and only if, P is a square.*

Proof. Let P be the determinant of an alternating matrix M with entries in $\mathbb{F} \cup \{x_1, \dots, x_m\}$. If we consider M as a matrix over the commutative ring $\mathbb{F}[x_1, \dots, x_m]$, we see that $P = \det M$ is the square of the Pfaffian of M which is an element of $\mathbb{F}[x_1, \dots, x_m]$ ([11] XV, §9, page 588).
Conversely, let $P = Q^2$ be the square of an element of $\mathbb{F}[x_1, \dots, x_m]$. As proved in [18], there exists a square matrix N with entries in $\mathbb{F} \cup \{x_1, \dots, x_m\}$ such that $\det N = Q$. The matrix

$$M = \begin{pmatrix} 0 & N \\ -N^T & 0 \end{pmatrix}$$

is alternate and satisfies $\det M = (\det N)^2 = Q^2 = P$. □

7. Concluding remarks

We proved in this paper that in characteristic 2, some polynomials do not admit any SDR. In the case of multilinear polynomials, we gave a complete characterization as well as algorithms to deal with these representations. We discovered some tight relations between the ability to find an SDR and to factorize the polynomial *modulo* some square polynomials. Thus we showed that the factorization in these quotient rings can be performed in polynomial time.

The main remaining open question is of course to get a full characterization of representable polynomials.

Conjecture. *A polynomial $P \in \mathbb{F}[x_1, \dots, x_m]$ is representable if, and only if, for some (equivalently any) tuple of squares $\ell \in \mathbb{F}^m$, $\textsc{Mult}_{\xi} P$ is factorizable* modulo *$\mathcal{I}(\ell)$ into linear polynomials $L_1, \dots, L_k \in \mathbb{F}[\xi_1, \dots, \xi_m][x_1, \dots, x_m]$.*

An example of problematic polynomial is $x_1^2 + x_1x_2 + x_1x_3 + x_2x_3$. Indeed, it can be factorized as $(x_1 + x_2)(x_1 + x_3)$. But once the projection *modulo* $\mathcal{I}_{\xi}$ is made, it is not so clear anymore how it can be factorized. One idea could be first to factorize the polynomial and then apply our results to each factor. Yet it is not clear whether this strategy can work.

If the conjecture can be proved, or if some other characterization of the same kind can be found, it would also remain to see if the algorithms designed for multilinear polynomials can be extended to the general case. Once again, the main difficulty is to deal with the fact that our algorithms use inverse of elements.

Even for multilinear polynomials, some questions remain. For instance, it could be interesting to make a quantitative study to know how many polynomials have SDRs. For instance, all polynomials in 2 variables are representable, and it seems that the proportion decreases as the number of variables increases.

The factorization algorithm we gave takes as input a polynomial in sparse representation. It could also be interesting to see whether some efficient algorithms can be designed for polynomials given as formulas or weakly-skew circuits as in [8].

Acknowledgments. B.G. thanks Erich L. Kaltofen, Pascal Koiran, Natacha Portier, Yann Strozecki and Sébastien Tavenas for fruitful discussions on the subject of this paper.

References

[1] Albert, A. Symmetric and alternate matrices in an arbitrary field, I. *Trans. Amer. Math. Soc. 43*, 3 (1938), 386–436.
[2] Beauville, A. Determinantal hypersurfaces. *Michigan Math. J 48* (2000), 39–64.
[3] Brändén, P. Obstructions to determinantal representability. *Adv. Math. 226*, 2 (2011), 1202–1212. arXiv:1004.1382.
[4] Dickson, L. Determination of all general homogeneous polynomials expressible as determinants with linear elements. *Trans. Amer. Math. Soc 22* (1921), 167–179.
[5] Diestel, R. *Graph Theory*, 3rd ed. Graduate Texts in Mathematics. Springer, 2006.
[6] Dixon, A. Note on the reduction of a ternary quantic to a symmetrical determinant. In *Proc. Cambridge Phil. Soc.* (1902), vol. 2, pp. 350–351.
[7] Florence, M. private communication, 2012.
[8] Grenet, B., Kaltofen, E. L., Koiran, P., and Portier, N. Symmetric Determinantal Representation of Formulas and Weakly Skew Circuits. In *Randomization, Relaxation, and Complexity in Polynomial Equation Solving*, L. Gurvits, P. Pébay, J. M. Rojas, and D. C. Thompson, Eds., no. 556 in Contemp. Math. Amer. Math. Soc., Providence, RI, 2011, pp. 61–96. arXiv:1007.3804, extended abstract in STACS'11.
[9] Helton, J., and Vinnikov, V. Linear matrix inequality representation of sets. *Commun. Pur. Appl. Math. 60*, 5 (2007), 654–674. arXiv:math/0306180.
[10] Helton, J. W., McCullough, S. A., and Vinnikov, V. Noncommutative convexity arises from linear matrix inequalities. *J. Funct. Anal. 240*, 1 (Nov. 2006), 105–191.
[11] Lang, S. *Algebra*, third ed., vol. 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
[12] Netzer, T., Plaumann, D., and Thom, A. Determinantal Representations and the Hermite Matrix. arXiv:1108.4380, 2011.
[13] Netzer, T., and Thom, A. Polynomials with and without determinantal representations. *Linear Algebra Appl. 437*, 7 (2012), 1579–1595. arXiv:1008.1931.
[14] Plaumann, D., Sturmfels, B., and Vinzant, C. Quartic curves and their bitangents. *J. Symb. Comput.* (2011). arXiv:1008.4104.
[15] Quarez, R. Symmetric determinantal representation of polynomials. *Linear Algebra Appl. 436*, 9 (2012), 3642–3660.
[16] Schweighofer, M. Describing convex semialgebraic sets by linear matrix inequalities, 2009. Tutorial Session at ISSAC'09. http://www.math.uni-konstanz.de/~schweigh/presentations/dcssblmi.pdf.
[17] Stein, W., et al. *Sage Mathematics Software (Version 4.5.3)*. The Sage Development Team, 2010. http://www.sagemath.org.
[18] Valiant, L. G. Completeness classes in algebra. In *Proc. STOC'79* (1979), pp. 249–261.
[19] Waterhouse, W. Symmetric determinants and Jordan norm similarities in characteristic 2. *Proc. Amer. Math. Soc.* (1985), 583–589.

LIP, UMR 5668, ÉNS de Lyon – CNRS – UCBL – INRIA, Université de Lyon
E-mail address: Bruno.Grenet@ens-lyon.fr

LIRMM, UMR 5506, CNRS, Université Montpellier II
URL: http://www.lirmm.fr/~monteil/

LIP, UMR 5668, ÉNS de Lyon – CNRS – UCBL – INRIA, Université de Lyon
E-mail address: Stephan.Thomasse@ens-lyon.fr