Improved method for finding optimal formulae for bilinear maps in a finite field

Svyatoslav Covanov

Improved method for finding optimal formulae for bilinear maps in a finite field

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. We apply in particular our approach to 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

1. Introduction

Finding optimal formulae for computing bilinear maps is a problem of algebraic complexity theory [7, 6, 26, 15], initiated by the discoveries of Karatsuba and Ofman [16] and Strassen [26]. It consists in determining almost optimal algorithms for important problems of complexity theory, among which the well studied complexity of matrix multiplication [26, 21, 9, 18] and the complexity of polynomial multiplication [16, 27, 24, 11].

As far as polynomial multiplication is concerned, the first improvement over the schoolbook method came from Karatsuba and Ofman [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 $A \cdot B$ 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 $O(n^{\log_2 3})$.

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

In 1969, Strassen [26] 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 of $O(n^{\log_2 7})$ instead of $O(n^{\log_2 8}) = O(n^3)$. Smirnov describes in [25] practical algorithms for 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 [25]. 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 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. 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 allows one to generate 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, and on the notion of "stem" of a vector space associated to such a bilinear map. 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, 23, 22]. Specifically, 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 action of the automorphism group. We are not able to provide sharp complexity analysis: the bounds that we thought about are too large.

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 algebraic structure of specific bilinear maps. This section can be skipped on a first read, because it is only required in proofs of the following section. In Section 5, we describe the theoretical aspect of our main contribution, which relies on the construction of coverings, and illustrate it with the examples of the short product and the matrix product. We discuss specific algorithmic aspects in Section 6: this part is quite technical and can be skipped on a first read. 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*

$$\mathbf{\Phi} = \begin{pmatrix} \Phi_0 \\ \Phi_1 \\ \Phi_2 \end{pmatrix} : (\mathbf{a}, \mathbf{b}) \mapsto \begin{pmatrix} a_0 b_0 \\ a_0 b_1 + a_1 b_0 \\ a_1 b_1 \end{pmatrix}.$$

Denoting by ϕ_0, ϕ_1, ϕ_2 and ϕ_3 the bilinear forms $(\mathbf{a}, \mathbf{b}) \mapsto a_0 b_0$, $(\mathbf{a}, \mathbf{b}) \mapsto a_0 b_0$, $(\mathbf{a}, \mathbf{b}) \mapsto a_0 b_0$ and $(\mathbf{a}, \mathbf{b}) \mapsto a_0 b_0$, respectively, we have

$$\mathbf{\Phi} = \phi_0 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \phi_1 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \phi_2 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \phi_3 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},$$

which corresponds to the schoolbook algorithm.

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 $\phi_1 + \phi_2 = \psi - \phi_0 - \phi_3$, we can rewrite $\mathbf{\Phi}$ as

$$\mathbf{\Phi} = \phi_0 \cdot \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} + \psi \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \phi_2 \cdot \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}.$$

The bilinear forms ϕ_0, ψ and ϕ_2 each correspond to exactly one multiplication over K. This decomposition corresponds to the Karatsuba algorithm. 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 $\phi(\mathbf{a}, \mathbf{b}) = \alpha(\mathbf{a}) \cdot \beta(\mathbf{b})$. 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 $\mathbf{\Phi} = (\Phi_0, \ldots, \Phi_{\ell-1})$ 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*.*

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 represent the corresponding matrices, we use 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 $\mathcal{L}(K^m, K^n; K)$. Indeed, finding formulas for computing the Φ_t's is equivalent to finding a family of rank-one bilinear forms generating T. Thus, we need to extend the definition of the rank to subspaces of $\mathcal{L}(K^m, K^n; K)$.

Notation 4. *For T a subspace of $\mathcal{L}(K^m, K^n; K)$, we denote by $\mathscr{S}_{m,n,r}(T)$ the set of subspaces $V \subset \mathcal{L}(K^m, K^n; K)$ spanned by a free family of rank-one bilinear forms of size r such that $T \subset V$.*

When $T = \mathrm{Span}(\emptyset)$, $\mathscr{S}_{m,n,r}(T)$ is 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 and we denote it simply by $\mathscr{S}_{m,n,r}$.

When m and n are clear from the context, these sets are simply denoted by $\mathscr{S}_r(T)$ and $\mathscr{S}_r$.

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 said to be the set of optimal decompositions of T.*

We observe that $\mathrm{rk}(T) \geq \dim(T)$.

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.

- Let $T = \mathrm{Span}(\Phi_0, \ldots, \Phi_{\ell-1}) \subset \mathcal{L}(K^m, K^n; K)$ of dimension ℓ;
- start with the known lower bound $r = \ell$ on the bilinear rank;
- compute $\mathscr{S}_r(T)$;
- if $\mathscr{S}_r(T) = \emptyset$, increment r and return to the previous step;
- if $\mathscr{S}_r(T) \neq \emptyset$, r is the bilinear 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 $\mathbf{\Phi} = (\Phi_0, \ldots, \Phi_{\ell-1})$ over a finite field. As described above, this is essentially equivalent to computing $\mathscr{S}_r(T)$ for $T = \mathrm{Span}(\Phi_0, \ldots, \Phi_{\ell-1})$ of dimension ℓ.

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. □

We denote by $\mathcal{G}$ the set of rank-one bilinear forms up to a multiplicative factor, isomorphic to $\mathscr{S}_{m,n,1}$. In a finite field, $\mathcal{G}$ is a finite set of cardinality $(\#K^m - 1)(\#K^n - 1)/(\#K - 1)^2$. 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 HasRankOneBasis 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 (such as product of 2×3 by 3×2 matrices, for example).

Algorithm 1 HasRankOneBasis (naive method)

Input: V subspace of $\mathcal{L}(K^m, K^n; K)$
Output: Boolean indicating whether $V \in \mathscr{S}_{\dim(V)}$
1: $\mathcal{H} \leftarrow \mathcal{G} \cap V$ ▷ $\#\mathcal{G}$ membership tests (Gaussian elimination)
2: **if** $\dim(\mathrm{Span}(\mathcal{H})) = \dim(V)$ **then**
3: **return true**
4: **else**
5: **return false**
6: **end if**

Algorithm BDEZ can be described as 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 subspace T of dimension ℓ and an integer r (r is a lower bound 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, an integer r
Output: $\mathscr{S}_r(T)$
1: **function** ExpandSubspace($V, \mathcal{H}, d, r$)
2: **if** $d = r$ and $\dim V = r$ and HasRankOneBasis(V) **then**
3: **return** $\{V\}$
4: **else**
5: $\mathcal{S} \leftarrow \emptyset$
6: **for** $i \in \{0, \ldots, \#\mathcal{H} - 1\}$ **do** ▷ $\mathcal{H} = \{\phi_i |\ i \in [0, \#\mathcal{H} - 1]\}$
7: $\mathcal{H}' \leftarrow \{\phi_{i+1}, \ldots, \phi_{\#\mathcal{H}-1}\} \mod \phi_i$ ▷ Gauss reduction modulo ϕ_i
8: $\mathcal{S} \leftarrow \mathcal{S} \cup$ ExpandSubspace($V \oplus \mathrm{Span}(\phi_i), \mathcal{H}', d+1, r$)
9: **end for**
10: **return** $\mathcal{S}$
11: **end if**
12: **end function**
13: **return** ExpandSubspace($T, \mathcal{G} \bmod T, \ell, r$) ▷ Gauss reduction of $\mathcal{G}$ modulo a basis of T

Algorithm BDEZ takes into account, on Line 7, the equivalence relation "modulo V": two distinct elements ϕ and ϕ' of $\mathcal{H}$ may be such that $V + \mathrm{Span}(\phi) = V + \mathrm{Span}(\phi')$. Reducing each element of $\mathcal{H}$ against V (via Gauss reduction) allows us to consider a single representative for each such equivalence class modulo V. A similar reduction is performed on Line 13 to compute $\mathcal{G} \bmod T$.

The recursive calls of this algorithm can be represented by 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 $\mathcal{G} = \{\phi_0, \phi_1, \phi_2, \phi_3\}$ and ignoring the reductions computed on Line 7, we would obtain generically, for $r - \ell = 3$, the tree given in Figure 1.

