Improved method to find optimal formulae for bilinear maps

Svyatoslav Covanov

Improved method to find optimal formulae for bilinear maps

Svyatoslav Covanov

Université de Lorraine, LORIA, UMR 7503, Vandoeuvre-lès-Nancy, F-54506, France

Inria, Villers-lès-Nancy, F-54600, France

CNRS, LORIA, UMR 7503, Vandoeuvre-lès-Nancy, F-54506, France

Abstract

In 2012, Barbulescu, Detrey, Estibals and Zimmermann proposed a new framework to exhaustively search for optimal formulae for evaluating bilinear maps, such as Strassen or Karatsuba formulae. The main contribution of this work is a new criterion to aggressively prune useless branches in the exhaustive search, thus leading to the computation of new optimal formulae, in particular for the short product modulo X^5 and the circulant product modulo $(X^5 - 1)$. Moreover, we are able to prove that there is essentially only one optimal decomposition of the product of 3×2 by 2×3 matrices up to the action of some group of automorphisms.

Keywords: bilinear rank, optimal formulae, polynomial multiplication, matrix multiplication, finite field arithmetic, bilinear map, automorphisms

1. Introduction

Finding optimal formulae for computing bilinear maps is a problem of algebraic complexity theory [7, 6, 25, 15], initiated by the discoveries of Karatsuba [16] and Strassen [25]. It consists in determining almost optimal algorithms for important problems of complexity theory, among which the well studied complexity of matrix multiplication [25, 9, 18] and the complexity of polynomial multiplication [16, 26, 23, 11].

As far as polynomial multiplication is concerned, the first improvement over the schoolbook method came from Karatsuba [16] in 1962, who proposed a decomposition of the bilinear map associated to the product of two polynomials of degree 1

$$A = a_0 + a_1 X \text{ and } B = b_0 + b_1 X.$$

Using the schoolbook algorithm, computing the product $P \cdot Q$ requires 4 multiplications over the coefficient ring: $a_0 b_0$, $a_1 b_0$, $a_0 b_1$, $a_1 b_1$. With the algorithm proposed by Karatsuba, the coefficients of the product $A \cdot B$ can be retrieved from the computation of the 3 following multiplications: $a_0 b_0$, $(a_0 + a_1)(b_0 + b_1)$, $a_1 b_1$. In particular, Karatsuba's algorithm can be applied recursively to improve the binary complexity of the multiplication of two n-bit integers: instead of $O(n^2)$ with the naive schoolbook algorithm, we obtain $O(n^{\log_2 3})$.

In 1969, Strassen [25] proposed formulae improving on the cost of the product of two 2×2 matrices. When applied recursively on large matrices, this leads to a binary complexity in $O(n^{\log_2 7})$ instead of $O(n^{\log_2 8}) = O(n^3)$. Smirnov describes in [24] practical algorithms for

Email address: svyatoslav.covanov@inria.fr (Svyatoslav Covanov)

matrices of higher dimensions. One can notice that, most of the time, optimal algorithms for matrix multiplication are unknown. For example, it is possible compute the product of 3×3 matrices over $\mathbb{C}$ with 23 multiplications [17], but the best known lower bound is still 19 [4].

State of the art. An obstacle to finding optimal formulae is the fact that the decomposition of bilinear maps is known to be NP-hard [14]. In terms of method, the least-squares method seems to be one of the most popular [24]. Another way to decompose a bilinear map consists in using ingredients from geometry [3] and to find a generalization of the decomposition of singular value decomposition for matrices to general tensors. However, these methods are essentially used over an algebraically closed field K (e.g. $K = \mathbb{C}$) and are not meant to produce all the possible decompositions for a bilinear map. In our context, we require a method for computing a rank decomposition over a finite field.

Montgomery proposed in [19] an algorithm to compute such a decomposition for the particular case of polynomials of small degree over a finite field. The author takes advantage of the fact that the number of possible formulae is always finite on a finite field. He obtains new formulae for the multiplication of polynomials of degree 4, 5 and 6 over $\mathbb{F}_2$. In [20], Oseledets proposes a heuristic approach and uses the formalism of vector spaces to solve the bilinear rank problem for the polynomial product over $\mathbb{F}_2$. Later, Barbulescu et al. proposed in [1] a unified framework, extending the idea proposed by Oseledets using the vector space formalism. This allows the authors to compute the bilinear rank of different applications, such as the short product or the middle product over a finite field. Their algorithm generates all the possible rank decompositions of any bilinear map over a finite field. We extend this work in the current article.

Contributions. The work presented is an improvement to the algorithm introduced in [1], allowing one to increase the family of bilinear maps over a finite field for which we are able to compute all the optimal formulae. Our algorithm relies on the automorphism group stabilizing a bilinear map represented as a vector space and on coverings of this vector space. It can be used for proving lower bounds on the rank of a bilinear map and it has applications for improving upper bounds on the Chudnovsky-Chudnovsky algorithms [8, 22, 21]. Especially, we compute all the decompositions for the short product of polynomials P and Q modulo X^5 and the product of 3×2 by 2×3 matrices. The latter problem was out of reach with the method used in [1]. We prove, in particular, that the set of possible decompositions for this matrix product is essentially unique, up to the automorphism group.

Roadmap. This article is organized as follows. In Section 2, we present the theoretical tools and the framework for this article, corresponding to the framework introduced in [1]. In Section 3, we present, with kind permission of the authors, unpublished improvements [2] taking into account the symmetries of bilinear maps. In Section 4, we describe the theoretical aspect of our main contribution, which relies on the construction of covering sets, and illustrate it with the example of the short product. We discuss specific algorithmic aspects in Section 5: this part is quite technical and can be skipped on a first read. In Section 6, we apply our idea to the particular case of the product of matrices 3×2 by 2×3. Finally, experimental timings are given in Section 7.

2. Preliminaries

We present in this section the definition of the mathematical objects that we manipulate in this work and we define the bilinear rank. We choose the characterization given by de Groote [10] or Bürgisser et al. [7, Ch. 14]. In particular, we introduce here the framework of [1] and the underlying linear algebra problem.

2.1. Problem statement

Let K be a field. Given a bilinear map $\mathbf{\Phi} : K^m \times K^n \to K^\ell$, the bilinear rank problem consists in finding the minimal number of multiplications between scalars used for evaluating $\mathbf{\Phi}$. The set $\mathcal{L}(K^m, K^n; K^\ell)$ denotes the set of bilinear maps from $K^m \times K^n$ to K^ℓ. Any bilinear map $\mathbf{\Phi}$ from $K^m \times K^n$ to K^ℓ can be seen as an element of $\mathcal{L}(K^m, K^n; K)^\ell$, whose coordinates are the bilinear forms $(\Phi_h)_{0 \le h < \ell}$.

Example 1 (Multiplication of linear polynomials)**.** *Let $A = a_0 + a_1 X$ and $B = b_0 + b_1 X$ be two polynomials over K. The product $A \cdot B$ is associated to the bilinear map $\mathbf{\Phi}$ taking as input the vectors $\mathbf{a} = (a_0, a_1)$ and $\mathbf{b} = (b_0, b_1)$ such that*

$$\mathbf{\Phi} : (\mathbf{a}, \mathbf{b}) \mapsto \begin{pmatrix} a_0 b_0 \\ a_0 b_1 + a_1 b_0 \\ a_1 b_1 \end{pmatrix}.$$

Thus, $\mathbf{\Phi}$ can be seen as an element of $\mathcal{L}(K^2, K^2; K)^3$, whose coefficients are the 3 bilinear forms

$$\begin{aligned} &\Phi_0 : (\mathbf{a}, \mathbf{b}) \mapsto a_0 b_0, \\ &\Phi_1 : (\mathbf{a}, \mathbf{b}) \mapsto a_0 b_1 + a_1 b_0 \text{ and} \\ &\Phi_2 : (\mathbf{a}, \mathbf{b}) \mapsto a_1 b_1. \end{aligned}$$

Let Ψ be an element of $\mathcal{L}(K^2, K^2; K)$ such that $\Psi : (\mathbf{a}, \mathbf{b}) \mapsto (a_0 + a_1)(b_0 + b_1)$. Then, since $\Phi_1 = \Psi - \Phi_0 - \Phi_2$, we can rewrite $\mathbf{\Phi}$ as

$$\mathbf{\Phi} = \begin{pmatrix} \Phi_0 \\ \Phi_1 \\ \Phi_2 \end{pmatrix} = \Phi_0 \cdot \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} + \Psi \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \Phi_2 \cdot \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}.$$

The bilinear forms Φ_0, Ψ and Φ_2 each correspond to exactly one multiplication over K. Thus, we can deduce that the bilinear rank of $\mathbf{\Phi}$ is at most 3. Actually, one can show that the bilinear rank of $\mathbf{\Phi}$ is equal to 3.

Formally, a bilinear form $\Phi \in \mathcal{L}(K^m, K^n; K)$ is said to have rank one if there exist two linear forms $\alpha \in \mathcal{L}(K^m; K)$ and $\beta \in \mathcal{L}(K^n; K)$ such that $\Phi(\mathbf{a}, \mathbf{b}) = \alpha(\mathbf{a}) \cdot \beta(\mathbf{b})$, which corresponds to a multiplication between coefficients. For $i \in \{0, \dots, m-1\}$ and $j \in \{0, \dots, n-1\}$, we denote by $e_{i,j}$ the bilinear forms $e_{i,j} : (\mathbf{a}, \mathbf{b}) \mapsto a_i b_j$. The $e_{i,j}$'s have rank one and form the canonical basis of $\mathcal{L}(K^m, K^n; K)$. This implies that any bilinear form can be expressed as a linear combination of bilinear forms of rank one.

Definition 2 (Bilinear rank)**.** *The rank of a bilinear form Φ, denoted by $\mathrm{rk}(\Phi)$, is defined as the minimal number of bilinear forms ϕ_t of rank one such that Φ is a linear combination of the ϕ_t's. Then, a family $(\phi_t)_t$ of cardinality $\mathrm{rk}(\Phi)$ is said to be an optimal decomposition of Φ.*

We extend this definition to bilinear maps $\mathbf{\Phi} \in \mathcal{L}(K^m, K^n; K)^\ell$: the rank r of $\mathbf{\Phi}$ is the cardinality of a minimal set of bilinear forms $(\phi_t)_{0 \le t < r}$ of rank one for which there exist vectors $\mathbf{c}_t \in K^\ell$ such that

$$\mathbf{\Phi} = \sum_{0 \le t < r} \phi_t \cdot \mathbf{c}_t.$$

We have a matrix equivalent of Definition 2. Indeed, for $\Phi \in \mathcal{L}(K^m, K^n; K)$, there exists a matrix $M \in \mathcal{M}_{m,n}(K)$ such that $\Phi(\mathbf{a}, \mathbf{b}) = \mathbf{a}^{\mathrm{T}} \cdot M \cdot \mathbf{b}$ for $\mathbf{a} \in K^m$ and $\mathbf{b} \in K^n$. In this situation, the usual matrix rank of M is equal to the rank of Φ defined as above. Let $\mathbf{\Phi} = (\Phi_0, \dots, \Phi_{\ell-1})$

be a bilinear map of rank r, for which each Φ_h for $0 \leq h < \ell$ is represented by $M_h \in \mathcal{M}_{m,n}(K)$. Consequently, there exists a set of r matrices $N_t \in \mathcal{M}_{m,n}(K)$ of rank one such that

$$\forall h \in \{0, \ldots, \ell - 1\}\,,\ M_h \in \mathrm{Span}(N_0, \ldots, N_{r-1}).$$

Example 3 (Short product of polynomials of degree 2)**.** *We describe in this example the matrices associated to the short product of two polynomials of degree* 2*. In particular, this example is used to illustrate the idea of Section 4.*

Let A and B be the polynomials $A = a_0 + a_1X + a_2X^2$ and $B = b_0 + b_1X + b_2X^2$. We denote by C the polynomial $A \cdot B \bmod X^3$:

$$C = a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2.$$

We consider A and B as vectors of K^3 denoted by $\mathbf{a}$ and $\mathbf{b}$, respectively. Let Φ_0, Φ_1 and Φ_2 be bilinear forms defined as

$$\begin{aligned}
\Phi_0 &: (\mathbf{a}, \mathbf{b}) \mapsto a_0b_0,\\
\Phi_1 &: (\mathbf{a}, \mathbf{b}) \mapsto a_0b_1 + a_1b_0,\\
\Phi_2 &: (\mathbf{a}, \mathbf{b}) \mapsto a_0b_2 + a_1b_1 + a_2b_0.
\end{aligned}$$

In order to get the corresponding matrices, we consider the canonical basis for $\mathcal{L}(K^3, K^3; K)$, i.e. the bilinear forms $e_{i,j}$ satisfying $e_{i,j} : (\mathbf{a}, \mathbf{b}) \mapsto a_ib_j$, for $0 \leq i, j < 3$. Then, the matrices M_h associated to Φ_h are

$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

2.2. A linear algebra problem

The approach of [1] consists in computing the rank of a bilinear map $\mathbf{\Phi} = (\Phi_0, \ldots, \Phi_{\ell-1})$ by considering $T = \mathrm{Span}(\Phi_0, \ldots, \Phi_{\ell-1})$, which is a subspace of $\mathcal{L}(K^m, K^n; K)$ (it is better to work with subspaces of $\mathcal{L}(K^m, K^n; K)$ rather than elements of $\mathcal{L}(K^m, K^n; K)^\ell$). Thus, we need to extend the definition of the rank to subspaces of $\mathcal{L}(K^m, K^n; K)$.

Notation 4. *We denote by $\mathscr{S}_{m,n,r}$ the set of subspaces $V \in \mathcal{L}(K^m, K^n; K)$ spanned by a free family of rank-one bilinear forms of size r. For T a subspace of $\mathcal{L}(K^m, K^n; K)$, the set $\mathscr{S}_{m,n,r,T}$ is the set of $V \in \mathscr{S}_{m,n,r}$ such that $T \subset V$. When m and n are clear from the context, these sets are simply denoted by $\mathscr{S}_r$ and $\mathscr{S}_{r,T}$.*

We use Notation 4 to define the rank of a subspace $T \in \mathcal{L}(K^m, K^n; K)$ in Definition 5.

Definition 5 (Rank of a subspace of $\mathcal{L}(K^m, K^n; K)$)**.** *Let T be a subspace of $\mathcal{L}(K^m, K^n; K)$. We denote by $\mathrm{rk}(T)$ the smallest r such that $\mathscr{S}_{r,T} \neq \emptyset$. The set $\mathscr{S}_{\mathrm{rk}(T),T}$ is the set of optimal decompositions of T.*

Let $\mathbf{\Phi} = (\Phi_0, \ldots, \Phi_{\ell-1}) \in \mathcal{L}(K^m, K^n; K)^\ell$ and $T = \mathrm{Span}(\Phi_0, \ldots, \Phi_{\ell-1}) \subset \mathcal{L}(K^m, K^n; K)$. Decomposing a bilinear map $\mathbf{\Phi} \in \mathcal{L}(K^m, K^n; K)^\ell$ into linear combination of r rank-one bilinear forms is equivalent to computing $\mathscr{S}_{r,T}$. Our approach focuses on the latter point of view, which is also the point of view taken by Algorithm [1, Alg. 1].

General strategy for computing the bilinear rank. Taking into account the formalism proposed in Section 2.2, the algorithmic strategy we use to compute the bilinear rank of a bilinear map is stated as follows, for a target subspace $T \subset \mathcal{L}(K^m, K^n; K)$ of dimension ℓ:

- start with an intial guess $r = \ell$ (we necessarily have $\mathrm{rk}(T) \geq \dim(T)$);
- compute $\mathscr{S}_{r,T}$;
- if $\mathscr{S}_{r,T} = \emptyset$, increment r and return to the previous step;
- at the end, r is the rank and $\mathscr{S}_{r,T}$ the set of optimal decompositions.

2.3. The BDEZ Algorithm (Barbulescu, Detrey, Estibals, Zimmermann)

We describe in this section Algorithm [1, Alg. 1], which is a recursive method to solve the bilinear rank problem for a bilinear map over a finite field. As described above, this is essentially equivalent to computing $\mathscr{S}_{r,T}$ for a given subspace $T \subset \mathcal{L}(K^m, K^n; K)$ of dimension ℓ. This bilinear map can be represented by a vector space T of dimension ℓ for which we compute $\mathscr{S}_{r,T}$.