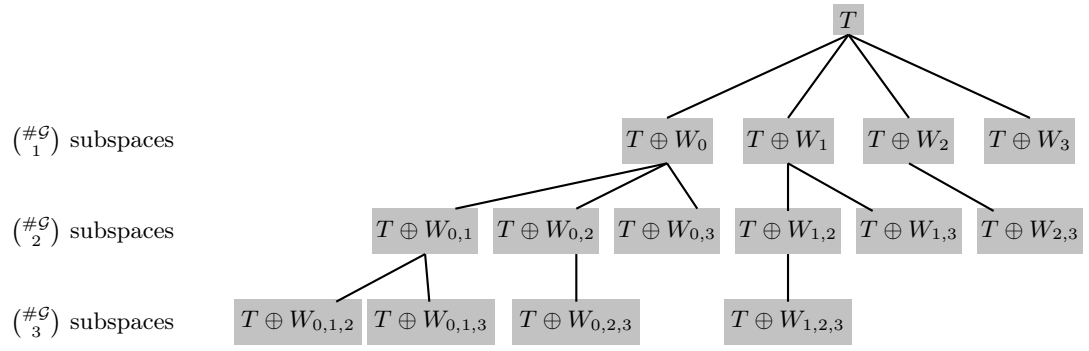

Figure 1: Tree of recursive calls in an exhaustive search with depth $r - \ell = 3$

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 rank-preserving automorphisms of $\mathcal{L}(K^m, K^n; K)$. Their action is defined in Section 3.1.

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 Propositon 7.

Proposition 7 (Automorphisms preserving the rank)**.** *An element $\sigma = (\mu, \nu) \in \mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ acts on $\mathcal{L}(K^m, K^n; K)$ via*

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

The action defined above is a group action preserving the rank of a subspace of bilinear forms. By linearity, we extend this action to subspaces of $\mathcal{L}(K^m, K^n; K)$.

Proof. For $\sigma = (\mu, \nu), \sigma' = (\mu', \nu') \in \mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ and $\Phi \in \mathcal{L}(K^m, K^n; K)$, we have

$$\forall \mathbf{a}, \mathbf{b},\ (\Phi \circ \sigma) \circ \sigma'(\mathbf{a}, \mathbf{b}) = (\Phi \circ \sigma)(\mu'(\mathbf{a}), \nu'(\mathbf{b})) = \Phi(\mu(\mu'(\mathbf{a})), \nu(\nu'(\mathbf{b}))) = \Phi \circ (\sigma \circ \sigma')(\mathbf{a}, \mathbf{b}).$$

Since all the elements of $\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ are invertible, we have automorphisms.

Henceforth, we prove that this group preserves the rank. First, let $\phi \in \mathcal{L}(K^m, K^n; K)$ of rank one. There exist $\alpha \in \mathcal{L}(K^m; K)$ and $\beta \in \mathcal{L}(K^n; K)$ such that $\phi : (\mathbf{a}, \mathbf{b}) \mapsto \alpha(\mathbf{a}) \cdot \beta(\mathbf{b})$. There exist $\mu \in \mathrm{GL}(K^m)$ and $\nu \in \mathrm{GL}(K^n)$ such that $\phi \circ \sigma : (\mathbf{a}, \mathbf{b}) \mapsto \alpha(\mu(\mathbf{a})) \cdot \beta(\nu(\mathbf{b}))$. Since $\alpha \circ \mu \in \mathcal{L}(K^m; K)$ and $\beta \circ \nu \in \mathcal{L}(K^n; K)$, $\phi \circ \sigma$ is a rank-one bilinear form.

Since the automorphisms preserve the rank of rank-one bilinear forms, by linearity and by definition of the rank of a bilinear form, it preserves the rank of any bilinear form. For any subspace $T \subset \mathcal{L}(K^m, K^n; K)$ and any $\sigma \in \mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$, we have $\mathrm{rk}(T \circ \sigma) = \mathrm{rk}(T)$. □

Remark 8. *Note that, when $m = n$, Proposition 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 $\Phi \circ \tau : (\mathbf{a}, \mathbf{b}) \mapsto \Phi(\mathbf{b}, \mathbf{a})$.*

Notation 9 (Group action on matrices)**.** *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 vice versa.*

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 the bilinear forms represented by the 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*

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

Since we will often refer to subgroups of $\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ stabilizing elements of $\mathcal{L}(K^m, K^n; K)$ in the following, we define the notion of setwise stabilizer.

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

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

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

In the rest of this work, we often refer to the "stabilizer" of a given set $\mathcal{T}$. Each time, we exclusively mean the setwise stabilizer of $\mathcal{T}$, which is, in general, different from the pointwise stabilizer of $\mathcal{T}$. Indeed, the pointwise stabilizer of $\mathcal{T}$ is defined as $\{\sigma \in \mathrm{GL}(K^m) \times \mathrm{GL}(K^n) \mid \forall \Phi \in \mathcal{T}, \; \Phi \circ \sigma = \Phi\}$.

The algorithmic improvement originally presented in [2] comes from the fact that, for any target space $T \subset \mathcal{L}(K^m, K^n; K)$ 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 $\mathscr{S}_r(\mathrm{Span}(T))/\mathrm{Stab}(T)$, 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;
- enumerate $\mathscr{S}_r(T)$ 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 group $\mathrm{Stab}(T)$ and an integer $r \geq \ell$.

Algorithm 3 BDEZStab

Input: $T \subset \mathcal{L}(K^m, K^n; K)$,$\mathrm{Stab}(T)$, an integer r
Output: A set of representatives of $\mathscr{S}_r(T)/\mathrm{Stab}(T)$
1: **function** ExpandSubspace($V, \mathcal{H}, U, d, r$) ▷
$V \subset \mathcal{L}(K^m, K^n; K), \mathcal{H} \subset \mathcal{G}, U \subset \mathrm{Stab}(T), r \in \mathbb{N}$
2: **if** $d = r$ and $\dim V = r$ and HasRankOneBasis(V) **then**
3: **return** $\{V\}$
4: **else**
5: $\mathcal{S} \leftarrow \emptyset$
6: $\mathcal{O} \leftarrow \mathcal{H}/U$ ▷ ϕ and ϕ' lie in the same orbit if $V \oplus \mathrm{Span}(\phi) = (V \oplus \mathrm{Span}(\phi')) \circ \sigma$
7: **for** $i \in \{0, \ldots, \#\mathcal{O} - 1\}$ **do** ▷ $\mathcal{O} = \{O_i \mid i \in \{0, \ldots, \#\mathcal{O} - 1\}\}$
8: $\phi \leftarrow$ Representative(O_i) ▷ Choose a representative of the orbit O_i
9: $U' \leftarrow \mathrm{Stab}\left(V \oplus \mathrm{Span}(\{\phi\})\right) \cap U$
10: $\mathcal{H}' \leftarrow \cup_{j \geq i} O_j$
11: $\mathcal{S} \leftarrow \mathcal{S} \cup$ ExpandSubspace($V, \mathcal{H}', U', d + 1, r$)
12: **end for**
13: **return** $\mathcal{S}$
14: **end if**
15: **end function**
16: **return** ExpandSubspace($T, \mathcal{G}, \mathrm{Stab}(T), \ell, r$)

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 $\sigma(\phi_3) = \phi_2$.

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 the enumeration 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 9 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.

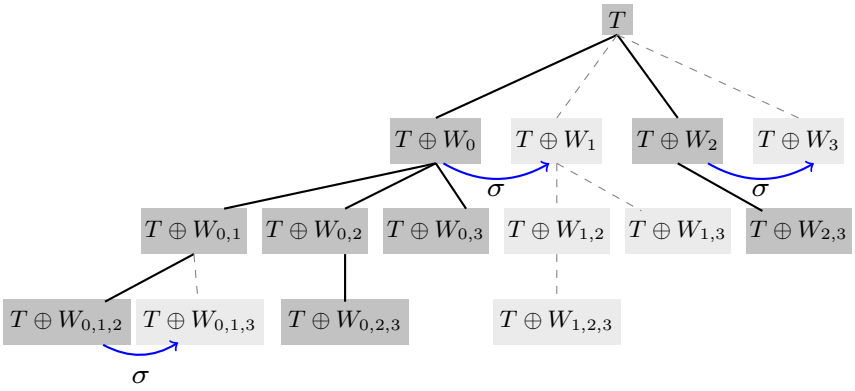

Figure 2: Pruning branches in an exhaustive search using automorphisms.

4. Algebraic structure of some bilinear maps

In this section, we describe the structure of some vector spaces corresponding to bilinear maps that are considered in our applications. This section can be skipped on a first read. It is needed to prove properties of specific bilinear maps that are stated in Section 5. In particular, we need to know the structure of the stabilizer of a vector space in order to be able to improve on the exhaustive search.