In order to get all the vector spaces $V \in \mathscr{S}_r$ such that $T \subset V$, we compute the vector spaces $W \in \mathscr{S}_{r-\ell}$ such that $T \oplus W \in \mathscr{S}_r$. In other terms, instead of enumerating all the elements of $\mathscr{S}_r$, we rather enumerate complementary subspaces of T in $\mathscr{S}_{r-\ell}$. This restriction can be done thanks to Proposition [1, Prop. 1], reformulated as Proposition 6 using the formalism of Section 2.2.

Proposition 6. *Let T be a subspace of dimension ℓ of $\mathcal{L}(K^m, K^n; K)$, let $r \geq \ell$ be an integer. For any $V \in \mathscr{S}_{r,T}$, there exists $W \in \mathscr{S}_{r-\ell}$ such that $T \oplus W = V$.*

Proof. Let $\mathcal{B}$ be a basis of V composed of rank-one matrices. We define inductively a sequence of subspaces $(W_t)_{0 \leq t \leq r-\ell}$, such that for any t we have $W_t \in \mathscr{S}_t$, as follows.

- The set W_0 is the null subspace and satisfies $T \oplus W_0 \subset V$ and $\dim T \oplus W_0 = \ell$.
- For $t \in \{1, \ldots, r-\ell\}$, assuming that $T \oplus W_{t-1} \subset V$ and $\dim(T \oplus W_{t-1}) = \ell + t - 1$, there exists $b \in \mathcal{B}$ such that $b \notin T \oplus W_{t-1}$ (otherwise $T \oplus W_{t-1} = V$ and $\dim V \leq r-1$, which is a contradiction). Then, we define W_t as $W_t = W_{t-1} \oplus \mathrm{Span}(b)$. The subspace W_t satisfies $T \oplus W_t \subset V$, $\dim(T \oplus W_t) = \ell + t$ and $W_t \in \mathscr{S}_t$.

Taking $W = W_{r-\ell}$, Proposition 6 is proved. □

In a finite field, the set of rank-one bilinear forms up to a multiplicative factor is a finite set of cardinality $\frac{(\#K^m-1)(\#K^n-1)}{(K-1)^2}$. Moreover, Algorithm BDEZ requires a test to determine whether, for $V \in \mathcal{L}(K^m, K^n; K)$ of dimension r, we have $V \in \mathscr{S}_r$: we denote by VecSpHasGoodBasis this test. A naive method to perform this test is described in Algorithm 1. We could think of other methods based on solving bilinear systems, but it does not seem efficient in our applications. However, an optimized version of this algorithm is used for particular bilinear maps (product of 2×3 by 3×2 matrices for example).

Algorithm 1 VecSpHasGoodBasis (naive method)

Input: V of dimension r in $\mathcal{L}(K^m, K^n; K)$
Output: Boolean indicating whether $V \in \mathscr{S}_r$
1: $\mathcal{H} \leftarrow \mathcal{G} \cap V$ ▷ $\mathcal{G}$ is the set of rank-one bilinear forms of $\mathcal{L}(K^m, K^n; K)$
2: **if** $\dim(\mathrm{Span}(\mathcal{H})) = r$ **then**
3: **return true**
4: **else**
5: **return false**
6: **end if**

Algorithm BDEZ can be described as a a recursive optimized version of the backtracking method constructing all the sets of cardinality $r - \ell$ of independent bilinear forms of rank one. The input of the first call to BDEZ is: a target T of dimension ℓ, the set of rank-one bilinear forms up to a multiplicative factor and an integer r (r is a guess on the rank of T, as explained at the end of Section 2.2).

Algorithm 2 BDEZ

Input: $T \subset \mathcal{L}(K^m, K^n; K)$ of dimension ℓ, $\mathcal{G}$ the set of rank-one bilinear forms, r
Output: $\mathscr{S}_{r,T}$
1: **function** ExpandSubspace($V, \mathcal{H}, r$)
2: **if** $\dim V = r$ and VecSpHasGoodBasis(V) **then**
3: **return** $\{V\}$
4: **else**
5: $\mathcal{S} \leftarrow \emptyset$
6: $\mathcal{H} \leftarrow \mathcal{H}/_V$ ▷ If $\phi' - \phi \in V$, $\phi' \equiv \phi \bmod V$
7: **for** $u \in \{0, \ldots, \#\mathcal{H} - 1\}$ **do** ▷ $\mathcal{H} = \{\phi_u |\ u \in [0, \#\mathcal{H} - 1]\}$
8: $\mathcal{S} \leftarrow \mathcal{S} \cup$ ExpandSubspace($V \oplus \mathrm{Span}(\phi_u)$, $\{\phi_{u+1}, \ldots, \phi_{\#\mathcal{H}-1}\}$, r)
9: **end for**
10: **return** $\mathcal{S}$
11: **end if**
12: **end function**
13: **return** ExpandSubspace($T, \mathcal{G}, r$)

Algorithm BDEZ takes into account, on Line 6, the equivalence relation "modulo V": two distinct elements h and h' of $\mathcal{H}$ may be such that $V + h = V + h'$. We compute this reduction by representing the vector space V with a colum echelon form matrix that is used to reduce the elements of $\mathcal{H}$ via a Gauss reduction.

This algorithm can be described using a tree in which each node at depth $r-\ell$ corresponds to a vector space $T \oplus W_{u_1,u_2,\ldots,u_{r-\ell}}$ of dimension r generated by a basis of T and rank-one matrices $\phi_{u_1}, \phi_{u_2}, \ldots, \phi_{u_{r-\ell}}$. For example, assuming that the initial set of rank-one bilinear forms is $\{\phi_0, \phi_1, \phi_2, \phi_3\}$ and ignoring the reduction computed on Line 6, we would obtain generically for $r - \ell = 3$ the tree given in Figure 1.

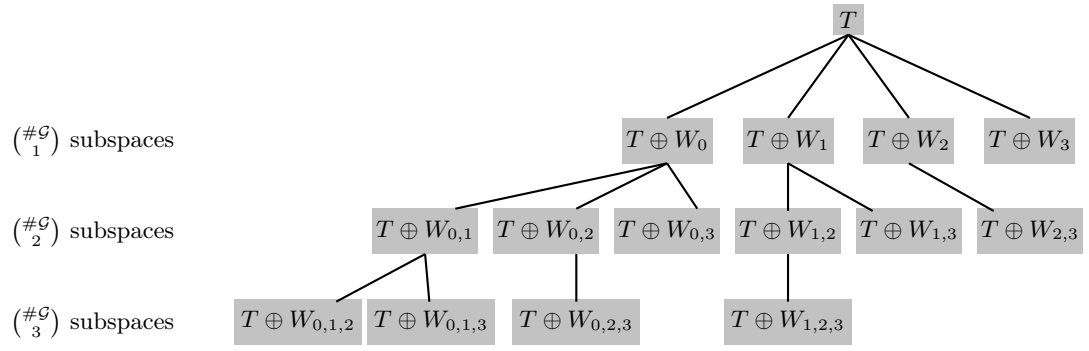

Figure 1: Tree of recursive calls in an exhaustive search with depth $r - \ell = 3$

3. Improving on BDEZ using symmetries

We present in this section, with kind permission from the authors, an unpublished improvement [2] to Algorithm BDEZ. This improvement takes into account the fact that we can define automorphisms of $\mathcal{L}(K^m, K^n; K)$, whose action is defined in Section 3.1. They preserve the rank of bilinear forms.

3.1. Action of automorphisms on $\mathcal{L}(K^m, K^n; K)$

We work with subspaces of $\mathcal{L}(K^m, K^n; K)$ rather than with bilinear maps, as in Section 2.2. Consequently, we need to adapt the automorphism group defined in Definition [7, Def. 14.11] to the case of subspaces of $\mathcal{L}(K^m, K^n; K)$, which is done in Definition 7.

Definition 7 (Action of $\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$)**.** *An element $\sigma = (\sigma_x, \sigma_y) \in \mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ acts on $\mathcal{L}(K^m, K^n; K)$ via*

$$\Phi \circ \sigma : (\mathbf{a}, \mathbf{b}) \mapsto \Phi(\sigma_x(\mathbf{a}), \sigma_y(\mathbf{b})).$$

The elements of $\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ are automorphisms of $\mathcal{L}(K^m, K^n; K)$. By linearity, we extend this action to subspaces of $\mathcal{L}(K^m, K^n; K)$.

Remark 8. *Note that, when $m = n$, Definition 7 is not the most general notion of automorphisms that we may have: for simplicity, we do not take into account the possible transposition τ acting on any $\Phi \in \mathcal{L}(K^m, K^m; K)$, via*

$$\Phi \circ \tau : (\mathbf{a}, \mathbf{b}) \mapsto \Phi(\mathbf{b}, \mathbf{a}).$$

Remark 9. *The group $\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ is isomorphic to the group $\mathrm{GL}_m(K) \times \mathrm{GL}_n(K)$, acting on matrices M via*

$$M \cdot (X, Y) = X^{\mathrm{T}} \cdot M \cdot Y.$$

Thus, we often consider elements of $\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ as elements of $\mathrm{GL}_m(K) \times \mathrm{GL}_n(K)$ and conversely.

Example 10 (Action of $\mathrm{GL}(K^2) \times \mathrm{GL}(K^2)$)**.** *Let us consider the subspace V of $\mathcal{L}(K^2, K^2; K)$ generated by bilinear forms represented by matrices M_1 and M_2 defined as*

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, M_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

We take $\sigma = (X, Y)$ *such that* $X = Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

The subspace $V' = V \circ \sigma$ *is generated by* M_1' *and* M_2'*, defined as*

$$M_1' = X^{\mathrm{T}} \cdot M_1 \cdot Y = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \; M_2' = X^{\mathrm{T}} \cdot M_2 \cdot Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Henceforth, since we refer to subgroups of $\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ stabilizing elements of $\mathcal{L}(K^m, K^n; K)$, we define what is a stabilizer.

Definition 11 (Stabilizer)**.** *For a subset* $T \subset \mathcal{L}(K^m, K^n; K)$*, we denote by* $\mathrm{Stab}(T)$ *the subgroup of* $\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ *stabilizing* T*:*

$$\mathrm{Stab}(T) = \{\sigma \in \mathrm{GL}(K^m) \times \mathrm{GL}(K^n) \mid T \circ \sigma = T\}.$$

We use the same notation for a subspace $T \subset \mathcal{L}(K^m, K^n; K)$*.*

Our algorithmic improvement comes from the fact that, for any target space $T \in \mathcal{L}(K^m, K^n; K)$ of dimension ℓ and any integer $r \geq \ell$, we have

$$\forall \sigma \in \mathrm{Stab}(T), \; \mathscr{S}_{r,T} \circ \sigma = \mathscr{S}_{r,T},$$

because σ preserves the rank. Thus, we can restrict our interest to the computation of the quotient $\mathscr{S}_{r,T}/\mathrm{Stab}(T)$ instead of $\mathscr{S}_{r,T}$.

3.2. BDEZ with stabilizer

In order to find all the elements of $\mathscr{S}_{r,T}$, it is sufficient to obtain one representative per equivalence class of $\mathscr{S}_{r,T}/\mathrm{Stab}(T)$, from which one can recover the whole orbits through the group action of $\mathrm{Stab}(T)$. Moreover, we can compute $\mathscr{S}_{r,T}/\mathrm{Stab}(T)$ faster than $\mathscr{S}_{r,T}$. Thus, we adapt our general strategy to this idea.

General strategy for computing the bilinear rank using automorphisms. The new algorithmic strategy we are considering is stated as follows, for a target subspace $T \subset \mathcal{L}(K^m, K^n; K)$ of dimension ℓ and the associated subgroup $\mathrm{Stab}(T)$ of automorphisms stabilizing T:

- start with an initial guess $r = \ell$;
- compute $\mathscr{S}_{r,T}/\mathrm{Stab}(T)$ (the set $\mathscr{S}_{r,T}$ up to the action of $\mathrm{Stab}(T)$);
- if $\mathscr{S}_{r,T}/\mathrm{Stab}(T) = \emptyset$, increment r and return to the previous step;
- recover $\mathscr{S}_{r,T}$ using the action of $\mathrm{Stab}(T)$;
- at the end, r is the rank and $\mathscr{S}_{r,T}$ the set of optimal decompositions.

Algorithm BDEZStab is a recursive approach for the computation of one representative per equivalence class. The input of the first call to BDEZStab is: a target subspace T of dimension ℓ, the set of rank-one bilinear forms of $\mathcal{L}(K^m, K^n; K)$ up to a multiplicative factor, the group $\mathrm{Stab}(T)$ and an integer $r \geq \ell$.

Figure 2 describes this recursive approach using a tree and illustrates how some branches are pruned, relying on Proposition 12. We assume that the initial set of rank-one bilinear forms is $\{\phi_0, \phi_1, \phi_2, \phi_3\}$ and that we have $\sigma \in \mathrm{Stab}(T)$ such that $\sigma(\phi_0) = \phi_1$, $\sigma(\phi_1) = \phi_0$, $\sigma(\phi_2) = \phi_3$ and $\sigma(\phi_3) = \phi_2$.

Algorithm 3 BDEZStab

Input: $T \subset \mathcal{L}(K^m, K^n; K)$, $\mathcal{G}$ a set of rank-one bilinear forms, $\mathrm{Stab}(T)$, r
Output: $\mathscr{S}_{r,T}/\mathrm{Stab}(T)$

1: **function** ExpandSubspace($V, \mathcal{H}, U, r$)
2: **if** $\dim V = r$ and VecSpHasGoodBasis(V) **then**
3: **return** $\{V\}$
4: **else**
5: $\mathcal{S} \leftarrow \emptyset$
6: $\mathcal{O} \leftarrow (\mathcal{H}/V)/U$ ▷ If $(V \oplus \phi) = (V \oplus \phi') \circ \sigma$ for $\sigma \in U$, then $\phi' \equiv \phi \bmod V \bmod U$
7: **for** $u \in \{0, \ldots, \#\mathcal{O} - 1\}$ **do** ▷ $\mathcal{O} = \{o_u \mid u \in \{0, \ldots, \#\mathcal{O} - 1\}\}$
8: $U' \leftarrow \mathrm{Stab}\,(V \oplus \mathrm{Span}\,(o_u)) \cap U$
9: $\mathcal{S} \leftarrow \mathcal{S} \cup$ ExpandSubspace$(V, \{h \in \mathcal{H} \mid \exists v \geq u,\ h = o_v \bmod U\}, U', r)$
10: **end for**
11: **return** $\mathcal{S}$
12: **end if**
13: **end function**
14: **return** ExpandSubspace$(T, \mathcal{G}, \mathrm{Stab}(T), r)$

Proposition 12. *Let T and V be subspaces of $\mathcal{L}(K^m, K^n; K)$ such that $V \in \mathscr{S}_{r,T}$. Then, given the orbit $\phi \circ \mathrm{Stab}(T)$ of a bilinear form ϕ of rank one, if V satisfies $V \cap (\phi \circ \mathrm{Stab}(T)) \neq \emptyset$, then there exists an element V' in the equivalence class of V for the action of $\mathrm{Stab}(T)$ and such that $\phi \in V'$.*

Proof. There exists $\sigma \in \mathrm{Stab}(T)$ such that $\phi \circ \sigma \in V$. We can then take $V' = V \circ (\sigma^{-1})$, which meets all the conditions. □

The particularity of BDEZStab is that, instead of enumerating all the elements of $\mathcal{H}$ as in BDEZ, we restrict ourselves to one element per equivalence class for the action of $U \subset \mathrm{Stab}(V)$. We use in particular the fact that the additional computations such as stabilizers on Line 8 are negligible, compared to the speed-up obtained by pruning branches in BDEZ. Heuristically, BDEZStab is faster than BDEZ by a factor $\#\,\mathrm{Stab}\,(T)$. This method constitutes the state of the art for the current work: our contribution is compared to the performance of this algorithm.