4.1. Short product

For the purpose of this section, we restrict our discussion to the specific case defined as follows. Let ℓ be a positive integer, let $\mathbf{\Phi}$ be the bilinear map $\mathbf{\Phi} \in \mathcal{L}(K^\ell, K^\ell; K^\ell)$ defined by the short product

$$\mathbf{\Phi} : \begin{pmatrix} a_0 \\ \vdots \\ a_{\ell-1} \end{pmatrix}, \begin{pmatrix} b_0 \\ \vdots \\ b_{\ell-1} \end{pmatrix} \mapsto \begin{pmatrix} c_0 \\ \vdots \\ c_{\ell-1} \end{pmatrix}$$

such that $\sum_{0 \le i < \ell} c_i X^{\ell-1-i} = (\sum_{0 \le i < \ell} a_i X^i)(\sum_{0 \le i < \ell} b_i X^{\ell-1-i}) \mod X^\ell$. Let T be the subspace of $\mathcal{L}(K^\ell, K^\ell; K)$ spanned by the ℓ bilinear forms that are the coordinates of $\mathbf{\Phi}$, denoted by $\Phi_0, \ldots, \Phi_{\ell-1}$.

The matrix representing the element $\sum_{0 \le i < \ell} m_i \Phi_i \in T$, where $m_i \in K$, is

$$M(m_0, \ldots, m_{\ell-1}) = \begin{bmatrix} m_0 & m_1 & \cdots & m_{\ell-1} \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & m_1 \\ 0 & \cdots & 0 & m_0 \end{bmatrix},$$

in the canonical basis. This matrix is an upper triangular Toeplitz matrix.

Let N be the matrix $M(0, \ldots, 1, 0)$. The matrix N is a nilpotent matrix such that

$$\forall j \in \{0, \ldots, \ell-1\}, \; M(0, \ldots, 0, 1, \underbrace{0, \ldots, 0}_{j \text{ zeros}}) = N^j,$$

and $N^\ell = 0$. The elements of the algebra $K[N]$ are the upper triangular Toeplitz matrices and $K[N] \cong K[X]/(X^\ell)$.

We provide in Theorem 13 a useful property describing the action of $\mathrm{Stab}(T)$ on T.

Theorem 13. *Let any integer $\ell \geq 2$:*

1. *the orbit of the identity matrix $I = N^0$ for the action of $\mathrm{Stab}(T)$ is the set of invertible matrices of T;*
2. *the orbit of N for the action of $\mathrm{Stab}(T) \cap \mathrm{Stab}(I)$ is the set of nilpotent matrices of T;*
3. *for any pair (Ψ, Ψ') of elements of T such that $\mathrm{rk}(\Psi) = \ell$ and $\mathrm{rk}(\Psi') = \ell - 1$, there exists $\sigma \in \mathrm{Stab}(T)$ such that*
$$(\Psi \circ \sigma, \Psi' \circ \sigma) = (I, N);$$
4. *we have $\mathrm{Stab}(I) \cap \mathrm{Stab}(N) \subset \mathrm{Stab}(T)$ and the cardinality of $\mathrm{Stab}(T)$ is $(\#K)^{3\ell-4}(\#K-1)^3$.*

Proof. See Appendix A.1. □

4.2. Matrix product

We denote by $\mathbf{\Phi}_{p,q,r}$ the bilinear map corresponding to the $p \times q$ by $q \times r$ matrix product:

$$\begin{array}{rccc} \mathbf{\Phi}_{p,q,r}: & \mathcal{M}_{p,q}(K) \times \mathcal{M}_{q,r}(K) & \longrightarrow & \mathcal{M}_{p,r}(K) \\ & (A, B) & \longmapsto & A \cdot B \end{array}.$$

We denote by $\Phi_{i,j}$ the bilinear forms such that $\Phi_{i,j}(A, B)$ is the coefficient (i, j) of $\mathbf{\Phi}_{p,q,r}(A, B)$ for $i \in \{0, \ldots, p-1\}, j \in \{0, \ldots, r-1\}$. The elements $\Phi_{i,j}$ satisfy $\Phi_{i,j}(A, B) = \sum_{0 \leq h < q} a_{i,h} b_{h,j}$.

The bilinear map $\mathbf{\Phi}_{p,q,r}$ is represented by a subspace of $\mathcal{L}(K^{pq}, K^{qr}; K)$ denoted by

$$T_{p,q,r} = \mathrm{Span}((\Phi_{i,j})_{i,j}).$$

In order to represent the elements of $T_{p,q,r}$ in terms of matrices of $\mathcal{M}_{pq,qr}$, we need an order on the $a_{i,h}$'s and $b_{h,j}$'s.

- For the $a_{i,h}$'s, we fix the following order: $a_{i,h} \leq a_{i',h'}$ if $i \leq i'$ or $i = i'$ and $h \leq h'$, which is the row-major order.
- For the $b_{h,j}$'s, we fix the following order: $b_{h,j} \leq b_{h',j'}$ if $j \leq j'$ or $j = j'$ and $h \leq h'$, which is the column-major order.

Then, in the bases of $\mathcal{M}_{p,q}$ and $\mathcal{M}_{q,r}$ given by the $a_{i,h}$'s and $b_{h,j}$'s ordered as above, the elements of $T_{p,q,r}$ can be represented as matrices of $\mathcal{M}_{pq,qr}$ divided in blocks of size $q \times q$ equal to I_q the identity matrix of $\mathcal{M}_{q,q}$. Consequently, this space is isomorphic to $\mathcal{M}_{p,r} \otimes I_q$ and all the elements of $T_{p,q,r}$ have a rank which is multiple of q.

Example 14 (Matrix representation of elements of $T_{2,2,2}$)**.** *The elements of $T_{2,2,2}$ are represented by matrices of $\mathcal{M}_{4,4}$ spanned by*

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

corresponding to the coefficients $a_{0,0}b_{0,0} + a_{0,1}b_{1,0}$, $a_{0,0}b_{0,1} + a_{0,1}b_{1,1}$, $a_{1,0}b_{0,0} + a_{1,1}b_{1,0}$ and $a_{1,0}b_{0,1} + a_{1,1}b_{1,1}$, respectively. The previous matrices can also be expressed as

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes I_2, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \otimes I_2, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes I_2, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes I_2,$$

respectively.

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

$$\Phi_{i,j} = \sum_{0 \leq h < q} e_i \otimes f_h \otimes f_h \otimes g_j.$$

Theorem 15. *For the group action $M \cdot (X, Y) \mapsto X^{\mathrm{T}} M Y$, the subgroup stabilizing the vector space $T_{p,q,r}$ can be described as the group given by the pairs $(P \otimes R^{\mathrm{T}}, Q \otimes (R^{-1}))$ for $P \in \mathrm{GL}_p$, $R \in \mathrm{GL}_q$, and $Q \in \mathrm{GL}_r$.*

Proof. See Appendix A.2. □

Corollary 16. *The elements of $T_{p,q,r}$ of a given rank lie in the same orbit under the action of* $\mathrm{Stab}(T_{p,q,r})$.

Example 17 (Action of the stabilizer of $T_{2,2,2}$)**.** *The stabilizer of $T_{2,2,2}$ is generated by the following elements of* $\mathrm{GL}(K^4) \times \mathrm{GL}(K^4)$*:*

$$\left(\begin{pmatrix}1&0&1&0\\0&1&0&1\\0&0&1&0\\0&0&0&1\end{pmatrix}, \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\right), \left(\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}, \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\right),$$

$$\left(\begin{pmatrix}1&1&0&0\\0&1&0&0\\0&0&1&1\\0&0&0&1\end{pmatrix}, \begin{pmatrix}1&1&0&0\\0&1&0&0\\0&0&1&1\\0&0&0&1\end{pmatrix}\right), \left(\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}, \begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\right),$$

$$\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, \begin{pmatrix}1&0&1&0\\0&1&0&1\\0&0&1&0\\0&0&0&1\end{pmatrix}\right), \left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, \begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}\right).$$

The vector space of $T_{2,2,2}$ is isomorphic to $\mathcal{M}_{2,2} \otimes I_2$. Thus the elements of $T_{2,2,2}$ have rank 0, 2 *or* 4.

Via the action of $\mathrm{Stab}(T_{2,2,2})$*, all the elements of rank* 2 *can all be mapped to the element*

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

Similarly, via the action of $\mathrm{Stab}(T_{2,2,2})$*, all the elements of rank* 4 *can all be mapped to the element*

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

5. Coverings of subspaces of bilinear forms

Our contribution consists in reducing the number of vector spaces W that we need to enumerate in order to get those that satisfy $T \oplus W \in \mathscr{S}_r$, where T is the vector space representing a given bilinear map. To this effect, we restrict the enumeration to vector spaces W satisfying some properties which are 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 and the matrix product. In Section 6, we deal with practical and computational aspects.

5.1. Theoretical aspect

Our strategy consists, first, for any $r \geq \ell$, in constructing g sets $\mathcal{E}_{i,r}$ for $i \in \{0, \ldots, g-1\}$, that are all subsets of $\mathscr{S}_{r-\ell+k_i}$, where k_i is a nonnegative integer, and that satisfy some property described in Definition 18.

Definition 18 (Covering of a vector space)**.** *Let T be a subspace of $\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ of dimension ℓ. Let $\{\mathcal{E}_{i,r}\}_{0 \leq i < g}$ be a set of subsets parameterized by an integer $r \geq \ell$ and where $\mathcal{E}_{i,r} \subset \mathscr{S}_{r-\ell+k_i}$, k_i being a nonnegative integer, for all $i \in \{0, \ldots, g-1\}$,. Then, $(\mathcal{E}_{i,r})_{0 \leq i < g}$ is said to be a covering of T if and only if, for any vector space $W \in \mathscr{S}_{r-\ell}$ such that $T \oplus W \in \mathscr{S}_r$, there exist an index $i \in \{0, \ldots, g-1\}$, a subspace $V \in \mathcal{E}_{i,r}$, and an automorphism $\sigma \in \mathrm{Stab}(T)$ such that $T + (V \circ \sigma) = T \oplus W$.*

Proposition 19. *Given T as above and a covering $(\mathcal{E}_{i,r})_{0 \leq i < g}$ of T, then, for any $r \geq \ell$, we have*

$$\mathscr{S}_r(T) \subset \{T + V \mid \exists i \in \{0, \ldots, g-1\}\,,\ V \in \mathcal{E}_{i,r} \circ \mathrm{Stab}(T)\}.$$

Proof. Let $V \in \mathscr{S}_r(T)$. By Proposition 6, there exists $W \in \mathscr{S}_{r-\ell}$ such that $T \oplus W = U$. Then, by Definition 18, there exist an index $i \in \{0, \ldots, g-1\}$, a subspace $V \in \mathcal{E}_{i,r}$, and an automorphism $\sigma \in \mathrm{Stab}(T)$ such that $T + (V \circ \sigma) = T \oplus W$. Taking $V' = V \circ \sigma$, we thus have $U = T + V'$ and $V' \in \mathcal{E}_{i,r} \circ \mathrm{Stab}(T)$, which proves the inclusion. □

Thus, assuming that we have a method for computing the $\mathcal{E}_{i,r}$'s, we are able to cover the whole set $\mathscr{S}_r(T)$. For example, the set composed of the single set $\mathcal{E}_{0,r} = \mathscr{S}_{r-\ell}/\mathrm{Stab}(T)$ is a covering of T and can be enumerated using BDEZStab. We describe below how we construct the $\mathcal{E}_{i,r}$'s that we use in practice.

Definition 20 (Stem of a vector space)**.** *For a vector space T, a set $\{F_i\}_{0 \leq i < g}$ of g subspaces $F_i \subset T$ of dimension k_i is said to be a* stem *of T if and only if, for any basis $\mathcal{B}$ of T, there exist $i \in \{0, \ldots, g-1\}$, an automorphism $\sigma \in \mathrm{Stab}(T)$ and a free family $\mathcal{F} \subset \mathcal{B}$ of size k_i such that*

$$\mathrm{Span}(\mathcal{F}) \circ \sigma = F_i.$$

Proposition 21. *For a vector space T, a stem 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 $\{\mathcal{E}_{i,r}\}_{0 \leq i < g}$, where each $\mathcal{E}_{i,r}$ is a set of representatives of the quotient $\mathscr{S}_{r-\ell+k_i}(F_i)/U_i$, is a covering of T.*

Proof. Let $W \in \mathscr{S}_{r-\ell}$ be such that $T \oplus W \in \mathscr{S}_r$. Take a basis $\mathcal{W}$ of W, and complete it into a basis of $T \oplus W$ using ℓ rank-one bilinear forms, denoted by $\{\psi_i\}_{0 \leq i < \ell}$. For all $i \in \{0, \ldots, \ell-1\}$, write $\psi_i = t_i + w_i$, with $t_i \in T$ and $w_i \in W$.

The t_i's are linearly independent. Otherwise, there would exist coefficients $(\lambda_i)_{0 \leq i < \ell}$ such that $\sum_{i=0}^{\ell-1} \lambda_i t_i = 0$, whence $\sum_{i=0}^{\ell-1} \lambda_i \psi_i = \sum_{i=0}^{\ell-1} \lambda_i w_i$, which would then contradict the fact that $\{\psi_i\}_{0 \leq i < \ell}$ completes $\mathcal{W}$ into a basis of $T \oplus W$.

Consequently, $\mathcal{B} = \{t_i\}_{0 \le i < \ell}$ is a free family of ℓ vectors of T and, as $\dim(T) = \ell$, $\mathcal{B}$ is a basis of T. Then, by Definition 20, there exist an index $i \in \{0, \ldots, g-1\}$, a subset $\mathcal{F} \subset \mathcal{B}$ of size $k_i = \dim(F_i)$, and an automorphism $\sigma \in \mathrm{Stab}(T)$ such that $\mathrm{Span}(\mathcal{F}) \circ \sigma = F_i$.

Let $V = W \oplus \mathrm{Span}(\mathcal{F})$. Writing $\mathcal{F} = \{t_i\}_{i \in I}$, with $I \subset \{0, \ldots, \ell-1\}$, we define $\mathcal{F}' = \{\psi_i\}_{i \in I}$. Since $\psi_i = t_i + w_i$ and $\mathrm{Span}(\mathcal{F}') \in \mathscr{S}_{k_i}$, we have $V = W \oplus \mathrm{Span}(\mathcal{F}) = W \oplus \mathrm{Span}(\mathcal{F}') \in \mathscr{S}_{r-\ell+k_i}$.

Now, consider $V' = V \circ \sigma = (W \oplus \mathrm{Span}(\mathcal{F})) \circ \sigma$: we also have $V' \in \mathscr{S}_{r-\ell+k_i}$, as automorphisms preserve the bilinear rank, and $F_i = \mathrm{Span}(\mathcal{F}) \circ \sigma \subset V'$, whence $V' \in \mathscr{S}_{r-\ell+k_i}(F_i)$.

Finally, let $V'' \in \mathcal{E}_{i,r}$ be a representative of the equivalence class of V' in the quotient set $\mathscr{S}_{r-\ell+k_i}(F_i)/U_i$: there exists an automorphism $\gamma \in U_i$ such that $V'' = V' \circ \gamma$. We then have

$$T + (V'' \circ \gamma^{-1} \circ \sigma^{-1}) = T + (V' \circ \sigma^{-1}) = T + V = T + (W \oplus \mathrm{Span}(\mathcal{F})) = T \oplus W$$

where the last equality comes from the fact that $\mathrm{Span}(\mathcal{F}) \subset T$. Finally, as $\gamma^{-1} \circ \sigma^{-1} \in \mathrm{Stab}(T)$, this proves the result. □

Given T and a stem of T, we can derive a new algorithm that computes $\mathscr{S}_r(T)$ via the computation of some intermediate sets $\mathcal{E}_{i,r} = \mathscr{S}_{r-\ell+k_i}(F_i)/U_i$ for $i \in \{0, \ldots, g-1\}$.

Example 22 (Two examples of stems)**.** *For any vector space T, let $\mathcal{B}$ be a basis of T. There exists a subset of $\mathcal{B}$ generating T (namely, $\mathcal{B}$): $\{T\}$ is a stem of T. There exists also a subset of $\mathcal{B}$ generating* $\mathrm{Span}(\emptyset)$ *(namely, $\emptyset$): $\{\mathrm{Span}(\emptyset)\}$ is a stem of T.*

- *An enumeration algorithm that uses $\{T\}$ as a stem amounts to computing $\mathscr{S}_r(T)/\mathrm{Stab}(T)$. In this case, we did not decompose the original problem into simpler problems.*
- *If the stem chosen is the set $\{\mathrm{Span}(\emptyset)\}$, this is equivalent to enumerate a set of representatives of the quotient $\mathscr{S}_{r-\ell}(\mathrm{Span}(\emptyset))/\mathrm{Stab}(T)$. For this purpose, no better methods than* BDEZStab *is known.*

Thus, BDEZStab can be seen as an approach derived from the stem $\{\mathrm{Span}(\emptyset)\}$. We propose here other strategies that are derived from stems, given by sets of subspaces $F_i \subset T$ of dimension k_i. The enumeration of a set $\mathscr{S}_{r-\ell+k_i}(F_i)$ is interesting in practice if its cardinality is less than $\#\mathscr{S}_{r-\ell}$. However, its cost depends also on the algorithms used for the computation of quotients and stabilizers and on how large k_i is, which is detailed below.