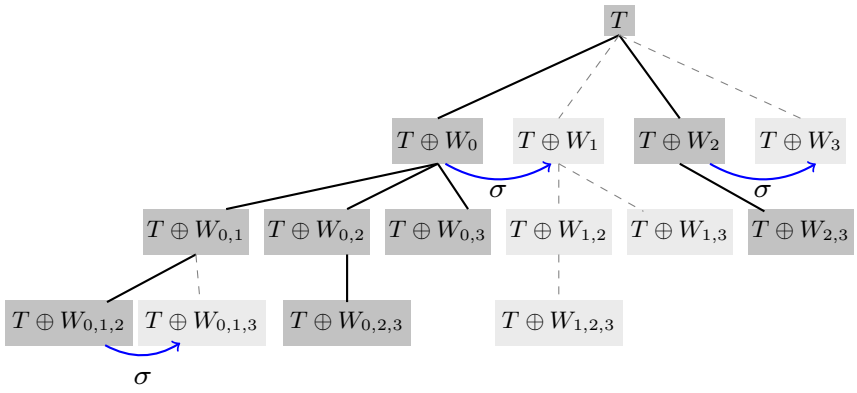

Figure 2: Pruning branches in an exhaustive search using automorphisms.

4. Covering sets of optimal decompositions

Our contribution consists in reducing the number of vector spaces W that we need to enumerate in order to get those that satsify $T \oplus W \in \mathscr{S}_r$, where T is a vector space representing a bilinear map. To this effect, we restrict ourselves to vector spaces W satisfying some properties intrinsic to T. In this section, the definition and theoretical aspects of the set of vector spaces satisfying these properties are treated, illustrated via the example of the short product. In Section 5, we deal with practical and computational aspects.

4.1. Covering sets

Our strategy consists, first, for any $r \geq \ell$, in constructing g sets $\{\mathcal{E}_{i,r}\}_i$ that are g subsets of $\mathscr{S}_{r-\ell+k_i}$, where k_i is a nonnegative integer, satisfying some property described in Definition 13.

Definition 13. *For a vector space T of dimension ℓ and an integer $r \geq \ell$, we say that $\{\mathcal{E}_{i,r}\}_{0\leq i<g}$ satisfies property $\mathfrak{P}_T$ if, for any vector space $W \in \mathscr{S}_{r-\ell}$ satisfying $T \oplus W \in \mathscr{S}_r$, there exists $i \in \{0, \ldots, g-1\}$, $W' \in \mathcal{E}_{i,r}$ and $\sigma \in \mathrm{Stab}(T)$ such that $W \subset W' \circ \sigma$.*

In particular, we have $\mathscr{S}_{r,T} \subset \{T + W' \mid \exists i \in \{0, \ldots, g-1\},\ W' \in \mathcal{E}_{i,r} \circ \mathrm{Stab}(T)\}$. Thus, assuming that we have a method to compute the $\mathcal{E}_{i,r}$'s, we are able to obtain the set $\mathscr{S}_{r,T}$. For example, for $g = 1$, the singleton containing the set $\mathcal{E}_{0,r} = \mathscr{S}_{r-\ell}/\mathrm{Stab}(T)$, satisfies Property $\mathfrak{P}_T$ and is obtained via BDEZStab. We describe below how we construct the $\mathcal{E}_{i,r}$'s that we use in practice.

Notation 14. *For an integer $d \geq 0$ and a bilinear form $\Phi \in \mathcal{L}(K^m, K^n; K)$, we denote by $\mathcal{V}_d(\Phi)$ the set of subspaces $W \in \mathscr{S}_d$ such that*

$$\min_{\Psi \in W} \mathrm{rk}(\Phi - \Psi) = 1.$$

We provide via Theorem 15 an equation involving the bases of T, that we use in combination with some property parametrized by T.

Theorem 15. *Let T be a subspace of $\mathcal{L}(K^m, K^n; K)$ of rank r and dimension ℓ. Let $W \in \mathscr{S}_{r-\ell}$, such that $T \oplus W \in \mathscr{S}_r$. Then, there exists a basis $\mathcal{B} = (t_0, \ldots, t_{\ell-1})$ of T such that*

$$\forall h \in \{0, \ldots, \ell-1\},\ W \in \mathcal{V}_{r-\ell}(t_h).$$

Proof. By hypothesis, there exist r bilinear forms of rank one $(\phi_0, \ldots, \phi_{r-1})$ forming a basis of $T \oplus W$. We can moreover assume that $W = \mathrm{Span}(\phi_\ell, \ldots, \phi_{r-1})$. Since $\phi_h \notin W$ for $h < \ell$, we have

$$\forall h < \ell, \exists (t_h, w_h) \in T \times W,\ \phi_h = t_h + w_h.$$

The t_h's, corresponding to the bilinear forms ϕ_h for $h < \ell$, form a subset of T generating a vector space of dimension ℓ since

$$T \oplus W = \mathrm{Span}(t_0, \ldots, t_{\ell-1}) \oplus \mathrm{Span}(\phi_\ell, \ldots, \phi_{r-1})$$

and $\dim(T \oplus W) = r$. Thus, $\mathrm{Span}((t_h)_{0\leq h<\ell})$ is a subspace of T of dimension ℓ. □

Theorem 15 can be reformulated via Equation 1:

$$\{W \in \mathscr{S}_{r-\ell} \mid T \oplus W \in \mathscr{S}_r\} \subset \bigcup_{\mathcal{B} \text{ basis of } T} \left(\bigcap_{\Phi \in \mathcal{B}} \mathcal{V}_{r-\ell}(\Phi) \right). \tag{1}$$

The main ingredient in the construction of the sets satisfying $\mathfrak{P}_T$ is to produce g subspaces $F_i = \mathrm{Span}(\{\Psi_{i,0}, \ldots, \Psi_{i,k_i-1}\}) \subset T$ of dimension k_i such that they form a covering of T in the sense of Definition 16.

Definition 16 (Covering sets of a vector space)**.** *For a vector space T, a set of g subspaces $F_i \subset T$ of dimension k_i is a covering of T if and only if for any basis $\mathcal{B}$ of T, there exist $i \in \{0, \ldots, g-1\}$, $\sigma \in \mathrm{Stab}(T)$ and $\mathcal{U} \subset \mathcal{B}$ such that*

$$\#\mathcal{U} = k_i \text{ and } \mathrm{Span}(\mathcal{U}) \circ \sigma = F_i.$$

A set of g subspaces $\{F_i\}_i$ is not a covering of T in the classical sense: it produces a covering of the set of bases of T. There are two extreme cases for the possible coverings of T. The first extreme case is the covering given by $\{\mathrm{Span}(\emptyset)\}$. The second extreme case is the covering given by $\{T\}$: any basis $\mathcal{B}$ of T satisfies, for any $\sigma \in \mathrm{Stab}(T)$, $\mathrm{Span}(\mathcal{B}) \circ \sigma = T$.

Proposition 17. *For a vector space T and a covering $\{F_i\}_{0 \le i < g}$ of T, we have*

$$\{W \in \mathscr{S}_{r-\ell} \mid T \oplus W \in \mathscr{S}_r\} \subset \bigcup_{\substack{0 \le i \le g-1 \\ \mathcal{F} \text{ basis of } F_i}} \left(\bigcap_{\Phi \in \mathcal{F}} \mathcal{V}_{r-\ell}(\Phi) \right) \circ \mathrm{Stab}(T). \tag{2}$$

Proof. This inclusion is derived from Equation 1 by using the fact that for any basis $\mathcal{B}$ of T we have

$$\forall \mathcal{U} \subset \mathcal{B}, \ \bigcap_{\Phi \in \mathcal{B}} \mathcal{V}_{r-\ell}(\Phi) \subset \bigcap_{\Phi \in \mathcal{U}} \mathcal{V}_{r-\ell}(\Phi)$$

and that for subsets $\mathcal{E}$ and $\mathcal{E}'$ of $\mathscr{S}_{r-\ell}$, for which there exists $\sigma \in T$ such that $\mathcal{E} \circ \sigma = \mathcal{E}'$, we have $\mathcal{E} \cup \mathcal{E}' \subset \mathcal{E} \circ \mathrm{Stab}(T)$. □

Notation 18. *For a subspace F of bilinear forms, we denote by $\mathcal{C}_d(F)$ the subset of $\mathscr{S}_d$ of vector spaces W such that $F \subset W$.*

Observing that for any subspace of bilinear forms F and $\sigma \in \mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ we have $\mathcal{C}_d(F) \circ \sigma = \mathcal{C}_d(F \circ \sigma)$, for any subgroup U of $\mathrm{Stab}(F)$, a quotient of the form $\mathcal{Q} = \mathcal{C}_d(F)/U$ satisfies

$$\forall W \in \mathcal{Q}, \sigma \in U, \ W \circ \sigma \in \mathcal{C}_d(F).$$

We use this observation in Proposition 19 to provide the general form of the $\mathcal{E}_{i,r}$'s.

Proposition 19. *For a vector space T, a covering of T given by g subspaces $F_i \subset T$, and g subgroups $U_i \subset \mathrm{Stab}(T) \cap \mathrm{Stab}(F_i)$, the set of $\mathcal{E}_{i,r}$'s, such that $\mathcal{E}_{i,r} = \mathcal{C}_{r-\ell+k_i}(F_i)/U_i$, satisfies Property $\mathfrak{P}_T$.*

Proof. Let $W \in \mathscr{S}_{r-\ell}$ be such that $T \oplus W \in \mathscr{S}_r$. There exists, according to Proposition 17, an integer $i \in \{0, \ldots, g-1\}$, $\mathcal{F}$ a basis of F_i and $\sigma \in \mathrm{Stab}(T)$ such that

$$W \in \bigcap_{\Phi \in \mathcal{F}} \mathcal{V}_{r-\ell}(\Phi) \circ \sigma.$$

Letting $W' = W \oplus (F_i \circ \sigma)$, we have $W' \in \mathscr{S}_{r-\ell+k_i}$, using the definition of $\mathcal{V}_{r-\ell}(\Phi)$ for $\Phi \in \mathcal{F}$. Moreover, $\mathrm{Span}(\mathcal{F}) \circ \sigma = F_i \circ \sigma \subset W'$, which means that $W' \in \mathcal{E}_{i,r} \circ \mathrm{Stab}(T)$. Consequently, the set of $\mathcal{E}_{i,r}$'s satisfies $\mathfrak{P}_T$. □

In theory, the larger the groups U_i are, the smaller the $\mathcal{E}_{i,r}$ are. Thus, in theory, we may assume that $U_i = \mathrm{Stab}(T) \cap \mathrm{Stab}(F_i)$. However, due to the method that we use to compute the $\mathcal{E}_{i,r}$'s, the U_i's are defined differently.

If the covering chosen is the set $\{\mathrm{Span}(\emptyset)\}$, we are led to use the trivial covering given by $\mathcal{C}_{r-\ell}(\mathrm{Span}(\emptyset))/\mathrm{Stab}(T)$, which leads to the same number of calls to VecSpHasGoodBasis as in

BDEZStab. If the covering is $\{T\}$: we are led to compute $\mathcal{C}_r(T)/\mathrm{Stab}(T)$, which is equivalent to the naive strategy consisting in computing $\mathscr{S}_r/\mathrm{Stab}(T)$ and the vector spaces containing T. Thus, our approach can be understood as a mixed strategy between BDEZ and the naive algorithm, and we unify these two approaches within a unique framework. Between these two strategies, there exist intermediate strategies given by sets of g subspaces $F_i \subset T$ of dimension k_i. There is pratical limit on their dimension k_i, due to precomputations that are used in our method and which constitute a bottleneck. No automatic method is known to determine, given a vector space T, which subspaces of T should be used specifically: we adapt our method for each T. We provide for the short product, in Section 4.2, an example of such families.

In order to compute a set of the form $\mathcal{C}_{r-\ell+k_i}(F_i)/U_i$ we divide the computation of this set into two steps. Let $\mathcal{F}_i$ be a basis of F_i. Our strategy assumes that $U_i = \mathrm{Stab}(T) \cap \mathrm{Stab}(\mathcal{F}_i) \subset \mathrm{Stab}(T) \cap \mathrm{Stab}(F_i)$. The first step consists in computing

$$\mathcal{C}_{r-\ell+k}(F_i)/\mathrm{Stab}(\mathcal{F}_i).$$

The method used for this step is adapted for the choice $U_i = \mathrm{Stab}(T) \cap \mathrm{Stab}(\mathcal{F}_i)$. So far, we are unable to describe a method computing a similar quotient for a group larger than $\mathrm{Stab}(\mathcal{F}_i)$. The second step applies the action of the left transversal

$$\mathrm{Stab}(\mathcal{F}_i)/\mathrm{Stab}(T) \cap \mathrm{Stab}(\mathcal{F}_i),$$

that we computed with the algorithms proposed in [12] for example. The first step is done with the assumption that we have precomputed the quotient

$$\mathscr{S}_{r-\ell+k}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n).$$

Consequently, given the largest "k" for which we are able to compute $\mathscr{S}_{r-\ell+k}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$, the free families of bilinear forms $\mathcal{F}_i$ of cardinality k_i that we use should satisfy $k_i \leq k$.

We describe in Algorithm CoveringSetsMethod the global strategy to find optimal formulae for T.

Notation 20. *For a free family $\mathcal{F}$ of k bilinear forms and a positive integer d, we let*

$$\tilde{\mathcal{C}}_{d+k}(\mathcal{F}) = \mathcal{C}_{d+k}(\mathrm{Span}(\mathcal{F}))/\mathrm{Stab}(\mathcal{F}).$$

We assume that we have a subspace T and a set of g free families $\mathcal{F}_0, \ldots, \mathcal{F}_{g-1}$ of T such the set $\{\mathrm{Span}(\mathcal{F}_i)\}_i$ is a covering of T. We let, for any $i \in \{0, \ldots, g-1\}$, $\tilde{\mathcal{E}}_{i,r}$ be the set $\tilde{\mathcal{C}}_{r-\ell+k_i}(\mathcal{F}_i)$.

Algorithm 4 CoveringSetsMethod

Input: $T, \{\mathcal{F}_i\}_{0\leq i<g}, \left\{\mathscr{S}_{r-\ell+k_i}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)\right\}_{0\leq i<g}, r$
Output: $\mathscr{S}_{r,T}$

$\mathcal{S} \leftarrow \emptyset$
for $i \in \{0, \ldots, g-1\}$ **do**
  $\mathcal{Q} \leftarrow \tilde{\mathcal{C}}_{r-\ell+k_i}(\mathcal{F}_i)$, obtained from $\mathscr{S}_{r-\ell+k_i}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$
  $\mathcal{L} \leftarrow \mathrm{Stab}(\mathcal{F}_i)/\mathrm{Stab}(T) \cap \mathrm{Stab}(\mathcal{F}_i)$
  for $\sigma \in \mathcal{L}, W \in \mathcal{Q}$ **do**
    if VecSpHasGoodBasis$(T + (W \circ \sigma))$ **then**
      $\mathcal{S} \leftarrow \mathcal{S} \cup \{T + (W \circ \sigma)\}$
    end if
  end for
end for
return $\bigcup_{V\in\mathcal{S}} V \circ \mathrm{Stab}(T)$

This strategy assumes that we have precomputed the quotients

$$\left\{\mathscr{S}_{r-\ell+k_i}/\mathrm{GL}(K^m)\times\mathrm{GL}(K^n)\right\}_i.$$

The cardinality of $\mathscr{S}_{r-\ell+k_i}/\mathrm{GL}(K^m)\times\mathrm{GL}(K^n)$ is smaller than $\#\mathscr{S}_{r-\ell+k_i}$ by a factor at least $\#\,\mathrm{GL}(K^{\min(m,n)})$. We explain how to compute it in Section 5.3. The computation of the quotient $\mathcal{Q}$ on Line 3 is detailed in Section 5.1.

4.2. A covering of the optimal decompositions for the short product

We illustrate our idea with the example of the short product

$$\Pi_\ell : (A,B) \longmapsto A\cdot B \bmod X^\ell = \begin{pmatrix} a_0b_0 \\ a_1b_0+a_0b_1 \\ \vdots \\ a_{\ell-1}b_0+\cdots+a_0b_{\ell-1}\end{pmatrix}.$$

We denote by $\pi_0,\ldots,\pi_{\ell-1}$ the bilinear forms such that

$$\forall i\geq 0,\ \pi_i(A,B)=\sum_{j\in\{0,\ldots,i\}} a_{i-j}b_j$$

and by T_ℓ the subspace $\mathrm{Span}(\pi_0,\ldots,\pi_{\ell-1})$.

In order to produce a covering of the vector spaces W satisfying $T_\ell\oplus W\in\mathscr{S}_{r,T_\ell}$ that we compute with CoveringSetsMethod, we need a covering of T. This covering is given in Proposition 21.

Proposition 21 (Covering of short product)**.** *Let ℓ and $r\geq\ell$. The set $\{\mathrm{Span}(\pi_{\ell-1},\pi_{\ell-2})\}$is a covering of T_ℓ: for any basis $\mathcal{B}$ of T_ℓ, there exists $\sigma\in\mathrm{Stab}(T_\ell)$ and $\mathcal{U}\subset\mathcal{B}$ of cardinality 2 such that*

$$\mathrm{Span}(\mathcal{U})\circ\sigma=\mathrm{Span}(\pi_{\ell-1},\pi_{\ell-2}).$$

Consequently, $\mathcal{C}_{r-\ell+2}(\mathrm{Span}(\pi_{\ell-1},\pi_{\ell-2}))$ produces a covering of $\mathscr{S}_{r,T_\ell}$.

We give in Table 1 the cardinality of coverings of $\mathscr{S}_{r,T_\ell}$ given by Proposition 21 for the example T_3:

set	**cardinality**
$\mathcal{C}_2(\mathrm{Span}(\emptyset))=\mathscr{S}_2$	980
$\mathcal{C}_3(\mathrm{Span}(\pi_2))$	28
$\mathcal{C}_4(\mathrm{Span}(\pi_2,\pi_1))$	6

Table 1: Comparison of the cardinality for $K=\mathbb{F}_2$ of 3 coverings of $\mathscr{S}_{5,T_3}$.

Lemma 22. *The cardinality of the stabilizer of T_ℓ is equal to $(\#K)^{3\ell-4}\cdot(\#K-1)^3$ for $\ell\geq 2$. For any pair (Ψ,Ψ') of elements of T_ℓ such that $\mathrm{rk}(\Psi)=\ell$ and $\mathrm{rk}(\Psi')=\ell-1$, there exists $\sigma\in\mathrm{Stab}(T_\ell)$ such that*

$$(\Psi\circ\sigma,\Psi'\circ\sigma)=(\pi_{\ell-1},\pi_{\ell-2}).$$

Moreover

$$\mathrm{Stab}(\pi_{\ell-1})\cap\mathrm{Stab}(\pi_{\ell-2})\subset\mathrm{Stab}(T_\ell).$$

Proof. It is a consequence of Appendix A.1. □

Proof of Proposition 21. We first observe that for any $\Phi \in \mathrm{Span}(\pi_0, \ldots, \pi_i)$, $\mathrm{rk}(\Phi) \leq i+1$. Therefore, any element of rank ℓ in T_ℓ has a non zero coordinate over $\pi_{\ell-1}$ in its decomposition over the basis $(\pi_0, \ldots, \pi_{\ell-1})$ and, reciprocally, any element having a non zero coordinate over $\pi_{\ell-1}$ has rank ℓ. Thus, a basis $\mathcal{B}$ contains necessarily an element of rank ℓ denoted by Ψ. The element Ψ has a non zero coordinate over $\pi_{\ell-1}$, when we decompose it over $\{\pi_0, \ldots, \pi_{\ell-1}\}$. Similarly, there exists $\Psi' \in \mathcal{B}$ such that there exists $\lambda \in K$ for which $\Psi' - \lambda\Psi$ has rank $\ell - 1$.

We use Lemma 22 to find an element $\sigma \in \mathrm{Stab}(T_\ell)$ such that

$$(\Psi \circ \sigma, \Psi' \circ \sigma) = (\pi_{\ell-1}, \pi_{\ell-2}) \text{ or } (\Psi \circ \sigma, (\Psi - \lambda\Psi') \circ \sigma) = (\pi_{\ell-1}, \pi_{\ell-2}),$$

which concludes. □

In conclusion, we need to compute the following set: $\tilde{\mathcal{C}}_{r-\ell+2}(\{\pi_{\ell-1}, \pi_{\ell-2}\})$. We describe in Section 5 how we perform Line 3 of Algorithm CoveringSetsMethod. The set $\mathcal{L}$ on Line 4 is, for the short product, a set containing one element, which is the identity element of $\mathrm{GL}(K^\ell) \times \mathrm{GL}(K^\ell)$. For other bilinear maps, we use exactly the same ideas: from a bilinear map to another one, the cases implied by Theorem 15 are different. We describe more precisely how it works for the matrix product in Section 6.

5. How to compute subspaces containing specific bilinear forms

We propose in this section a method to compute a covering of $\mathscr{S}_{r,T}$, where T is a target space of dimension ℓ. The covering is a set of subspaces containing a specific set of bilinear forms described as in Section 4 or 6. More specifically, we are interested in computing sets defined as $\tilde{\mathcal{C}}_{r-\ell+k}(\{\Psi_0, \ldots, \Psi_{k-1}\})$, for $\Psi_0, \ldots, \Psi_{k-1}$ bilinear forms of $\mathcal{L}(K^m, K^n; K)$. Those can be described as sets of subspaces of rank $r - \ell + k$ containing a prescribed set $\{\Psi_0, \ldots, \Psi_{k-1}\}$ of bilinear forms, up to the action of $\mathrm{Stab}(\{\Psi_0, \ldots, \Psi_{k-1}\})$.

5.1. General approach

First, our strategy consists in precomputing the quotient $\mathscr{S}_{m,n,r-\ell+k}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$. The cardinality of this quotient is smaller than $\#\mathscr{S}_{m,n,r-\ell+k}$ by construction. We explain how to compute it in Section 5.3. This computation bounds the possible coverings that we consider in our approach.

We need essentially to explain how to compute the quotient $\mathcal{Q}$ in Algorithm CoveringSetsMethod, which is done in Algorithm 5.

Correctness of Algorithm 5. Let W' a representative of an orbit in

$$\tilde{\mathcal{C}}_{r-\ell+k}(\{\Psi_0, \ldots, \Psi_{k-1}\}).$$

There exists σ' and $W \in \mathscr{S}_{r-\ell+k}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ such that $W \circ \sigma' = W'$. Thus, we have $\{\Psi_0, \ldots, \Psi_{k-1}\} \circ \sigma'^{-1} \subset W$ and the set $\left\{\Psi_0 \circ \sigma'^{-1}, \ldots, \Psi_{k-1} \circ \sigma'^{-1}\right\}$ satisfies the predicate on Line 4. Any σ such that $\{\Psi_0, \ldots, \Psi_{k-1}\} \circ \sigma'^{-1} \circ \sigma = \{\Psi_0, \ldots, \Psi_{k-1}\}$ satisfies

$$\sigma \in \sigma' \circ \mathrm{Stab}(\{\Psi_0, \ldots, \Psi_{k-1}\}),$$

which means that an element of $W \circ \sigma' \circ \mathrm{Stab}(\{\Psi_0, \ldots, \Psi_{k-1}\}) = W' \circ \mathrm{Stab}(\{\Psi_0, \ldots, \Psi_{k-1}\})$ is included in the list returned by Algorithm 5. Thus, the list returned contains at least one representative per orbit of $\mathcal{Q}$.

Algorithm 5 IntermediateSetViaQuotientComputation

Input: $\mathscr{S}_{m,n,r-\ell+k}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n), \Psi_0, \ldots, \Psi_{k-1}$
Output: One representative per orbit of $\mathcal{Q}$, defined as above
1: $\mathcal{L} \leftarrow \emptyset$
2: **for** $W \in \mathscr{S}_{m,n,r-\ell+k}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ **do**
3: **for** $\{\{\Phi_0, \ldots, \Phi_{k-1}\} \subset W \mid \forall t,\ \mathrm{rk}(\Phi_t) = \mathrm{rk}(\Psi_t)\}/\mathrm{Stab}(W)$ **do**
4: **if** $\exists \sigma \in \mathrm{GL}(K^m) \times \mathrm{GL}(K^n),\ \{\Phi_0, \ldots, \Phi_{k-1}\} \circ \sigma = \{\Psi_0, \ldots, \Psi_{k-1}\}$ **then**
5: $\mathcal{L} \leftarrow \mathcal{L} \cup \{W \circ \sigma\}$
6: **end if**
7: **end for**
8: **end for**
9: **return** $\mathcal{L}$

If we have in the list two elements in the same orbit, it would mean that there exists two subsets $\{\Phi_0, \ldots, \Phi_{k-1}\}$ and $\{\Phi'_0, \ldots, \Phi'_{k-1}\}$ of a subspace W such that $\{\Phi_0, \ldots, \Phi_{k-1}\}$ and $\{\Phi'_0, \ldots, \Phi'_{k-1}\}$ are sent via σ and σ', two elements of $\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$, on $\{\Psi_0, \ldots, \Psi_{k-1}\}$, and there exists $\gamma \in \mathrm{Stab}(\{\{\Psi_0, \ldots, \Psi_{k-1}\}\})$ such that $W \circ \sigma = W \circ \sigma' \circ \gamma$.

Thus, $\sigma' \circ \gamma \circ \sigma^{-1} \in \mathrm{Stab}(W)$, which means that $\{\Phi_0, \ldots, \Phi_{k-1}\}$ and $\{\Phi'_0, \ldots, \Phi'_{k-1}\}$ are in the same orbit for the group $\mathrm{Stab}(W)$ and this is not allowed by the definition of the quotient on Line 3. □

Testing the predicate of Line 4 is a problem generalizing the problem of [7, Ch. 19] and [15]: given two pairs (M_0, M_1) and (N_0, N_1) of $(\mathcal{M}_{m,n})^2$, determine whether there exists two invertible matrices X and Y such that $(X^{\mathrm{T}} M_0 Y, X^{\mathrm{T}} M_1 Y) = (N_0, N_1)$, which is done by computing a Weierstrass-Kronecker canonical form for (M_0, M_1). When we consider more than 2 matrices, for example 3 matrices (M_0, M_1, M_2) sent on (N_0, N_1, N_2), we compute (X, Y) such that (M_0, M_1) is sent on (N_0, N_1) and we compose it with elements of $\mathrm{Stab}\, M_0 \cap \mathrm{Stab}\, M_1/\mathrm{Stab}\, M_2$, computed with the algorithms proposed in [12] for example. The complexity for finding all the automorphisms σ in IntermediateSetViaQuotientComputation is bounded by the cardinality of $\mathscr{S}_{r-\ell+k}$ (which is comparable to BDEZ) by construction, and is hard to estimate more precisely. In our applications, it appears to be negligible compared to BDEZ.

5.2. Application to the short product

We come back to the example given in Section 4 corresponding to the short product. We remind that T_ℓ is the subspace obtained from the bilinear map given by the short product modulo ℓ and that we need to compute the set $\mathcal{Q}_{\ell,r-\ell} = \tilde{\mathcal{C}}_{r-\ell+2}(\{\pi_{\ell-1}, \pi_{\ell-2}\})$ for a given integer r.

If we take $\ell = 3$, we can represent π_2 and π_1, in a basis which is not the canonical basis (simplifying the representation for the short product), by the matrices

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Thus, for a given couple (N_0, N_1) of matrices representing bilinear forms of a subspace $W \in \mathscr{S}_{\ell,\ell,r-\ell+2}/\mathrm{GL}(K^\ell) \times \mathrm{GL}(K^\ell)$, we are looking for invertible matrices X and Y such that

$$X^{\mathrm{T}} N_0 Y = I \text{ and } X^{\mathrm{T}} N_1 Y = M,$$

Algorithm 6 IntermediateSetViaQuotientComputation (Short product)

Input: $\mathscr{S}_{\ell,\ell,r-\ell+2}/\mathrm{GL}(K^\ell) \times \mathrm{GL}(K^\ell)$
Output: One representative per orbit of $\mathcal{Q}_{\ell,r-\ell}$, defined as above
1: $\mathcal{L} \leftarrow \emptyset$
2: **for** $W \in \mathscr{S}_{\ell,\ell,r-\ell+2}/\mathrm{GL}(K^\ell) \times \mathrm{GL}(K^\ell)$ **do**
3: **for** $\Psi \in \{\Phi \in W \mid \mathrm{rk}(\Phi) = \ell\}/\mathrm{Stab}(W)$ **do**
4: Let σ such that $\Psi \circ \sigma = \pi_{\ell-1}$ ▷ We obtain σ via a Gauss reduction
5: $W' \leftarrow W \circ \sigma$
6: **for** $\Psi' \in \{\Phi \in W' \mid \mathrm{rk}(\Phi) = \ell - 1\}/\mathrm{Stab}(W') \cap \mathrm{Stab}(\pi_{\ell-1})$ **do**
7: **if** $\exists \sigma' \in \mathrm{Stab}(\pi_{\ell-1}),\ \Psi' \circ \sigma' = \pi_{\ell-2}$ **then** ▷ Using that $\pi_{\ell-2}$ and Ψ' are similar
8: $\mathcal{L} \leftarrow \mathcal{L} \cup \{W \circ \sigma \circ \sigma'\}$
9: **end if**
10: **end for**
11: **end for**
12: **end for**
13: **return** $\mathcal{L}$

which is done in Algorithm 6. As it is precised on Line 4, we find X and Y such that $X^{\mathrm{T}} N_0 Y = I$ via Gauss reduction. Then, we need to check whether $X^{\mathrm{T}} B Y$ and M are similar or not ($(X^{\mathrm{T}} N_1 Y)^\ell$ should be the null matrix), as done on Line 7.

Once we have computed $\mathcal{Q}_{\ell,r-\ell}$, it remains to compute the left transversal

$$\mathcal{L}_\ell = \mathrm{Stab}(\{\pi_{\ell-1}, \pi_{\ell-2}\})/\mathrm{Stab}(T_\ell) \cap \mathrm{Stab}(\{\pi_{\ell-1}, \pi_{\ell-2}\})$$

and to compute $\mathcal{Q}_{\ell,r-\ell} \circ \mathcal{L}_\ell$. According to Lemma 22, we have $\#\mathcal{L}_\ell = 1$, which means that Algorithm 6 returns actually $\tilde{\mathcal{C}}_{r-\ell+2}(\{\pi_{\ell-1}, \pi_{\ell-2}\}) \circ \mathcal{L}$.

In terms of complexity, we do not have explicit bounds. However, we can state that the complexity depends linearly on $\#\mathscr{S}_{r-\ell+2,\ell,\ell}/\mathrm{GL}(K^\ell) \times \mathrm{GL}(K^\ell)$ and on the number of pairs of bilinear forms (Φ, Ψ) per element of $\mathscr{S}_{r-\ell+2,\ell,\ell}/\mathrm{GL}(K^\ell) \times \mathrm{GL}(K^\ell)$ such that $\mathrm{rk}(\Phi) = \ell$ and $\mathrm{rk}(\Psi) = \ell - 1$.

5.3. Computing the orbits of vector spaces of bilinear forms

In this section, we propose an approach for computing the set $\mathscr{S}_{m,n,d}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$, required by the algorithm described in Section 5.1. This step implies the kind of reductions that are applied in Section 4.1. Its cost is at least exponential in d, m and n and difficult to proceed.

Notation 23. *We denote by Ω_d the quotient $\mathscr{S}_{d,d,d}/\mathrm{GL}(K^d) \times \mathrm{GL}(K^d)$ for any $d \geq 1$.*

First, we describe how we represent elements of $\mathscr{S}_{m,n,d}$ and we prove that given the knowledge of Ω_d we can deduce the elements of $\mathscr{S}_{m,n,d}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ for any m and n from this precomputation.

Let W be an element of $\mathscr{S}_{m,n,d}$. There exists d rank-one bilinear forms $\phi_t : (\mathbf{a}, \mathbf{b}) \mapsto \alpha_t(\mathbf{a}) \cdot \beta_t(\mathbf{b})$ such that $W = \mathrm{Span}\left((\phi_t)_{t \in \{1,\ldots,d\}}\right)$. In the canonical basis of K^m and K^n, we represent α_t and β_t as matrices of $\mathcal{M}_{1,m}$ and $\mathcal{M}_{1,n}$. Thus, there exists two matrices U and V, whose rows are respectively given by the linear forms α_t and β_t, and W can be represented by the couple (U, V). Such a representation is not unique (for example, any permutation of the rows of (U, V) gives a valid representation). In particular, for a couple of matrices (U, V) representing some vector space W, there exists $\sigma = \sigma_x \times \sigma_y$ in $\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ such that the couple of matrices $(U', V') = (U \circ \sigma_x, V \circ \sigma_y)$ representing $W \circ \sigma$ is the reduced column echelon forms of the matrices U and V.