No automatic method is known to determine, how to choose a stem for a given vector space T: we have to provide a stem for each T. This task has to be done by hand specifically for each bilinear map. We will actually do so in Section 5.2 and 5.3 for the examples of the short product and the matrix. To this end, the determination of the stabilizer, as done in Section 4, plays a key role.

In order to compute a set of the form $\mathscr{S}_{r-\ell+k_i}(F_i)/U_i$, we proceed in two steps. Let $\mathcal{F}_i$ be a basis of F_i. Our strategy assumes that we have a finite representation of a group U_i such that $U_i \subset \mathrm{Stab}(T) \cap \mathrm{Stab}(F_i)$. In Proposition 21, the larger the groups U_i are, the smaller the $\mathcal{E}_{i,r}$'s are. And we prefer to keep the $\mathcal{E}_{i,r}$'s as small as possible, since it gives smaller sets to enumerate. Thus, this should lead us to choose $U_i = \mathrm{Stab}(T) \cap \mathrm{Stab}(F_i)$. However, in practice, the method used in our implementation is specialized to the choice $U_i = \mathrm{Stab}(T) \cap \mathrm{Stab}(\mathcal{F}_i) \subset \mathrm{Stab}(T) \cap \mathrm{Stab}(F_i)$ (we have $\mathrm{Stab}(\mathcal{F}_i) \subset \mathrm{Stab}(F_i)$) because only in this case do we have a practical algorithm to enumerate a set of representatives for the quotient $\mathscr{S}_{r-\ell+k_i}(F_i)/U_i$.

Notation 23. *For a free family $\mathcal{F}$ of k bilinear forms and a positive integer d, we let*

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

In order to enumerate sets of the form $\mathscr{S}_{r-\ell+k_i}(F_i)/\mathrm{Stab}(T) \cap \mathrm{Stab}(\mathcal{F}_i)$, we adopt a two-step strategy.

Remark 24. *This strategy requires the precomputation of a set of representatives of the quotient*

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

Section 6.3 describes how to compute such a set.

However, there is a pratical limit on their dimension k_i, due to the precomputations that are used in our method and that constitute a bottleneck. Assuming that

$$\#\left(\mathscr{S}_d/\mathrm{GL}(K^d) \times \mathrm{GL}(K^d)\right)$$

behaves as $(d!)^{1.1}$ over $\mathbb{F}_2$ (which is an empirical estimate), storing a set of representatives of

$$\mathscr{S}_d/\mathrm{GL}(K^d) \times \mathrm{GL}(K^d)$$

for $d = 13$ would require 15 terabytes for instance. Consequently, given the largest "d" for which we are able to compute in practice

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

we have a practical constraint on how large the $r - \ell + k_i$'s may be: we should have $r - \ell + k_i \leq d$ for all i.

Thus, we precompute the quotient $\mathscr{S}_{r-\ell+k_i}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$. The first step consists in computing $\tilde{\mathscr{S}}_{r-\ell+k_i}(\mathcal{F}_i)$ and is detailed in Section 6.1. The second step applies the action of the left transversal

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

which can be computed using the algorithms proposed in [12] for example.

We describe in Algorithm CoveringSetsMethod the global strategy to find optimal formulae for T in the sense of the bilinear rank, that is, to enumerate $\mathscr{S}_r(T)$ given a stem. We assume that we are given a subspace T and a set of g free families $\mathcal{F}_0, \ldots, \mathcal{F}_{g-1}$ of T such that $\{\mathrm{Span}(\mathcal{F}_i)\}_i$ forms a stem of T.

Algorithm 4 CoveringSetsMethod

Input: $T \in \mathcal{L}(K^m, K^n; K)$ of dimension ℓ, an integer r, a stem $\{\mathcal{F}_i\}_{0 \leq i < g}$, the sets $\left\{\mathscr{S}_{r-\ell+k_i}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)\right\}_{0 \leq i < g}$
Output: $\mathscr{S}_r(T)$

1: $\mathcal{S} \leftarrow \emptyset$
2: **for** $i \in \{0, \ldots, g-1\}$ **do**
3: $\quad \mathcal{Q} \leftarrow \tilde{\mathscr{S}}_{r-\ell+k_i}(\mathcal{F}_i)$, obtained from $\mathscr{S}_{r-\ell+k_i}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ ▷ See Section 6
4: $\quad \mathcal{L} \leftarrow \mathrm{Stab}(\mathcal{F}_i)/\mathrm{Stab}(T) \cap \mathrm{Stab}(\mathcal{F}_i)$
5: $\quad$ **for** $W \in \mathcal{Q}, \sigma \in \mathcal{L}$ **do**
6: $\quad\quad$ **if** HasRankOneBasis$(T + (W \circ \sigma))$ **then**
7: $\quad\quad\quad \mathcal{S} \leftarrow \mathcal{S} \cup \{T + (W \circ \sigma)\}$
8: $\quad\quad$ **end if**
9: $\quad$ **end for**
10: **end for**
11: **return** $\bigcup_{V \in \mathcal{S}} V \circ \mathrm{Stab}(T)$

The computation of the quotient $\mathcal{Q}$ on Line 3 is detailed in Section 6.1.

5.2. A stem for the short product

We use the same notations as in Section 4.1: we denote by $\Phi_0, \ldots, \Phi_{\ell-1}$ the bilinear forms such that

$$\forall i \geq 0,\ \Phi_i(A, B) = \sum_{j \in \{0,\ldots,\ell-1-i\}} a_{i-j} b_{\ell-1-j}$$

and by T the subspace $\mathrm{Span}(\Phi_0, \ldots, \Phi_{\ell-1})$.

In order to produce a covering of the vector spaces W satisfying $T \oplus W \in \mathscr{S}_r(T)$ that we compute with CoveringSetsMethod, we need a stem of T. This stem is given in Proposition 25.

Proposition 25 (Stem for the short product)**.** *For any $\ell \geq 2$ the singleton $\{\mathrm{Span}(\Phi_0, \Phi_1)\}$ is a stem of T: for any basis $\mathcal{B}$ of T, there exists $\sigma \in \mathrm{Stab}(T)$ and $\mathcal{F} \subset \mathcal{B}$ of cardinality 2 such that*

$$\mathrm{Span}(\mathcal{F}) \circ \sigma = \mathrm{Span}(\Phi_0, \Phi_1).$$

Proof. We first observe that for any $\Phi \in \mathrm{Span}(\Phi_{\ell-1-i}, \ldots, \Phi_{\ell-1})$, $\mathrm{rk}(\Phi) \leq i+1$. Therefore, any element of rank ℓ in T has a nonzero coordinate over Φ_0 in its decomposition over the basis $(\Phi_0, \ldots, \Phi_{\ell-1})$ and, reciprocally, any element having a nonzero coordinate over Φ_0 has rank ℓ. Thus, a basis $\mathcal{B}$ of T necessarily contains an element of rank ℓ denoted by Ψ. The element Ψ has a nonzero coordinate over Φ_0, when we decompose it over $\{\Phi_0, \ldots, \Phi_{\ell-1}\}$. Similarly, there exist $\Psi' \in \mathcal{B}$ and $\lambda \in K$ for which $\Psi' - \lambda\Psi$ has rank $\ell - 1$.

We then use Theorem 13 to find an element $\sigma \in \mathrm{Stab}(T)$ such that

$$(\Psi \circ \sigma, \Psi' \circ \sigma) = (\Phi_0, \Phi_1) \text{ or } (\Psi \circ \sigma, (\Psi - \lambda\Psi') \circ \sigma) = (\Phi_0, \Phi_1),$$

which concludes. □

We give in Table 1 the cardinality of coverings of $\mathscr{S}_r(T)$ given by Proposition 25.

set	**cardinality**
$\mathscr{S}_2(\mathrm{Span}(\emptyset)) = \mathscr{S}_2$	980
$\mathscr{S}_3(\mathrm{Span}(\Phi_0))$	28
$\mathscr{S}_4(\mathrm{Span}(\Phi_0, \Phi_1))$	6

Table 1: Comparison of the cardinality for $\ell = 3$ of three coverings of T for $K = \mathbb{F}_2$.

In conclusion, we need to compute the following set: $\tilde{\mathscr{S}}_{r-\ell+2}(\{\Phi_0, \Phi_1\})$. We describe in Section 6 how we perform Line 3 of Algorithm CoveringSetsMethod. The set $\mathcal{L}$ on Line 4 of CoveringSetsMethod is, for the short product, a set containing one element, which is the identity element of $\mathrm{GL}(K^\ell) \times \mathrm{GL}(K^\ell)$.