Example 24. *Let us consider the vector space W of $\mathscr{S}_{3,4,6}$ generated by the rank-one bilinear forms represented by*

$$M_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, M_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, M_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$
$$M_4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, M_5 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, M_6 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The couple of matrices (U, V) associated to W is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Moreover, assuming that we have a representation of the elements of $\mathscr{S}_{d,d,d}/\mathrm{GL}(K^d) \times \mathrm{GL}(K^d)$ in terms of couples of matrices (U, V) in reduced column echelon form, a set of representatives for

$$\mathscr{S}_{m,n,d}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$$

can be seen as matrices (U', V') in reduced column echelon form and for which there exists matrices $(U, V) \in \mathcal{M}^2_{d,d}$ obtained by a zero-padding. We obtain all the elements of

$$\mathscr{S}_{m,n,d}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$$

by considering the subset of $\Omega_d = \mathscr{S}_{d,d,d}/\mathrm{GL}(K^d) \times \mathrm{GL}(K^d)$ of elements represented by matrices (U, V) in reduced column echelon form such that $\mathrm{rk}(U) \leq \min(m, d)$ and $\mathrm{rk}(V) \leq \min(n, d)$.

Our strategy consists in deducing Ω_d from the computation of Ω_{d-1}. Algorithm 7 describes this strategy: for each vector space W of Ω_{d-1}, we extend it to a vector space of $\mathcal{L}(K^d, K^d; K)$ by padding with zeros, and we consider the vector spaces $W \oplus \mathrm{Span}(\phi)$ that can be obtained by adding an element ϕ of rank one. We remove from the set of $W \oplus \mathrm{Span}(\phi)$ the vector spaces that are isomorphic via an isomorphism test. We determine whether two vector spaces W' and W are isomorphic if there exists a basis of W' such that the corresponding couple of matrices (U', V') in reduced column echelon form is equal to (U, V). The complexity of this approach depends on the number of bases of rank-one bilinear forms of W, which is, compared to d, not large generically.

Algorithm 7 IterativeQuotientsComputation

Input: Ω_{d-1}, a set $\mathcal{G}$ of rank-one bilinear forms
Output: Ω_d

1: $\widehat{\Omega}_{d-1} \leftarrow \mathsf{Extend}(\Omega_{d-1})$ ▷ We compute extensions of elements of Ω_{d-1} in $\mathcal{L}(K^d, K^d; K)$
2: $\mathcal{L} \leftarrow \emptyset$
3: **for** $W \in \widehat{\Omega}_{d-1}$ **do**
4: $\quad \mathcal{H} \leftarrow \mathcal{G}/_{\mathrm{Stab}\, W}$
5: $\quad$ **for** $h \in \mathcal{H}$ **do**
6: $\quad\quad \mathcal{L} \leftarrow \mathcal{L} \cup \{W \oplus \mathrm{Span}(h)\}$
7: $\quad$ **end for**
8: **end for**
9: **return** $\mathcal{L}/\mathrm{GL}(K^d) \times \mathrm{GL}(K^d)$ ▷ We remove isomorphic vector spaces in $\mathcal{L}$

The naive algorithm checking for each pair of elements of the set $\mathcal{L}$ whether they are isomorphic, computed in Algorithm 7, can be improved. Indeed, we propose to compute invariants for the group action induced by $\mathrm{GL}(K^d) \times \mathrm{GL}(K^d)$ and to compare subspaces having the same invariants. For example, for $W \in \mathscr{S}_{d,d,d}$, we consider the polynomial $P(W) = \sum_{0 \leq t \leq d} p_t(W) X^t$ such that

$$\forall t \geq 0,\ p_t(W) = \#\{\phi \in W |\ \mathrm{rk}(\phi) = t\}.$$

Therefore, for any $\sigma \in \mathrm{GL}(K^d) \times \mathrm{GL}(K^d)$, $P(W \circ \sigma) = P(W)$.

We have been able to compute Ω_d for $d \in \{1, \ldots, 8\}$ with an implementation in Magma V2.21-3 [5][1]. The timings are described in Table 2.

set	Ω_1	Ω_2	Ω_3	Ω_4	Ω_5	Ω_6	Ω_7	Ω_8
cardinality	1	3	9	31	141	969	$11,289$	$265,577$
time (s)	0	$4.0 \cdot 10^{-2}$	$6.0 \cdot 10^{-2}$	$1.8 \cdot 10^{-1}$	1.5	$1.8 \cdot 10$	$4.7 \cdot 10^2$	$1.8 \cdot 10^4$

Table 2: Timings for our approach to compute the sets Ω_d over $K = \mathbb{F}_2$ on a single core of a 3.3 GHz Intel Core i5-4590.

It would be interesting to obtain an upper bound on $\#\Omega_d$ with the good order of magnitude. Indeed, we are able to say for instance that $\#\Omega_d$ is bounded by the quantity

$$\left(\#K^d - 1\right)^2 \cdot \#\Omega_{d-1},$$

corresponding to the number of possible rank-one bilinear forms that we add to elements of Ω_{d-1} to obtain an element of Ω_d. This formula leads recursively to the following bound:

$$\#\Omega_d \leq \left(\prod_{t \in \{1,\ldots,d\}} (\#K^t - 1) \right)^2.$$

However, this upper bound differs by a huge factor from the true cardinality of Ω_d and cannot consequently be used in a complexity analysis.

To conclude, we provide in Figure 3 how subspaces of Ω_3 over $\mathbb{F}_2$ are related to Ω_2 and Ω_1 by using its poset structure. We represent an element of Ω_d by a couple of matrices (U, V) of $M^2_{d,d}$.

[1] The code of this implementation can be found at the address http://karancode.gforge.inria.fr

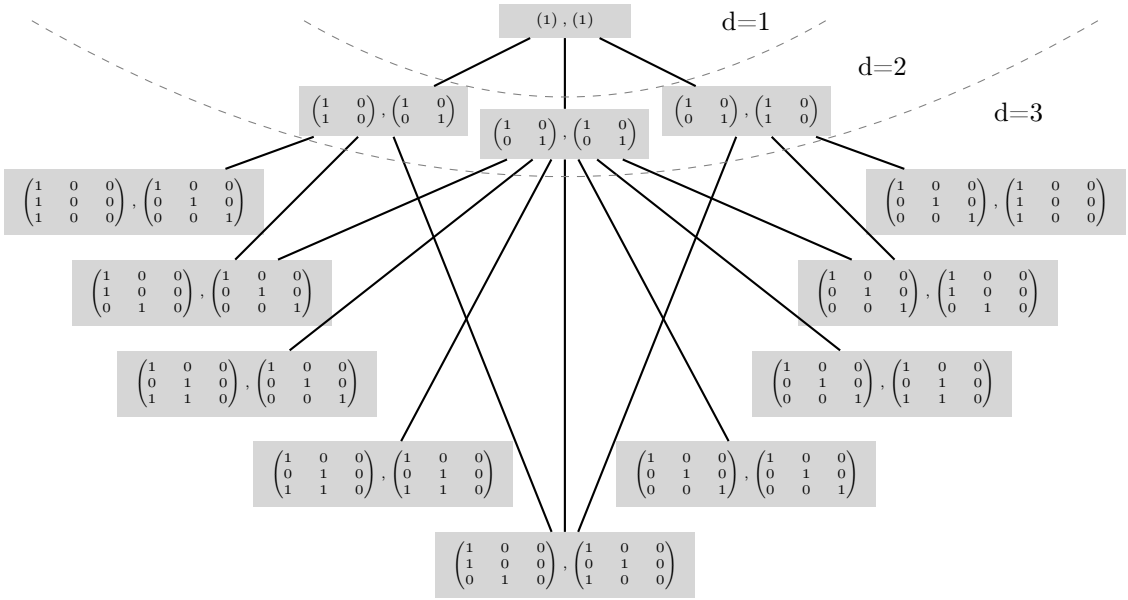

Figure 3: Partially ordered structure of the Ω_d for $d \leq 3$

6. Application to the matrix product 3×2 by 2×3 over $\mathbb{F}_2$

We describe in this section how to apply the idea of Section 4 to the case of matrix product. Although Section 6.1 can be considered on any finite field K, the covering sets given in the following section assumes that we are working with $K = \mathbb{F}_2$. We focus our interest on the special case given by the bilinear map

$$\begin{array}{rccc} \Pi_{3,2,3}: & \mathcal{M}_{3,2}(\mathbb{F}_2) \times \mathcal{M}_{2,3}(\mathbb{F}_2) & \longrightarrow & \mathcal{M}_{3,3}(\mathbb{F}_2) \\ & (A, B) & \longmapsto & A \cdot B \end{array}.$$

The rank of this bilinear map is known [13]: it has rank 15. However, all the optimal formulae are not known. We denote by $\pi_{i,j}$ the bilinear forms such that $\pi_{i,j}(A, B)$ is the coefficient (i, j) of $\Pi_{3,2,3}(A, B)$ for $i, j \in \{0, 1, 2\}$. The elements $\pi_{i,j}$ satisfy $\pi_{i,j}(A, B) = a_{i,0}b_{0,j} + a_{i,1}b_{1,j}$.

The target subspace of $\mathcal{L}(K^6, K^6; K)$ considered is denoted by

$$T_{3,2,3} = \mathrm{Span}((\pi_{i,j})_{i,j\in\{0,1,2\}}).$$

The approach proposed in this section can be generalized to any matrix product (albeit at the expanse of combinatorial blowup).

6.1. Structure of matrix product

The elements of $T_{3,2,3}$ can be represented as matrices of $\mathcal{M}_{6,6}$ divided in blocks of size 2×2 equal to

$$\begin{pmatrix} \delta & 0 \\ 0 & \delta \end{pmatrix}, \delta \in K.$$

Let (e_i), (f_h) and (g_j) be the canonical bases of K^3, K^2 and K^3. The subspace $T_{3,2,3}$ can be easily characterized with the tensor notation: it is generated by the vectors, for $i, j \in \{0, 1, 2\}$,

$$e_i \otimes f_0 \otimes f_0 \otimes g_j + e_i \otimes f_1 \otimes f_1 \otimes g_j.$$

Consequently, this space is isomorphic to $\mathcal{M}_{3,3} \otimes I_2$, where I_2 is the identity matrix.

Proposition 25. *For the group action $M \cdot (X, Y) \mapsto X^{\mathrm{T}} M Y$, the subgroup stabilizing the vector space $T_{3,2,3}$ can be described as the group given by the couples $(P \otimes R, Q \otimes (R^{-1}))$ for $P \in \mathrm{GL}_p$, $R \in \mathrm{GL}_q$, and $Q \in \mathrm{GL}_r$.*

Proof. It is a consequence of Appendix A.2. □

In particular, the elements of $T_{3,2,3}$ of a given rank are in the same orbit under the action of $\mathrm{Stab}(T_{3,2,3})$.

6.2. Decomposition of the matrix product $(3, 2, 3)$

We produce a covering of $T_{3,2,3}$ given by five subspaces of $T_{3,2,3}$. Let $\mathcal{B}$ be a basis of $T_{3,2,3}$.

- If there exists an element Φ of rank 6 in $\mathcal{B}$, then there exists $\sigma \in \mathrm{Stab}(T_{3,2,3})$ such that $\pi_{0,0} + \pi_{1,1} + \pi_{2,2} \in \mathcal{B} \circ \sigma$. Otherwise, any element Φ of $\mathcal{B}$ has rank smaller or equal to 4 and we have to distinguish two cases.
- If there exists an element Φ of rank 4, there exists σ such that $\pi_{0,0} + \pi_{1,1} \in \mathcal{B} \circ \sigma$ and, consequently, there exists another element $\Phi' \in \mathcal{B}$ of rank 2 or 4 whose coordinate over $\pi_{2,2}$ in the basis $(\pi_{i,j})_{i,j}$ is not null: we need to look at the possible orbits in which Φ' is included under the action of the subgroup of $\mathrm{Stab}(T_{3,2,3})$ preserving the fact that Φ is in the orbit of $\pi_{0,0} + \pi_{1,1}$. We can prove that there exists 3 such orbits and that there exists $\sigma \in \mathrm{Stab}(T_{3,2,3})$ and $\mathcal{U} \subset \mathcal{B}$ of cardinality 2 such that

$$\mathcal{U} \circ \sigma \in \begin{cases} \{\pi_{0,0} + \pi_{1,1}, \pi_{0,1} + \pi_{2,2}\} \\ \text{or} \\ \{\pi_{0,0} + \pi_{1,1}, \pi_{1,1} + \pi_{2,2}\} \\ \text{or} \\ \{\pi_{0,0} + \pi_{1,1}, \pi_{2,2}\}. \end{cases}$$

- All the elements of $\mathcal{B}$ have rank 2 and there exists $\mathcal{U} \subset \mathcal{B}$ and $\sigma \in \mathrm{Stab}(T_{3,2,3})$ such that

$$\mathcal{U} \circ \sigma = \{\pi_{0,0}, \pi_{1,1}, \pi_{2,2}\}.$$

In conclusion, we consider 5 intermediate sets:

- $\tilde{\mathcal{C}}_7(\{\pi_{0,0} + \pi_{1,1} + \pi_{2,2}\})$, set of subspaces containing the diagonal element $\pi_{0,0} + \pi_{1,1} + \pi_{2,2}$,
- $\tilde{\mathcal{C}}_8(\{\pi_{0,0} + \pi_{1,1}, \pi_{0,1} + \pi_{2,2}\})$, set of subspaces containing $\pi_{0,0} + \pi_{1,1}$ and $\pi_{0,1} + \pi_{2,2}$,
- $\tilde{\mathcal{C}}_8(\{\pi_{0,0} + \pi_{1,1}, \pi_{1,1} + \pi_{2,2}\})$, set of subspaces containing $\pi_{0,0} + \pi_{1,1}$ and $\pi_{1,1} + \pi_{2,2}$,
- $\tilde{\mathcal{C}}_8(\{\pi_{0,0} + \pi_{1,1}, \pi_{2,2}\})$, set of subspaces containing $\pi_{0,0} + \pi_{1,1}$ and $\pi_{2,2}$,
- $\tilde{\mathcal{C}}_9(\{\pi_{0,0}, \pi_{1,1}, \pi_{2,2}\})$, set of subspaces containing $\pi_{0,0}$, $\pi_{1,1}$ and $\pi_{2,2}$.

6.3. Taking the Hamming weight into consideration

We describe in this section a trick allowing one to speed-up the execution of our approach for the matrix product. However, this part is technical and can be skipped on a first read.

We note that in the sets proposed in Section 6.2, it might happen that there exists $W' \in \tilde{\mathcal{C}}_7(\{\pi_{0,0}+\pi_{1,1}+\pi_{2,2}\})$ and $W \in \tilde{\mathcal{C}}_9(\{\pi_{0,0},\pi_{1,1},\pi_{2,2}\})$ such that $T_{3,2,3}+W = T_{3,2,3}+W'$. Thus, we want to avoid in $\tilde{\mathcal{C}}_9(\{\pi_{0,0},\pi_{1,1},\pi_{2,2}\})$ the exploration of vector spaces $W \in \mathscr{S}_9$ such that there exists $W' \subset W$ belonging to other explored sets and satisfying $T+W' \in \mathscr{S}_{15}$.

For this purpose, we need to look at a basis $\mathcal{B}$ of rank-one bilinear forms for each element W of the set $\tilde{\mathcal{C}}_9(\{\pi_{0,0},\pi_{1,1},\pi_{2,2}\})$ and to consider the decomposition of $\pi_{0,0}$, $\pi_{1,1}$ and $\pi_{2,2}$ over this basis.

Definition 26 (Hamming weight for $\mathscr{S}_d$)**.** *Let $W \in \mathscr{S}_d$ and $\mathcal{B} = (\psi_0,\dots,\psi_{d-1})$ a basis of rank-one bilinear forms of W. Any $x \in W$ has a unique decomposition over $\mathcal{B}$:*

$$x = \sum_t \lambda_t \cdot \psi_t.$$

We define its Hamming weight over $\mathcal{B}$ as

$$\mathbb{H}_{\mathcal{B}}(x) = \#\{t \in \{0,\dots,d-1\} \mid \lambda_t \neq 0\}.$$

We can extend the definition of the Hamming weight to any subset $\mathcal{S}$ of W:

$$\mathbb{H}_{\mathcal{B}}(\mathcal{S}) = \min(\{\#I \mid I \subset \{0,\dots,d-1\}, \mathcal{S} \subset \mathrm{Span}((\psi_t)_{t\in I})\}).$$

Let W be a subspace such that $W \in \tilde{\mathcal{C}}_9(\{\pi_{0,0},\pi_{1,1},\pi_{2,2}\})$ and $T_{3,2,3}+W \in \mathscr{S}_{15}$ and let $\mathcal{B}$ be a basis of $T_{3,2,3}+W$ composed of rank-one bilinear forms obtained by taking a basis of W and by completing it in a basis of $T_{3,2,3}+W$. We prove that we can assume that

$$\mathbb{H}_{\mathcal{B}}(\pi_{0,0}+\pi_{1,1}+\pi_{2,2}) = \mathbb{H}_{\mathcal{B}}(\pi_{0,0})+\mathbb{H}_{\mathcal{B}}(\pi_{1,1})+\mathbb{H}_{\mathcal{B}}(\pi_{2,2}) \text{ and } \mathbb{H}_{\mathcal{B}}(\pi_{0,0}+\pi_{1,1}+\pi_{2,2}) > 6.$$

Theorem 27. *If $\mathbb{H}_{\mathcal{B}}(\pi_{0,0}+\pi_{1,1}+\pi_{2,2}) \neq \mathbb{H}_{\mathcal{B}}(\pi_{0,0})+\mathbb{H}_{\mathcal{B}}(\pi_{1,1})+\mathbb{H}_{\mathcal{B}}(\pi_{2,2})$, there exists $W' \subset W$ such that*

$$\exists \sigma \in \mathrm{Stab}(T_{3,2,3}),\ W' \circ \sigma \in \begin{cases} \mathcal{C}_7(\mathrm{Span}(\pi_{0,0}+\pi_{1,1}+\pi_{2,2})) \\ \qquad\qquad or \\ \mathcal{C}_8(\mathrm{Span}(\pi_{0,0}+\pi_{1,1},\pi_{0,1}+\pi_{2,2})) \\ \qquad\qquad or \\ \mathcal{C}_8(\mathrm{Span}(\pi_{0,0}+\pi_{1,1},\pi_{2,2})) \end{cases}$$

and

$$T_{3,2,3}+W' \in \mathscr{S}_{15}.$$

Proof. We have by hypothesis $\mathbb{H}_{\mathcal{B}}(\pi_{0,0}+\pi_{1,1}+\pi_{2,2}) < \mathbb{H}_{\mathcal{B}}(\pi_{0,0})+\mathbb{H}_{\mathcal{B}}(\pi_{1,1})+\mathbb{H}_{\mathcal{B}}(\pi_{2,2})$. Thus, there exist two elements $\Psi \in \mathcal{B}$ and $\Phi \in \{\pi_{0,0},\pi_{1,1},\pi_{2,2}\}$ such that the coordinate of Φ on Ψ is not zero and the coordinates of $\pi_{0,0}+\pi_{1,1}+\pi_{2,2}$ on Ψ is zero. By considering the vector space $W' = \mathrm{Span}(\mathcal{B}-\{\Psi\})$, we have $W' \subset W$, $\pi_{0,0}+\pi_{1,1}+\pi_{2,2} \in W'$ and $\Phi \notin W'$, which means that $\dim(W') \in \mathscr{S}_8$. We have

$$\dim(T_{3,2,3} \cap W') = 2 < 3 = \dim(T_{3,2,3} \cap W),$$

which means that $\dim(T_{3,2,3}+W') = 15$ and $T_{3,2,3}+W' = T_{3,2,3}+W \in \mathscr{S}_{15}$.

If there exists in $T_{3,2,3} \cap W'$ two elements Φ_1 and Φ_2 of rank smaller or equal to 4 such that $\Phi_1 + \Phi_2 = \pi_{0,0} + \pi_{1,1} + \pi_{2,2}$, then

$$\exists \sigma \in \mathrm{Stab}(T_{3,2,3}),\ W' \circ \sigma \in \begin{cases} \mathcal{C}_8(\mathrm{Span}(\pi_{0,0} + \pi_{1,1}, \pi_{0,1} + \pi_{2,2})) \\ \text{or} \\ \mathcal{C}_8(\mathrm{Span}(\pi_{0,0} + \pi_{1,1}, \pi_{2,2})) \end{cases}.$$

Otherwise, there exists $W'' \subset W'$ such that

$$\exists \sigma \in \mathrm{Stab}(T_{3,2,3}),\ W'' \circ \sigma \in \mathcal{C}_7(\mathrm{Span}(\pi_{0,0} + \pi_{1,1} + \pi_{2,2}))$$

and $T_{3,2,3} + W'' \in \mathscr{S}_{15}$, which concludes. □

We prove in Appendix B that we can assume $\mathbb{H}_{\mathcal{B}}(\pi_{0,0} + \pi_{1,1} + \pi_{2,2}) > 6$.

7. Experimental results

An implementation in Magma V2.21-3 [5] of the algorithms presented in the previous sections has been done. We compare in this section the timings obtained from various instances of the bilinear rank problem for these different algorithms. Our Magma implementation of the algorithm described in [1] is clearly slower than the original C version. However, since we are interested in the speed-up obtained from our work, we need a fair approach. We show in particular that Algorithm BDEZStab, although it has not been written in a multi-threaded version and in C, improves considerably on the timings estimated in [1]. The new algorithm proposed in the current article is denoted by CoveringSetsMethod: compared to Algorithm BDEZStab, it constitutes a huge speed-up on particular instances of bilinear rank problems among which the matrix product, discussed in Sections 7.2 and 7.3, and the short product, discussed in Section 7.4. All the timings presented in this section have been done on a single core 3.3 GHz Intel Core i5-4590.

7.1. Recursive approach

We need a few notations to denote the various bilinear maps we are interested in:

- $\mathsf{MatProduct}_{(p,q,r)}$ denotes the product of matrices $p \times q$ by $q \times r$,
- $\mathsf{ShortProduct}_\ell$ denotes the short product of polynomials of degree ℓ,
- $\mathsf{CirculantProduct}_\ell$ the product of polynomials modulo $X^\ell - 1$.

We describe in Table 3 timings for various bilinear maps and the implementations of BDEZ and BDEZStab. The number of tests represents the number of calls to VecSpHasGoodBasis.

It is possible to estimate the time it would take to obtain a result for a bilinear rank problem out of reach for BDEZ or BDEZStab. Indeed, if we run Algorithm BDEZ for a given bilinear map with an estimated rank equal to r, we get a certain number of tests $\mathcal{N}_{r-\ell}$ (ℓ is the dimension of the vector space obtained from the original bilinear map). We consider the ratio $\frac{\mathcal{N}_{r-\ell}}{\mathcal{N}_{r-\ell-1}}$ to guess $\mathcal{N}_{r-\ell+1}$. Assuming that this ratio decreases with r, which seems to hold empirically, we have

$$\mathcal{N}_{r-\ell+1} \leq \frac{\mathcal{N}_{r-\ell}}{\mathcal{N}_{r-\ell-1}} \cdot \mathcal{N}_{r-\ell}. \tag{3}$$

bilinear map	rank	algorithm	nb. of tests	time (s)
$\mathsf{MatProduct}_{(2,2,2)}$	7	BDEZ	$1.05 \cdot 10^6$	$8.5 \cdot 10$
		BDEZStab	$6.8 \cdot 10^3$	$5.0 \cdot 10^{-1}$
$\mathsf{MatProduct}_{(3,2,3)}$	15	BDEZ	$9.2 \cdot 10^{19}$ (est.)	$1.1 \cdot 10^{17}$ (est.)
		BDEZStab	$2.6 \cdot 10^{13}$ (est.)	$3.4 \cdot 10^{10}$ (est.)
		CoveringSetsMethod	$\mathbf{1.6 \cdot 10^9}$	$\mathbf{8.5 \cdot 10^5}$
$\mathsf{MatProduct}_{(2,3,2)}$	11	BDEZ	$2.3 \cdot 10^{23}$ (est.)	$2.7 \cdot 10^{20}$ (est.)
		BDEZStab	$4.6 \cdot 10^{18}$ (est.)	$5.4 \cdot 10^{15}$ (est.)
		CoveringSetsMethod	$\mathbf{6.3 \cdot 10^{10}}$	$\mathbf{4.1 \cdot 10^6}$
$\mathsf{ShortProduct}_3$	5	BDEZ	$5.9 \cdot 10^2$	$1.4 \cdot 10^{-1}$
		BDEZStab	$3.4 \cdot 10$	0.0
$\mathsf{ShortProduct}_4$	8	BDEZ	$5.2 \cdot 10^7$	$4.3 \cdot 10^3$
		BDEZStab	$3.1 \cdot 10^5$	$2.7 \cdot 10$
		CoveringSetsMethod	$\mathbf{2.8 \cdot 10^2}$	$\mathbf{3.0}$
$\mathsf{ShortProduct}_5$	11	BDEZ	$1.8 \cdot 10^{16}$ (est.)	$5.7 \cdot 10^{12}$ (est.)
		BDEZStab	$6.9 \cdot 10^{11}$ (est.)	$2.2 \cdot 10^8$ (est.)
		CoveringSetsMethod	$\mathbf{6.3 \cdot 10^6}$	$\mathbf{2.4 \cdot 10^3}$
$\mathsf{ShortProduct}_6$	14	BDEZ	$3.9 \cdot 10^{26}$ (est.)	$4.7 \cdot 10^{23}$ (est.)
		BDEZStab	$2.0 \cdot 10^{19}$ (est.)	$2.7 \cdot 10^{16}$ (est.)
$\mathsf{CirculantProduct}_3$	4	BDEZ	36	0.0
		BDEZStab	6	$0.1 \cdot 10^{-2}$
$\mathsf{CirculantProduct}_4$	8	BDEZ	$5.2 \cdot 10^7$	$4.3 \cdot 10^3$
		BDEZStab	$3.1 \cdot 10^5$	$2.7 \cdot 10$
$\mathsf{CirculantProduct}_5$	10	BDEZ	$4.0 \cdot 10^{13}$ (est.)	$1.2 \cdot 10^{10}$ (est.)
		BDEZStab	$1.0 \cdot 10^{10}$ (est.)	$3.5 \cdot 10^6$ (est.)
		CoveringSetsMethod	$\mathbf{8.8 \cdot 10^8}$	$\mathbf{5.4 \cdot 10^3}$
$\mathsf{CirculantProduct}_6$	12	BDEZ	$1.0 \cdot 10^{20}$ (est.)	$1.3 \cdot 10^{17}$ (est.)
		BDEZStab	$1.1 \cdot 10^{15}$ (est.)	$1.5 \cdot 10^{12}$ (est.)

Table 3: Timings obtained with Algorithm BDEZ and BDEZStab for various bilinear maps over $K = \mathbb{F}_2$.

Thus, we are able to predict timings for bilinears indicated in Table 3 via to this assumption, which allows us to compare Algorithm BDEZ to other approaches for problems of larger sizes. We estimate the number of tests by computing

$$\frac{\mathcal{N}_1}{\mathcal{N}_0} \cdot \frac{\mathcal{N}_2}{\mathcal{N}_1} \cdots \left(\frac{\mathcal{N}_t}{\mathcal{N}_{t-1}}\right)^{r-\ell-t}$$

where $r - \ell$ is the difference $\mathrm{rk}(T) - \dim(T)$ for T representing a bilinear map. The time can be estimated with a similar technique. We observe that the speed-up seems to match with $\#\,\mathrm{Stab}(T)$, which is what was expected. The computations in Table 3 relying on BDEZStab that are estimated have not been effectively done because we focused on the implementation of CoveringSetsMethod, producing more results.

It is not clear how to estimate timings for our approach CoveringSetsMethod beyond what has been done and reported in Table 3. However, for the set of bilinear maps for which CoveringSetsMethod allows one to compute all the optimal formulae, we observe a clear speed-up compared to BDEZStab. In order to compute bilinear maps of larger degrees using this method,

we need to be able to compute and store all the elements of

$$\mathscr{S}_{10}/\mathrm{GL}(K^{10}) \times \mathrm{GL}(K^{10})$$

for $\mathsf{ShortProduct}_6$ (and even more for other bilinear maps), which has not been done yet and requires a specific effort for an optimized implementation of the algorithm described in Section 5.3. Moreover, being able to decompose a matrix product of larger dimensions requires to improve on the theoretical aspect of our strategy, since the size of the required set

$$\mathscr{S}_{15}/\mathrm{GL}(K^{9}) \times \mathrm{GL}(K^{9})$$

is expected to be too large, based on the apparent exponential growth of the progression of the sets described in Table 2.

Henceforth, we describe how we computed optimal formulae for bilinear maps given in Table 3 via our approach using the covering sets. We provide some technical details, specific to each bilinear map, necessary for an implementation.

7.2. Matrix product $(3, 2, 3)$

We give in this section the timings obtained with our approach for solving the matrix product $(3, 2, 3)$. We use the same notations as in Section 6. We remind that we denote by $\Pi_{3,2,3}$ the bilinear map

$$\begin{array}{rccc} \Pi_{3,2,3}: & \mathcal{M}_{3,2}(\mathbb{F}_2) \times \mathcal{M}_{2,3}(\mathbb{F}_2) & \longrightarrow & \mathcal{M}_{3,3}(\mathbb{F}_2) \\ & (A, B) & \longmapsto & A \cdot B \end{array}.$$

We denote by $\pi_{i,j}$ the bilinear forms such that $\pi_{i,j}(A, B)$ is the coefficient (i, j) of $\Pi_{3,2,3}(A, B)$. The subspace $T_{3,2,3}$ is defined by

$$T_{3,2,3} = \mathrm{Span}(\{\pi_{i,j}\}_{i,j})$$

As described in Section 5.1, we need to precompute the quotients

$$\mathscr{S}_{6+k}/\mathrm{GL}(K^{6+k}) \times \mathrm{GL}(K^{6+k})$$

for $k \in \{1, 2, 3\}$, and we prove that we can restrict ourselves to subspaces containing at least one element of rank 6 (in particular, the whole quotient for $k = 3$ is not required). The techniques for computing theses subsets are described in Section 5.3.

The intermediate sets, corresponding to the quotient $\mathcal{Q}$ computed with $\mathsf{IntermediateSetViaQuotientComputation}$ in Section 5, are computed in $1.6 \cdot 10^5$ seconds. They are defined as the following sets: $\tilde{\mathcal{E}}_0 = \tilde{\mathcal{C}}_7(\{\pi_{0,0} + \pi_{1,1} + \pi_{2,2}\})$, $\tilde{\mathcal{E}}_1 = \tilde{\mathcal{C}}_8(\{\pi_{0,0} + \pi_{1,1}, \pi_{0,1} + \pi_{2,2}\})$, $\tilde{\mathcal{E}}_2 = \tilde{\mathcal{C}}_8(\{\pi_{0,0} + \pi_{1,1}, \pi_{1,1} + \pi_{2,2}\})$, $\tilde{\mathcal{E}}_3 = \tilde{\mathcal{C}}_8(\{\pi_{0,0} + \pi_{1,1}, \pi_{2,2}\})$, $\tilde{\mathcal{E}}_4 = \tilde{\mathcal{C}}_9(\{\pi_{0,0}, \pi_{1,1}, \pi_{2,2}\})$. For the set $\tilde{\mathcal{E}}_4$, we remind that we compute actually a subset $\tilde{\mathcal{E}}'_4$ given by the special trick described in Section 6.3.

We give in Table 4 the time required to compute the second step of Section 5.1, which is the computation of $\mathcal{Q} \circ \mathcal{L}$.

set	cardinality	nb. tests	time (s)	nb. of solutions found
$\tilde{\mathcal{E}}_0$	$8.8 \cdot 10$	$1.2 \cdot 10^8$	$2.0 \cdot 10^5$	5
$\tilde{\mathcal{E}}_1$	$7.5 \cdot 10^5$	$2.2 \cdot 10^7$	$3.3 \cdot 10^5$	13
$\tilde{\mathcal{E}}_2$	$1.0 \cdot 10^4$	$2.8 \cdot 10^5$	$4.1 \cdot 10^2$	1
$\tilde{\mathcal{E}}_3$	$2.7 \cdot 10^5$	$5.9 \cdot 10^8$	$9.1 \cdot 10^5$	46
$\tilde{\mathcal{E}}'_4$	$2.5 \cdot 10^7$	$9.1 \cdot 10^8$	$1.3 \cdot 10^6$	2

Table 4: Computation of elements of $\mathscr{S}_{15,T_{3,2,3}}$.