5.3. A stem for the matrix product 3×2 by 2×3 over $\mathbb{F}_2$

We focus here on the special case given by the bilinear map

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

over $K = \mathbb{F}_2$. The rank of this bilinear map is known to be 15 [13]. However, all the optimal formulae are not known. We denote by $\Phi_{i,j}$ the bilinear forms such that $\Phi_{i,j}(A, B)$ is the coefficient (i, j) of $\boldsymbol{\Phi}_{3,2,3}(A, B)$ for $i, j \in \{0, 1, 2\}$. The elements $\Phi_{i,j}$ satisfy $\Phi_{i,j}(A, B) = a_{i,0} b_{0,j} + a_{i,1} b_{1,j}$.

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

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

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

We use the stem of $T_{3,2,3}$ given by Proposition 26.

Proposition 26 (Stem of the matrix product)**.** *The set*

$$\mathcal{C} = \{\mathrm{Span}(\{\Phi_{0,0}+\Phi_{1,1}+\Phi_{2,2}\}), \mathrm{Span}(\{\Phi_{0,0}+\Phi_{1,1}, \Phi_{0,1}+\Phi_{2,2}\}), \mathrm{Span}(\{\Phi_{0,0}+\Phi_{1,1}, \Phi_{1,1}+\Phi_{2,2}\}),$$

$$\mathrm{Span}(\{\Phi_{0,0}+\Phi_{1,1}, \Phi_{2,2}\}), \mathrm{Span}(\{\Phi_{0,0}, \Phi_{1,1}, \Phi_{2,2}\})\}$$

is a stem of $T_{3,2,3}$: for any basis $\mathcal{B}$ of $T_{3,2,3}$, there exists $\mathcal{F} \subset \mathcal{B}$ and $\sigma \in \mathrm{Stab}(T_{3,2,3})$ such that

$$\mathrm{Span}(\mathcal{F}) \circ \sigma \in \mathcal{C}.$$

Proof. Let $\mathcal{B}$ be a basis of $T_{3,2,3}$.

- If there exists an element Φ of rank 6 in $\mathcal{B}$, then, according to Corollary 16, there exists $\sigma \in \mathrm{Stab}(T_{3,2,3})$ such that $\Phi_{0,0} + \Phi_{1,1} + \Phi_{2,2} \in \mathcal{B} \circ \sigma$. 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 $\Phi_{0,0} + \Phi_{1,1} \in \mathcal{B} \circ \sigma$ and, consequently, there exists another element $\Phi' \in \mathcal{B}$ of rank 2 or 4 whose coordinate over $\Phi_{2,2}$ in the basis $(\Phi_{i,j})_{i,j}$ is nonzero: 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 $\Phi_{0,0} + \Phi_{1,1}$. We can prove that there exist 3 such orbits and that there exists $\sigma \in \mathrm{Stab}(T_{3,2,3})$ and $\mathcal{F} \subset \mathcal{B}$ of cardinality 2 such that

$$\mathcal{F} \circ \sigma = \begin{cases} \{\Phi_{0,0} + \Phi_{1,1}, \Phi_{0,1} + \Phi_{2,2}\} \\ \text{or} \\ \{\Phi_{0,0} + \Phi_{1,1}, \Phi_{1,1} + \Phi_{2,2}\} \\ \text{or} \\ \{\Phi_{0,0} + \Phi_{1,1}, \Phi_{2,2}\}. \end{cases}$$

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

$$\mathcal{F} \circ \sigma = \{\Phi_{0,0}, \Phi_{1,1}, \Phi_{2,2}\}.$$

□

6. How to compute subspaces containing specific bilinear forms

We propose in this section a method for computing 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 5.2 or 5.3. More specifically, we are interested in computing sets defined as $\tilde{\mathscr{S}}_{r-\ell+k}(\{\Psi_0, \ldots, \Psi_{k-1}\})$, 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 $\mathrm{Stab}(\{\Psi_0, \ldots, \Psi_{k-1}\})$.

6.1. General approach

First, our strategy consists in precomputing the quotient $\mathscr{S}_{m,n,r-\ell+k}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$. This quotient is smaller than $\mathscr{S}_{m,n,r-\ell+k}$ by construction. We explain how to compute it in Section 6.3.

Algorithm 5 explains how we compute the quotient $\mathcal{Q}$ in Algorithm CoveringSetsMethod.

Algorithm 5 IntermediateSetViaQuotientComputation

Input: $\mathscr{S}_{m,n,r-\ell+k}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n), \{\Psi_0, \ldots, \Psi_{k-1}\} = \mathcal{F}$
Output: $\mathcal{Q}$ a sest of representatives per orbit of $\tilde{\mathscr{S}}_{r-\ell+k}(\mathcal{F})$
1: $\mathcal{Q} \leftarrow \emptyset$
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: $\mathcal{Q} \leftarrow \mathcal{Q} \cup \{W \circ \sigma\}$
6: **end if**
7: **end for**
8: **end for**
9: **return** $\mathcal{Q}$

Correctness of Algorithm 5. By construction, according to Line 4, any element of $\mathcal{Q}$ is an element of

$$\mathscr{S}_{r-\ell+k}(\{\Psi_0, \ldots, \Psi_{k-1}\}).$$

- First, we prove that any orbit of $\tilde{\mathscr{S}}_{r-\ell+k}(\{\Psi_0, \ldots, \Psi_{k-1}\})$ has a representative in $\mathcal{Q}$.

  Let W' be a representative of an orbit in $\tilde{\mathscr{S}}_{r-\ell+k}(\{\Psi_0, \ldots, \Psi_{k-1}\})$. There exist $\sigma \in \mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ and W a representative of an element of $\mathscr{S}_{m,n,r-\ell+k}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ 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 $\tilde{\mathscr{S}}_{r-\ell+k}(\{\Psi_0, \ldots, \Psi_{k-1}\})$.

- In the following, we prove that each orbit of $\tilde{\mathscr{S}}_{r-\ell+k}(\{\Psi_0, \ldots, \Psi_{k-1}\})$ has a unique representative in $\mathcal{Q}$.

  Assume that there exist $W, W' \in \mathcal{Q}$ and $\gamma \in \mathrm{Stab}(\{\Psi_0, \ldots, \Psi_{k-1}\})$ such that $W = W' \circ \gamma$. By construction, there exists $W_0, W_0' \in \mathscr{S}_{r-\ell+k}$ and $\sigma, \sigma' \in \mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ such that $W = W_0 \circ \sigma$ and $W' = W_0' \circ \sigma'$. Then $W_0' = W_0 \circ \sigma \circ \gamma^{-1} \circ \sigma'^{-1}$, whence $W_0' = W_0$ as on Line 2 of Algorithm 5 we enumerate only one representative of each orbit of $\mathscr{S}_{r-\ell+k}/\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$. Thus, $\sigma \circ \gamma^{-1} \circ \sigma'^{-1} \in \mathrm{Stab}(W_0)$.

  Still by construction, there exists $\{\Phi_0, \ldots, \Phi_{k-1}\}$ and $\{\Phi_0', \ldots, \Phi_{k-1}'\} \subset W_0$ such that

  $$\{\Phi_0, \ldots, \Phi_{k-1}\} \circ \sigma = \{\Psi_0, \ldots, \Psi_{k-1}\}$$

and

$$\{\Phi'_0, \ldots, \Phi'_{k-1}\} \circ \sigma' = \{\Psi_0, \ldots, \Psi_{k-1}\}.$$

Then,

$$\{\Phi'_0, \ldots, \Phi'_{k-1}\} = \{\Psi_0, \ldots, \Psi_{k-1}\} \circ \sigma'^{-1} = \{\Psi_0, \ldots, \Psi_{k-1}\} \circ \gamma^{-1} \circ \sigma'^{-1} = \{\Phi_0, \ldots, \Phi_{k-1}\} \circ \sigma \circ \gamma^{-1} \circ \sigma'^{-1}$$

and $\{\Phi_0, \ldots, \Phi_{k-1}\}$ is in the same orbit as $\{\Phi'_0, \ldots, \Phi'_{k-1}\}$ under the action of $\mathrm{Stab}(W_0)$, which is contradictory with the definition of the quotient on Line 3.

□

Testing the predicate on 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 two matrices, for example three matrices (M_0, M_1, M_2) mapped to (N_0, N_1, N_2), we compute (X, Y) such that (M_0, M_1) is mapped to (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 InvermediateSetViaQuotientComputation 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.

6.2. Application to the short product

We come back to the example given in Section 5.2 corresponding to the short product. We recall that T is the subspace obtained from the bilinear map given by the short product modulo ℓ and that we need to compute the set $\mathcal{Q} = \tilde{\mathscr{S}}_{r-\ell+2}(\{\Phi_0, \Phi_1\})$ for a given integer r.