In conclusion, we are able to decompose $\Pi_{3,2,3}$ over $\mathbb{F}_2$ and to give all the possible optimal decompositions. We have a speed-up of 10^4 compared to our implementation of Algorithm BDEZStab. Although the rank of this bilinear map was already known thanks to Hopcroft and Kerr [13], determining all the possible optimal decompositions was not a well studied problem to our knowledge.

We prove with our algorithm that there is only one class of equivalence of vector spaces $W \in \mathscr{S}_{6,6,15}$ containing $T_{3,2,3}$, for the group action induced by $\mathrm{Stab}(T_{3,2,3})$. It is interesting to note that this is also the case for $T_{2,2,2}$. We do not have this kind of result for the short product for example.

7.3. Matrix product $(2,3,2)$

We denote by $\Pi_{2,3,2}$ the bilinear map

$$\begin{array}{rccc} \Pi_{2,3,2}: & \mathcal{M}_{2,3}(\mathbb{F}_2) \times \mathcal{M}_{3,2}(\mathbb{F}_2) & \longrightarrow & \mathcal{M}_{2,2}(\mathbb{F}_2) \\ & (A,B) & \longmapsto & A \cdot B \end{array}$$

and $\pi_{i,j}$ its coefficients.

We compute the following sets, corresponding to the quotient $\mathcal{Q}$ computed with IntermediateSetViaQuotientComputation in Section 5, within $1.5 \cdot 10^6$ seconds:

- $\tilde{\mathcal{E}}_0 = \tilde{\mathcal{C}}_8(\{\pi_{0,0} + \pi_{1,1}, \pi_{0,0} + \pi_{0,1} + \pi_{1,0}\})$,
- $\tilde{\mathcal{E}}_1 = \tilde{\mathcal{C}}_8(\{\pi_{0,0} + \pi_{1,1}, \pi_{0,0}\})$.

We used, in particular, the fact that for any basis $\mathcal{B}$ of $T_{2,3,2}$, there exist two elements ϕ and ψ of $\mathcal{B}$ such that there exists an element in $\mathrm{Span}(\phi, \psi)$ whose decomposition over $(\pi_{0,0}, \pi_{1,1}, \pi_{0,1}, \pi_{1,0})$ has the following shape:

$$(1, 0, \lambda_3, \lambda_4) \text{ or } (0, 1, \lambda_3, \lambda_4).$$

The timings for the second step of the method proposed in Section 5 are described in Table 5.

set	cardinality	nb. tests	time (s)	nb. of solutions found
$\tilde{\mathcal{E}}_0$	139	$5.0 \cdot 10^4$	$6.2 \cdot 10^4$	44
$\tilde{\mathcal{E}}_1$	$3.8 \cdot 10^8$	$6.3 \cdot 10^{10}$	$4.1 \cdot 10^6$	5,614

Table 5: Computation of $\mathscr{S}_{11,T_{2,3,2}}$.

We obtained a speed-up of 10^9 compared to our implementation of BDEZStab, and we found 1096452 elements of $\mathscr{S}_{11,T_{2,3,2}}$, divided in 196 equivalence classes of solutions with respect to the action of $\mathrm{Stab}(T_{2,3,2})$. The computations described in Table 5 used an improved basic test VecSpHasGoodBasis specialized for $T_{2,3,2}$. This test uses the fact that, given a subspace W of $\tilde{\mathcal{E}}_0$ or $\tilde{\mathcal{E}}_1$, we have two elements t_0 and t_1 in $T_{2,3,2}$ in the 1-neighbourhood of W. We enumerate the elements of W at distance 1 from t_0 or t_1, instead of enumerating the whole set of rank-one bilinear forms.

7.4. Short product

We present in this section the timings obtained with our method for the decomposition of the short product. We managed to obtain all the elements of $\mathscr{S}_{r,T_\ell}$, where T_ℓ is the vector space generated by the bilinear forms associated to $\mathsf{ShortProduct}_\ell$ for $\ell = 4$ and $\ell = 5$ and $r = \mathrm{rk}(T_\ell)$.

bilinear map	nb. of tests	time (s)	nb. of solutions	equivalence classes
$\mathsf{ShortProduct}_4$	$2.8 \cdot 10^2$	3.0	$1,440$	220
$\mathsf{ShortProduct}_5$	$6.3 \cdot 10^6$	$2.4 \cdot 10^3$	$146,944$	$11,424$

Table 6: Computation of $\mathscr{S}_{r,T_\ell}$.

The last column of Table 6 describes the number of equivalence classes of vector spaces in $\mathscr{S}_{r,T_\ell}$, with respect to the group $\mathrm{Stab}(T_\ell)$.

7.5. Circulant product

We present in this section how to find, with our approach, optimal decompositions of the polynomial product modulo (X^5-1). We denote by T the target space spanned by the coefficients π_i of the bilinear map

$$\Pi : (A,B) \mapsto A \cdot B \bmod (X^5-1) = \begin{pmatrix} \pi_0 \\ \pi_1 \\ \pi_2 \\ \pi_3 \\ \pi_4 \end{pmatrix} = \begin{pmatrix} a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_0 \\ a_4b_2 + a_3b_3 + a_2b_4 + a_1b_0 + a_0b_1 \\ a_4b_3 + a_3b_4 + a_2b_0 + a_1b_1 + a_0b_2 \\ a_4b_4 + a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 \\ a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4 \end{pmatrix}.$$

The structure of T allows us to gain an interesting speed-up. Indeed, T has the following structure: there exists, up to a constant mulitplicative factor, a unique element of rank one $\phi = \pi_0 + \pi_1 + \pi_2 + \pi_3 + \pi_4$ and a hyperplane H such that H contains all the elements of rank 4 and all the elements of rank 5 are included in $\mathrm{Span}(\phi) \oplus H$. Moreover, the action of $\mathrm{Stab}(T)$ on $H - \{0\}$ is transitive (observed empirically), which means that all the elements of rank 4 are in the same orbit. Consequently, it is also transitive on $\mathrm{Span}(\phi) \oplus H$ and all the elements of rank 5 are in the same orbit.

Let $\mathcal{B} = \{\Phi_0, \ldots, \Phi_4\}$ be a basis of T. We distinguish then 2 cases: there exists i such that Φ_i has rank 5 or there is no such i, which implies that $\phi \in \mathcal{B}$. We deduce from these observations the following covering sets:

- $\tilde{\mathcal{E}}_0 = \tilde{\mathcal{C}}_6(\{\pi_4\})$ and
- $\mathcal{E}_1 = \mathscr{S}_{9,H}/\mathrm{Stab}(H)$ (any element $V \in \mathcal{E}_1$ satisfies $T \subset V + \mathrm{Span}(\phi) \in \mathscr{S}_{10}$).

We obtain the set $\mathcal{E}_1$ via the computation of a covering of $\mathcal{E}_1$ obtained with

$$\tilde{\mathcal{E}}_1 = \tilde{\mathcal{C}}_6(\{\pi_0 + \pi_1 + \pi_2 + \pi_3\}).$$

set	cardinality	nb. tests	time (s)	nb. of solutions found
$\tilde{\mathcal{E}}_0$	$5.2 \cdot 10$	$8.7 \cdot 10^7$	$3.1 \cdot 10^3$	0
$\tilde{\mathcal{E}}_1$	$2.0 \cdot 10^3$	$6.7 \cdot 10^5$	$2.4 \cdot 10^2$	264

Table 7: Computation of $\mathscr{S}_{10,T}$.

We have in Table 7 the timings for the second step of the procedure described in Section 5. The set $\mathscr{S}_{10,T}$ contains 2025 elements divided in 9 equivalence classes of solutions. Interestingly, the set $\tilde{\mathcal{E}}_1$ does not correspond to any element of $\mathscr{S}_{10,T}$. It means that, for a basis $\mathcal{B}$ of bilinear forms of rank one containing ϕ and generating a subspace of $\mathscr{S}_{10,T}$, the coordinate of the elements of rank 4 on ϕ is zero.

8. Conclusions

One of the most challenging problems in the field of bilinear complexity is the decomposition of the bilinear map given by the product of 3×3 matrices. Currently, our approach cannot be used to tackle this problem. However, we believe that it could be approached by further research in the direction of the Hamming weight idea developed in Section 6.3. An important obstacle is the fact that, assuming that the rank is 21, it requires to compute $\mathscr{S}_{15}/\mathrm{GL}(K^9) \times \mathrm{GL}(K^9)$, which is very large.

Another aspect which is not well understood currently for our approach is to establish a realistic complexity analysis. It requires a theoretical understanding of how the cardinality of the quotients $\mathscr{S}_d/\mathrm{GL}(K^d) \times \mathrm{GL}(K^d)$ behave asymptotically and a classification of their representatives.

Further research could focus on symmetric decompositions of bilinear maps, which have applications for the multiplication of polynomials over "small" finite fields (such as $\mathbb{F}_2$). Especially, we can improve on the upper bounds on the rank of the product of two polynomials of fixed degrees by improving on the bilinear complexity of the multiplication algorithms used in the Chudnovsky-Chudnovsky approach [8, 22, 21].

Finally, the approach proposed in this work allows one to compute exhaustively the optimal formulae for new bilinear maps, which was not feasible with [1]. Moreover, it uses combinatorial objects which are not well documented in the litterature, which may rekindle curiosity for them.

Acknowledgements

The author is grateful to Jérémie Detrey and Emmanuel Thomé for their helpful comments and suggestions.

[1] R. Barbulescu, J. Detrey, N. Estibals, and P. Zimmermann. Finding optimal formulae for bilinear maps. *Arithmetic of finite fields: 4th International Workshop, WAIFI 2012, Bochum, Germany, July 16-19, 2012. Proceedings*, pages 168–186, 2012. doi:10.1007/978-3-642-31662-3_12.

[2] R. Barbulescu, J. Detrey, N. Estibals, and P. Zimmermann. Finding optimal formulae for bilinear maps. AriC Seminar, Mar. 2012. URL: https://hal.inria.fr/hal-01413162.

[3] A. Bernardi, J. Brachat, P. Comon, and B. Mourrain. General tensor decomposition, moment matrices and applications. *Journal of Symbolic Computation*, 52:51–71, 2013. International Symposium on Symbolic and Algebraic Computation. doi:10.1016/j.jsc.2012.05.012.

[4] M. Bläser. On the complexity of the multiplication of matrices of small formats. *Journal of Complexity*, 19(1):43–60, 2003. doi:10.1016/S0885-064X(02)00007-9.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). doi:10.1006/jsco.1996.0125.

[6] R. W. Brockett and D. Dobkin. On the optimal evaluation of a set of bilinear forms. *Linear Algebra and its Applications*, 19(3):207–235, 1978. doi:10.1016/0024-3795(78)90012-5.

[7] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory*. Springer, 1st edition, 2010.

[8] D. Chudnovsky and G. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4(4):285–316, 1988. doi:10.1016/0885-064X(88)90012-X.

[9] D. Coppersmith and S. Winograd. Computational algebraic complexity editorial matrix multiplication via arithmetic progressions. *Journal of Symbolic Computation*, 9(3):251–280, 1990. doi:10.1016/S0747-7171(08)80013-2.

[10] H. F. de Groote. *Lectures on the Complexity of Bilinear Problems*. Springer-Verlag, 1987.

[11] D. Harvey, J. van der Hoeven, and G. Lecerf. Even faster integer multiplication. Technical report, ArXiv, 2014. arXiv:1407.3360.

[12] D. F. Holt, B. Eick, and E. A. O'Brien. *Handbook of computational group theory*. Discrete mathematics and its applications. Chapman & Hall/CRC, Boca Raton, 2005. URL: http://opac.inria.fr/record=b1102239.

[13] J. E. Hopcroft and L. R. Kerr. On minimizing the number of multiplications necessary for matrix multiplication. *SIAM Journal on Applied Mathematics*, 20(1):30–36, 1971. doi:10.1137/0120004.

[14] J. Håstad. Tensor rank is NP-complete. *Journal of Algorithms*, 11(4):644–654, 1990. doi:10.1016/0196-6774(90)90014-6.

[15] J. JáJá. Optimal evaluation of pairs of bilinear forms. *SIAM Journal on Computing*, 8(3):443–462, 1979. doi:10.1137/0208037.

[16] A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on automata. *Soviet Physics-Doklady*, 7:595–596, 1963. (English translation).

[17] J. D. Laderman. A noncommutative algorithm for multiplying 3×3 matrices using 23 multiplications. *Bull. Amer. Math. Soc.*, 82(1):126–128, 1976.

[18] F. Le Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, pages 296–303. ACM, 2014. doi:10.1145/2608628.2608664.

[19] P. Montgomery. Five, six, and seven-term Karatsuba-like formulae. *IEEE Transactions on Computers*, 54(3):362–369, 2005. doi:10.1109/TC.2005.49.

[20] I. Oseledets. Optimal Karatsuba-like formulae for certain bilinear forms in GF(2). *Linear Algebra and its Applications*, 429(8–9):2052–2066, 2008. doi:10.1016/j.laa.2008.06.004.

[21] M. Rambaud. Finding optimal Chudnovsky-Chudnovsky multiplication algorithms. *Arithmetic of Finite Fields: 5th International Workshop, WAIFI 2014, Gebze, Turkey, September 27-28, 2014. Revised Selected Papers*, pages 45–60, 2015. doi:10.1007/978-3-319-16277-5_3.

[22] H. Randriambololona. Bilinear complexity of algebras and the Chudnovsky–Chudnovsky interpolation method. *Journal of Complexity*, 28(4):489–517, 2012. doi:10.1016/j.jco.2012.02.005.

[23] A. Schönhage and V. Strassen. Schnelle Multiplikation großer Zahlen. *Computing*, 7(3-4):281–292, 1971. doi:10.1007/BF02242355.

[24] A. V. Smirnov. The bilinear complexity and practical algorithms for matrix multiplication. *Computational Mathematics and Mathematical Physics*, 53(12):1781–1795, 2013. doi:10.1134/S0965542513120129.

[25] V. Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356, 1969. doi:10.1007/BF02165411.

[26] A. L. Toom. The complexity of a scheme of functional elements realizing the multiplication of integers. *Soviet Mathematics Doklady*, 3:714–716, 1963. (English translation).

Appendix A. Computation of stabilizers

Appendix A.1. Stabilizer of the short product

We describe in this section the structure of the stabilizer of the vector space T_ℓ associated to the short product. In particular, we show that its cardinality is $(\#K)^{3\ell-4} \cdot (\#K-1)^3$ for $\ell \geq 2$.

For simplicity, the matrices used to represent the coefficients of the short product are not given by the canonical basis. We choose a basis such that T_ℓ is represented by the ring $K[M]$ of polynomials of degree small or equal to $\ell-1$ evaluated in the matrix M such that

$$\forall i,j \in \{0,\dots,\ell-2\},\ M[i,j] = M[i+1,j+1],$$

with $M[0,1]=1$ and $M[0,j]=0$ if $j \neq 1$. For example, for $\ell=4$,

$$a_0M^0 + a_1M^1 + a_2M^2 + a_3M^3 = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ 0 & a_0 & a_1 & a_2 \\ 0 & 0 & a_0 & a_1 \\ 0 & 0 & 0 & a_0 \end{pmatrix}.$$

We observe that the bilinear forms of rank exactly ℓ within T_ℓ are described by the matrices that can be expressed as $P(M)$ where P is a polynomial of degree smaller or equal to $\ell-1$ over K such that $P(0) \neq 0$.

Theorem 28. *There exist groups G_1, G_2 and G_3 such that for any element $L \in \mathrm{Stab}(T_\ell)$*

$$\exists!(N_1,N_2,N_3) \in G_1 \times G_2 \times G_3,\ L = N_3 \cdot N_2 \cdot N_1$$

and

- $G_1 \simeq \mathrm{Stab}(T_\ell)/\mathrm{Stab}(M^0) \cap \mathrm{Stab}(T_\ell)$,
- $G_2 \simeq \mathrm{Stab}(M^0) \cap \mathrm{Stab}(T_\ell)/\mathrm{Stab}(M^0) \cap \mathrm{Stab}(M) \cap \mathrm{Stab}(T_\ell)$,
- $G_3 = \mathrm{Stab}(M^0) \cap \mathrm{Stab}(M)$.

Moreover, $\#G_1 = \#K^{\ell-1}(\#K-1)$, $\#G_2 = \#K^{\ell-2}(\#K-1)$ and $\#G_3 = \#K^{\ell-1}(\#K-1)$.

Lemma 29. *For any element $N \in T_\ell$ of rank ℓ, there exists $R \in K[M]$ a polynomial of degree $\ell-1$ such that $R(0) \neq 0$ and $R(M) = N$. Then,*

$$\exists!N_1 \in \mathrm{Stab}(T_\ell)/\mathrm{Stab}(M^0) \cap \mathrm{Stab}(T_\ell),\ M^0 \cdot N_1 = R(M).$$

Thus, $\#\mathrm{Stab}(T_\ell)/\mathrm{Stab}(M^0) \cap \mathrm{Stab}(T_\ell) = \#K^{\ell-1} \cdot (\#K-1)$.

Proof. The cardinality of the set $\mathrm{Stab}(T_\ell)/\mathrm{Stab}(M^0) \cap \mathrm{Stab}(T_\ell)$ is equal to the cardinality of the orbit of M^0 under the action of $\mathrm{Stab}(T_\ell)$.

Any element in the orbit of M^0 has rank ℓ and any element of rank ℓ in T_ℓ is associated to a polynomial $R \in K[M]$ evaluated in M of degree $\ell - 1$ such that $R(0) \neq 0$. It remains to prove that the orbit of M^0 corresponds exactly to the set of rank-ℓ elements. Given $R \in K[M]$ such that $R(0) \neq 0$, we denote by $N_1(R)$ the element $(M^0, R(M))$. This element is in $\mathrm{Stab}(T_\ell)$ because, for any S, we have $R(M)S(M) = (RS \bmod X^\ell)(M)$, which is a polynomial evaluated in M of degree smaller or equal to $\ell - 1$. We have:

$$M^0 \cdot N_1(R) = (M^0)^{\mathrm{T}} \cdot M^0 \cdot R(M) = R(M).$$

Other choices for $N_1(R)$ are naturally equivalent under the action of $\mathrm{Stab}(M^0)$. □

Lemma 30. *For any element $N \in T_\ell$ of rank $\ell - 1$, there exists $R \in K[M]$ a polynomial of degree $\ell - 1$ such that $R(0) = 0$, $R'(0) \neq 0$ and $R(M) = N$. Then,*

$$\exists! N_2 \in \mathrm{Stab}(M^0) \cap \mathrm{Stab}(T_\ell)/\mathrm{Stab}(M^0) \cap \mathrm{Stab}(M) \cap \mathrm{Stab}(T_\ell),\ M \cdot N_2 = R(M).$$

Thus, $\#\mathrm{Stab}(M^0) \cap \mathrm{Stab}(T_\ell)/\mathrm{Stab}(M^0) \cap \mathrm{Stab}(M) \cap \mathrm{Stab}(T_\ell) = \#K^{\ell-2} \cdot (\#K - 1)$.

Proof. The cardinality of the set $\mathrm{Stab}(M^0) \cap \mathrm{Stab}(T_\ell)/\big(\mathrm{Stab}(M^0) \cap \mathrm{Stab}(M) \cap \mathrm{Stab}(T_\ell)\big)$ is equal to the cardinality of the orbit of M under the action of $\mathrm{Stab}(M^0) \cap \mathrm{Stab}(T_\ell)$.

An element of the orbit of M is an element of rank $\ell - 1$ and an element of rank $\ell - 1$ in T_ℓ is associated to a polynomial $R \in K[M]$ evaluated in M of degree $\ell - 1$ such that $R(0) = 0$ and $R'(0) \neq 0$. It remains to prove that M can mapped to any element of rank $\ell - 1$ via the action of $\mathrm{Stab}(M^0) \cap \mathrm{Stab}(T_\ell)$.

Let e_ℓ be the vector such that $R(M) \cdot e_\ell$ corresponds to the last colum of $R(M)$. We have $R(M)^{\ell-1} e_\ell \neq 0$. Thus, let $P(M)$ be the matrix whose columns are given by the tuple $(R(M)^{\ell-1} \cdot e_\ell, R(M)^{\ell-2} \cdot e_\ell, \ldots, R(M) \cdot e_\ell, e_\ell)$, we have $P(M)^{-1} R(M) P(M) = M$. We take $N_2(R) = (P(M)^{\mathrm{T}}, P(M)^{-1})$:

$$M \cdot N_2(R) = R(M) \text{ and } N_2(R) \in \mathrm{Stab}(M^0) \cap \mathrm{Stab}(T_\ell).$$

□

Lemma 31. *We have $\mathrm{Stab}(M^0) \cap \mathrm{Stab}(M) \subset \mathrm{Stab}(T_\ell)$ and for any $N_3 \in \mathrm{Stab}(M^0) \cap \mathrm{Stab}(M)$ there exists $R \in K[M]$ a polynomial of degree $\ell - 1$ such that $R(0) \neq 0$ and*

$$N_3 = ((R(M)^{-1})^{\mathrm{T}}, R(M)).$$

Thus, $\#\,\mathrm{Stab}(M^0) \cap \mathrm{Stab}(M) = \#K^{\ell-1} \cdot (\#K - 1)$.

Proof. Let $N_3 \in \mathrm{Stab}(M^0) \cap \mathrm{Stab}(M) \cap \mathrm{Stab}(T_\ell)$. There exists $P \in \mathrm{GL}_\ell$ such that $N_3 = ((P^{-1})^{\mathrm{T}}, P)$ and $P^{-1} M P = M$. We have $PM = MP$.

Multiplying a matrix by M on the left shifts the rows upward and multiplying M on the right shifts the columns on the right. Therefore, denoting by p_{ij} the coefficients of P, with $p_{00} \neq 0$ and $p_{i0} = 0$ for $i \geq 1$, we have

$$\forall (i,j) \in \{1, \ldots, \ell - 1\} \times \{0, \ldots, \ell - 1\}, p_{i,j} = p_{i+1,j+1}.$$

More particularly, P can be expressed as a polynomial R evaluated in M such that $R(0) \neq 0$:

$$N_3 = ((R(M)^{-1})^{\mathrm{T}}, R(M)) \text{ and } N_3 \in \mathrm{Stab}(T_\ell).$$

□

Proof of Theorem 28. Let $L \in \mathrm{Stab}(T_\ell)$. We denote by N the element $M^0 \cdot L$. According to Lemma 29, there exists a unique $N_1 \in G_1$ such that $M^0 \cdot N_1 = N$ and $L \cdot N_1^{-1} \in \mathrm{Stab}(M^0) \cap \mathrm{Stab}(T_\ell)$. According to Lemma 30, there exists a unique $N_2 \in G_2$ such that $M \cdot N_2 = M \cdot L \cdot N_1^{-1}$ and

$$N \cdot N_1^{-1} \cdot N_2^{-1} \in \mathrm{Stab}(M^0) \cap \mathrm{Stab}(M) \cap \mathrm{Stab}(T_\ell).$$

Finally, according to Lemma 31, there exists a unique $N_3 \in G_3$ such that

$$L \cdot N_1^{-1} \cdot N_2^{-1} = N_3,$$

which concludes. □

Appendix A.2. Stabilizer of the matrix product

We denote by $T_{p,q,r}$ the vector space given by the product of matrices $p \times q$ by $q \times r$, which is isomorphic to $\mathcal{M}_{p,r} \otimes I_q$ (we do not use the canonical basis for this representation). For the group action $M \cdot (X, Y) \mapsto X^{\mathrm{T}} M Y$, we want to prove that the subgroup stabilizing the vector space $T_{p,q,r}$ is isomorphic to $\mathrm{Stab}(\mathcal{M}_{p,r}) \otimes \mathrm{Stab}(I_q)$.

Let (X, Y) be a pair of invertible matrices such that $X^{\mathrm{T}} T_{p,q,r} Y = T_{p,q,r}$. For any $i \in \{0, \ldots, p-1\}$ and $j \in \{0, \ldots, q-1\}$, we denote by $M_{i,j}$ the matrix $X^{\mathrm{T}} \cdot (e_{i,j}) \cdot Y$, where $e_{i,j}$ is the canonical basis of $\mathcal{M}_{p,r}$. Denoting by $X_{i,h}$ the $q \times q$ blocks of X and $Y_{\ell,j}$ the $q \times q$ blocks of Y, we have $M_{i,j} = (X_{i,h} Y_{j,\ell})_{h,\ell}$ for any i and j. Consequently, since $X^{\mathrm{T}} \cdot (e_{i,j}) \cdot Y \in T_{p,q,r}$, we have

$$\forall i, j, h, \ell, \;\; X_{i,h} Y_{j,\ell} \in \mathrm{Span}(I_q). \tag{A.1}$$

Let (i, h) such that $X_{i,h}$ is not null and j any integer in $\{0, \ldots, q-1\}$. We have the inclusion

$$X_{i,h} \cdot \mathrm{Span}(\{Y_{j,0}, \ldots, Y_{j,q-1}\}) \subset \mathrm{Span}(I_q)$$

and, since Y is invertible, we even have the equality. Thus, for any (i, h) such that $X_{i,h}$ is not null, we have shown that $X_{i,h}$ is invertible. We have the same property for the blocks of Y.

Combining the fact that the blocks of X and Y that are not null are invertible and Equation (A.1), we can conclude that the stabilizer of $T_{p,q,r}$ is generated by matrices (X, Y) such that there exists $g \in \mathrm{GL}_q$ satisfying

$$X^{\mathrm{T}} \in \mathrm{GL}_p \otimes g \text{ and } Y \in \mathrm{GL}_r \otimes g^{-1}.$$

Appendix B. Using Hamming weight for the matrix product

We use the notations of Section 6.3: we consider W in the set $\tilde{\mathcal{C}}_9(\{\pi_{0,0}, \pi_{1,1}, \pi_{2,2}\})$ such that $T_{3,2,3} + W \in \mathscr{S}_{15}$ and we denote by $\mathcal{B}$ a basis of rank-one bilinear forms of W.

We saw in Section 6.3 why we can assume that

$$\mathbb{H}_{\mathcal{B}}(\pi_{0,0} + \pi_{1,1} + \pi_{2,2}) = \mathbb{H}_{\mathcal{B}}(\pi_{0,0}) + \mathbb{H}_{\mathcal{B}}(\pi_{1,1}) + \mathbb{H}_{\mathcal{B}}(\pi_{2,2}).$$

It remains to prove that we can make the following assumption: $\mathbb{H}_{\mathcal{B}}(\pi_{0,0} + \pi_{1,1} + \pi_{2,2}) > 6$.

First, we assume in our context that the elements of $\mathscr{S}_{15,T_{3,2,3}}$ obtained via the sets of W' such that

$$\exists \sigma \in \mathrm{Stab}(T_{3,2,3}), \; W' \circ \sigma \in \begin{cases} \mathcal{C}_7(\mathrm{Span}(\pi_{0,0} + \pi_{1,1} + \pi_{2,2})) \\ \text{or} \\ \mathcal{C}_8(\mathrm{Span}(\pi_{0,0} + \pi_{1,1}, \pi_{0,1} + \pi_{2,2})) \\ \text{or} \\ \mathcal{C}_8(\mathrm{Span}(\pi_{0,0} + \pi_{1,1}, \pi_{2,2})) \end{cases}$$

have been explored. Thus, it remains to explore the elements of $\mathcal{C}_9(\mathrm{Span}(\pi_{0,0}, \pi_{1,1}, \pi_{2,2}))$ allowing one to get new elements of $\mathscr{S}_{15,T_{3,2,3}}$. Consequently, getting back to our notations, we systematically consider that a vector space $W' \subset T_{3,2,3} + W$ in $\mathscr{S}_9$, with a basis $\mathcal{B}'$ of rank-one bilinear forms, such that $T_{3,2,3} \oplus W' \in \mathscr{S}_{15}$, satsifies

$$W' \circ \sigma \in \mathcal{C}_9(\mathrm{Span}(\pi_{0,0}, \pi_{1,1}, \pi_{2,2})).$$

We assume moreover that we have

$$\mathbb{H}_{\mathcal{B}' \circ \sigma}(\pi_{0,0} + \pi_{1,1} + \pi_{2,2}) = \mathbb{H}_{\mathcal{B}' \circ \sigma}(\pi_{0,0}) + \mathbb{H}_{\mathcal{B}' \circ \sigma}(\pi_{1,1}) + \mathbb{H}_{\mathcal{B}' \circ \sigma}(\pi_{2,2})$$

by Theorem 27.

Theorem 32. *There exists $W' \subset T_{3,2,3} + W$ in $\mathscr{S}_9$ having a basis $\mathcal{B}'$ of rank-one bilinear forms such that*

$$\exists \sigma \in \mathrm{Stab}(T_{3,2,3}),\ \mathrm{Span}(\pi_{0,0}, \pi_{1,1}, \pi_{2,2}) \circ \sigma \subset W' \text{ and } \mathbb{H}_{\mathcal{B}'}((\pi_{0,0} + \pi_{1,1} + \pi_{2,2}) \circ \sigma) > 6.$$

Proof. We deduce this theorem from Lemmata 33, 34 and 35. □

The Hamming weight over some basis is related to the rank by Lemma 33.

Lemma 33. *Let $W \in \mathscr{S}_d$ and $\mathcal{B}$ a basis of W composed of rank-one bilinear forms. For any subset $\mathcal{S}$ of W, we have*

$$\mathrm{rk}(\mathrm{Span}(\mathcal{S})) \leq \mathbb{H}_{\mathcal{B}}(\mathcal{S}).$$

Proof. Clear from the definition of the rank of a set $\mathcal{S}$ given in Definition 5. □

Lemma 34. *For any pair (Φ, Φ') of independent elements of rank 2 of $T_{3,2,3}$, we have*

$$\mathrm{rk}(\mathrm{Span}(\Phi, \Phi')) = 4.$$

Proof. If $\Phi + \Phi'$ has rank 4, the conclusion follows. Otherwise, $\mathrm{Span}(\Phi, \Phi')$ is isomorphic to $T_{2,2,1}$, whose rank is equal to 4: $T_{2,2,1}$ and $T_{2,1,2}$ have the same rank according to [10] and $T_{2,1,2}$ is a vector space of dimension one generated by a bilinear form of rank 4. □

Lemma 35. *Let $W' \subset W$ of dimension 6 such that $T_{3,2,3} \oplus W' \in \mathscr{S}_{15}$ and W' is generated by a subset of the basis $\mathcal{B}$ of W. There exists $\Phi \in T_{3,2,3}$ such that*

$$W' \oplus \Phi \in \mathcal{C}_7(\mathrm{Span}(\Phi)).$$

In particular, there exists Φ such that, taking $\mathcal{B}'$ a basis of rank-one elements of $W' \oplus \Phi$, we have

$$\mathbb{H}_{\mathcal{B}'}(\Phi) > 2.$$

Proof. According to Theorem 15, there exists a basis $\mathcal{B}'' = \{\psi_0, \ldots, \psi_{15}\}$ of $T_{3,2,3} \oplus W'$ of rank-one elements and containing a basis of W' of rank-one elements. Moreover, there exists a basis of $\{\Phi_0, \ldots, \Phi_8\}$ of $T_{3,2,3}$ such that $\Phi_i - \psi_i \in W'$ for any i. In our context, we are concerned by the case $\mathrm{rk}(\Phi_i) = 2$ for any t.

There is necessarily a couple $(\Phi_i, \Phi_{i'})$ such that

$$\mathbb{H}_{\mathcal{B}''}(\Phi_i + \Phi_{i'}) < \mathbb{H}_{\mathcal{B}''}(\Phi_i) + \mathbb{H}_{\mathcal{B}''}(\Phi_{i'}).$$

Otherwise, we would have $\#\mathcal{B}'' = 2 \cdot 9 = 18 \neq 15 = \mathrm{rk}(T_{3,2,3})$.

If $\mathbb{H}_{\mathcal{B}''}(\Phi_i) = 2$ and $\mathbb{H}_{\mathcal{B}''}(\Phi_{i'}) = 2$, then

$$\mathbb{H}_{\mathcal{B}''}(\{\Phi_i, \Phi_{i'}\}) \leq 3,$$

although $\mathrm{rk}(\mathrm{Span}(\Phi_i, \Phi_{i'})) = 4$ by Lemma 34. This is contradictory according to Lemma 33: in other terms, $\mathbb{H}_{\mathcal{B}''}(\Phi_i) > 2$ or $\mathbb{H}_{\mathcal{B}''}(\Phi_{i'}) > 2$. □