If we take $\ell = 3$, we can represent Φ_0 and Φ_1 by the matrices

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

Thus, for a given couple (M_0, M_1) of matrices representing bilinear forms of a subspace $W \in \mathscr{S}_{r-\ell+2}/\mathrm{GL}(K^\ell) \times \mathrm{GL}(K^\ell)$, we are looking for invertible matrices X and Y such that

$$X^{\mathrm{T}} M_0 Y = I \text{ and } X^{\mathrm{T}} M_1 Y = N,$$

which is done in Algorithm 6. As it is precised on Line 4 of Algorithm 6, we find X and Y such that $X^{\mathrm{T}} M_0 Y = I$ via Gauss reduction. Then, we need to check whether $X^{\mathrm{T}} M_1 Y$ and N are similar or not ($(X^{\mathrm{T}} M_1 Y)^\ell$ should be the null matrix for this purpose), as done on Line 7 of Algorithm 6.

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

$$\mathcal{L} = \mathrm{Stab}(\{I, N\}) / \mathrm{Stab}(T) \cap \mathrm{Stab}(\{I, N\})$$

and to compute $\mathcal{Q} \circ \mathcal{L}$. According to Theorem 13, we have $\#\mathcal{L} = 1$, which means that Algorithm 6 actually returns $\tilde{\mathscr{S}}_{r-\ell+2}(\{I, N\}) \circ \mathcal{L}$.

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

Algorithm 6 IntermediateSetViaQuotientComputation (Short product)

Input: $\mathscr{S}_{r-\ell+2}/\mathrm{GL}(K^\ell) \times \mathrm{GL}(K^\ell)$
Output: One representative per orbit of $\mathcal{Q}$, defined as above

$\mathcal{Q} \leftarrow \emptyset$
for $W \in \mathscr{S}_{\ell,\ell,r-\ell+2}/\mathrm{GL}(K^\ell) \times \mathrm{GL}(K^\ell)$ **do**
  for $\Psi \in \{\Phi \in W \mid \mathrm{rk}(\Phi) = \ell\}/\mathrm{Stab}(W)$ **do**
    Let σ such that $\Psi \circ \sigma = I$ ▷ We obtain σ via a Gauss reduction
    $W' \leftarrow W \circ \sigma$
    for $\Psi' \in \{\Phi \in W' \mid \mathrm{rk}(\Phi) = \ell - 1\}/\mathrm{Stab}(W') \cap \mathrm{Stab}(I)$ **do**
      if $\exists \sigma' \in \mathrm{Stab}(I),\ \Psi' \circ \sigma' = N$ **then** ▷ Using that N and Ψ' are similar
        $\mathcal{Q} \leftarrow \mathcal{Q} \cup \{W \circ \sigma \circ \sigma'\}$
      end if
    end for
  end for
end for
return $\mathcal{Q}$

6.3. 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 6.1. Its cost is at least exponential in d, m and n and difficult to estimate.

Notation 27. *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 exist d rank-one bilinear forms $\phi_t : (\mathbf{a}, \mathbf{b}) \mapsto \alpha_t(\mathbf{a}) \cdot \beta_t(\mathbf{b})$ such that $W = \mathrm{Span}\left((\phi_t)_{t\in\{0,\ldots,d-1\}}\right)$. 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 exist two matrices $U \in \mathcal{M}_{d,m}$ and $V \in \mathcal{M}_{d,n}$, whose rows are given by the linear forms α_t and β_t respectively, and W can be represented by the pair (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 pair of matrices (U, V) representing some vector space W, there exists $\sigma = \mu \times \nu$ in $\mathrm{GL}(K^m) \times \mathrm{GL}(K^n)$ such that the pair of matrices U', V', such that $(U', V') = (U \circ \mu, V \circ \nu)$ represents $W \circ \sigma$, are the reduced column echelon form of the matrices U and V, respectively.

Example 28. *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 pair of matrices (U, V) associated to W is

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

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 pairs of matrices $(U, V) \in \mathcal{M}_{d,d} \times \mathcal{M}_{d,d}$ in reduced column echelon form, we obtain all the elements of

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

by considering the subset Ω'_d 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 $\mathrm{rk}(V) \leq \min(n, d)$. Given m and n, a set of representatives for

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

can be seen as matrices $(U', V') \in \mathcal{M}_{d,m} \times \mathcal{M}_{d,n}$ in reduced column echelon form and for which there exists matrices $(U, V) \in \mathcal{M}^2_{d,d}$, representing an element of Ω'_d, obtained by adding $d-m$ an $d-n$ zero columns to U' and V', respectively, or by removing zero columns if $d < m$ or $d < n$.

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' of rank-one bilinear forms 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, compared to d, is not large generically. However, there are degenerate cases for which the nomber of bases is very large (exponential in d^2). These cases require specific code to recognize them and to treat them separately.

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 which checks for each pair of elements of the set $\mathcal{L}$ whether or not they are isomorphic, computed in Line 9 of 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 $d \in \{1, \ldots, 8\}$ and $K = \mathbb{F}_2$ 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	$11,289$	$265,577$
upper bound	1	9	$4.4 \cdot 10^2$	$9.9 \cdot 10^4$	$9.5 \cdot 10^7$	$3.8 \cdot 10^{11}$	$6.1 \cdot 10^{15}$	$4.0 \cdot 10^{20}$
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

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

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 show in Figure 3 how the subspaces of Ω_3 over $\mathbb{F}_2$ are related to Ω_2 and Ω_1 by using its partially ordered set structure. Each element of Ω_d is represented by the corresponding couple of matrices (U, V) of $\mathcal{M}^2_{d,d}$.

7. Experimental results

An implementation in Magma V2.21-3 [5] of the algorithms presented in the previous sections has been done[1]. 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 is neither multithreaded nor written 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

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

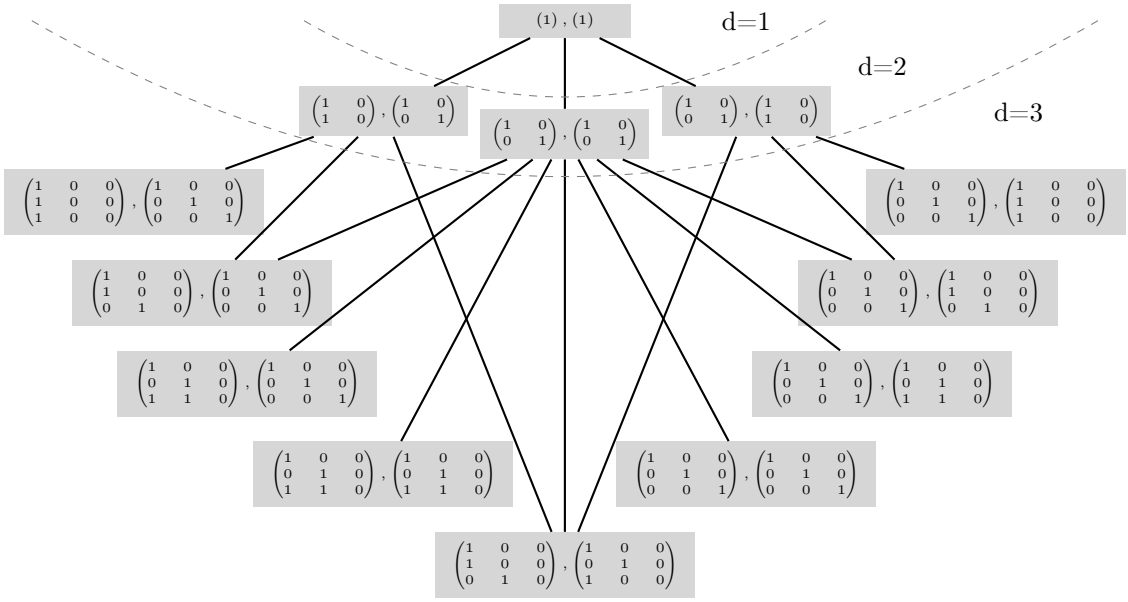

Figure 3: Partially ordered structure of the Ω_d for $d \leq 3$ and $K = \mathbb{F}_2$.

huge speed-up on particular instances of the bilinear rank problem 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 of a 3.3 GHz Intel Core i5-4590 processor.

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 product of polynomials modulo X^ℓ,
- $\mathsf{CirculantProduct}_\ell$ denotes the product of polynomials modulo $X^\ell - 1$.

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

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. We denote by $\mathcal{N}_t$ the number of calls to HasRankOneBasis in these algorithms when the input r is equal to $\ell + t$. (ℓ is the dimension of the vector space T corresponding to the bilinear map). Since when r is too large, BDEZ is too expensive, there is a practical limit on the known values of $\mathcal{N}_t$, t being a positive integer. We consider the ratio $\lceil \frac{\mathcal{N}_t}{\mathcal{N}_{t-1}} \rceil$ to estimate $\mathcal{N}_{t+1}$. Assuming that this ratio decreases with t, which seems to hold empirically, we have

$$\mathcal{N}_{t+1} \leq \left\lceil \frac{\mathcal{N}_t}{\mathcal{N}_{t-1}} \right\rceil \cdot \mathcal{N}_t, \tag{1}$$

t being a positive integer of $\{1, \ldots, r - \ell\}$.

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 bilinear maps 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

$$\mathcal{N}_t \cdot \left\lceil \frac{\mathcal{N}_t}{\mathcal{N}_{t-1}} \right\rceil^{r-\ell-t}$$

where $r-\ell$ is the difference $\mathrm{rk}(T) - \dim(T)$ for T representing a bilinear map and t is the largest integer for which we are able to compute $\mathcal{N}_t$. The time can be estimated with a similar technique. We observe that the speed-up seems to match with $\#\,\mathrm{Stab}(T)$, as expected. The estimated values in Table 3 relying on BDEZStab have not been effectively done because the implementation of CoveringSetsMethod allowed us to obtain more results, more efficiently. The estimations rely on the heuristic given by the Inequality 1. In the global strategy, we increase progressively the lower bound r on the rank, before running BDEZ, BDEZStab or CoveringSetsMethod. For $r < \mathrm{rk}(T)$, the time spent in those algorithms is negligible, because of the exponential growth of their complexity.

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 6.3. Moreover, being able to decompose a matrix product of larger dimensions, such as 3×3 by 3×3, requires to improve on the theoretical aspect of our strategy, since the size of the required set

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

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

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

7.2. Matrix product 3×2 *by* 2×3

We give in this section the timings obtained with our approach for computing the bilinear rank of the matrix product $(3, 2, 3)$ over $\mathbb{F}_2$. We use the same notations as in Section 5.3. We recall that we denote by $\mathbf{\Phi}_{3,2,3}$ the bilinear map

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

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

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

As described in Section 6.1, 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, given the stem that is used, we can restrict the enumeration to subspaces containing at least one element of rank 6. The techniques for computing theses subsets are described in Section 6.3.

The intermediate sets, corresponding to the quotient $\mathcal{Q}$ computed using IntermediateSetViaQuotientComputation in Section 6, were computed in $1.6 \cdot 10^5$ seconds. They are defined as the following sets: $\tilde{\mathcal{E}}_0 = \tilde{\mathscr{S}}_7(\{\Phi_{0,0} + \Phi_{1,1} + \Phi_{2,2}\})$, $\tilde{\mathcal{E}}_1 = \tilde{\mathscr{S}}_8(\{\Phi_{0,0} + \Phi_{1,1}, \Phi_{0,1} + \Phi_{2,2}\})$, $\tilde{\mathcal{E}}_2 = \tilde{\mathscr{S}}_8(\{\Phi_{0,0} + \Phi_{1,1}, \Phi_{1,1} + \Phi_{2,2}\})$, $\tilde{\mathcal{E}}_3 = \tilde{\mathscr{S}}_8(\{\Phi_{0,0} + \Phi_{1,1}, \Phi_{2,2}\})$, $\tilde{\mathcal{E}}_4 = \tilde{\mathscr{S}}_9(\{\Phi_{0,0}, \Phi_{1,1}, \Phi_{2,2}\})$. For the set $\tilde{\mathcal{E}}_4$, we actually used an additional trick, described in Appendix B, which allowed us to consider only a much smaller subset $\tilde{\mathcal{E}}'_4$.

We give in Table 4 the time required to compute the second step of Section 6.1, which corresponds to $\mathcal{Q} \circ \mathcal{L}$ calls to HasRankOneBasis.

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 $\mathbf{\Phi}_{3,2,3}$ 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 *by* 3×2

We denote by $\mathbf{\Phi}_{2,3,2}$ the bilinear map

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

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

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

- $\tilde{\mathcal{E}}_0 = \tilde{\mathscr{S}}_9(\{\Phi_{0,0} + \Phi_{1,1}, \Phi_{0,0} + \Phi_{0,1} + \Phi_{1,0}\})$,
- $\tilde{\mathcal{E}}_1 = \tilde{\mathscr{S}}_9(\{\Phi_{0,0} + \Phi_{1,1}, \Phi_{0,0}\})$.

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 $(\Phi_{0,0}, \Phi_{1,1}, \Phi_{0,1}, \Phi_{1,0})$ 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 6 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 1,096,452 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 HasRankOneBasis 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 $T_{2,3,2}$ such that there exist $w_0, w_1 \in W$ such that $t_0 - w_0$ and $t_1 - w_1$ have rank one. We enumerate the elements $w \in W$ such that the rank of $t_0 - w$ or $t_1 - w$ is one, 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 $\mathscr{S}_r(T)$, where T is the vector space generated by the bilinear forms associated to $\mathsf{ShortProduct}_\ell$ for $\ell = 4$ and $\ell = 5$ and $r = \mathrm{rk}(T)$.

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 $\mathscr{S}_r(T)$.

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

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 Φ_i of the bilinear map

$$\mathbf{\Phi} : (A, B) \mapsto A \cdot B \bmod (X^5 - 1) = \begin{pmatrix} \Phi_0 \\ \Phi_1 \\ \Phi_2 \\ \Phi_3 \\ \Phi_4 \end{pmatrix} = \begin{pmatrix} a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_0 \\ a_4b_2 + a_3b_3 + a_2b_4 + a_1b_0 + a_0b_1 \\ a_4b_3 + a_3b_4 + a_2b_0 + a_1b_1 + a_0b_2 \\ a_4b_4 + a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 \\ a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4 \end{pmatrix}.$$

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 $\phi = \Phi_0 + \Phi_1 + \Phi_2 + \Phi_3 + \Phi_4$ and a hyperplane H such that H contains all the elements of rank 4 and such that 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 (proved by an exhaustive enumeration in $\mathbb{F}_2$), 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: either 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 sets to compute:

- $\tilde{\mathcal{E}}_0 = \tilde{\mathscr{S}_6}(\{\Phi_4\})$ and
- $\mathcal{E}_1 = \mathscr{S}_9(\mathrm{Span}(H))/\mathrm{Stab}(H)$ (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

$$\tilde{\mathcal{E}}_1 = \tilde{\mathscr{S}_6}(\{\Phi_0 + \Phi_1 + \Phi_2 + \Phi_3\}).$$

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 6.1. The set $\mathscr{S}_{10}(T)$ contains 2025 elements divided in 9 equivalence classes of solutions. Interestingly, the set $\tilde{\mathcal{E}}_0$ 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 Appendix B. An important obstacle is the fact that, assuming that the rank is 21, it would require 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, 23, 22].

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.

Bibliography

[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] V. Y. Pan. Strassen's algorithm is not optimal trilinear technique of aggregating, uniting and canceling for constructing fast algorithms for matrix operations. In *Proceedings of the 19th Annual Symposium on Foundations of Computer Science*, SFCS '78, pages 166–176, Washington, DC, USA, 1978. IEEE Computer Society. doi:10.1109/SFCS.1978.34.

[22] 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.

[23] 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.

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

[25] 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.

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

[27] 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

In this section, we prove Theorem 13, using the notations of Section 4.1: the bilinear map

$$\mathbf{\Phi}_\ell : (A, B) \longmapsto A \cdot B \bmod X^\ell = \begin{pmatrix} a_{\ell-1}b_0 + \cdots + a_0 b_{\ell-1} \\ \vdots \\ a_1 b_0 + a_0 b_1 \\ a_0 b_0 \end{pmatrix}$$

is the bilinear map corresponding to the short product modulo X^ℓ, $\Phi_0, \ldots, \Phi_{\ell-1}$ are the bilinear forms such that

$$\forall i \geq 0,\ \Phi_i(A, B) = \sum_{j \in \{0,\ldots,\ell-1-i\}} a_{i-j} b_j$$

and T is the subspace $\mathrm{Span}(\Phi_0, \ldots, \Phi_{\ell-1})$.

We recall that T is represented by the ring $K[N]$ of polynomials of degree less than or equal to $\ell-1$ evaluated in the matrix N, which is a nilpotent matrix. For example, for $\ell=4$,

$$a_0N^0+a_1N^1+a_2N^2+a_3N^3=\begin{pmatrix}a_0&a_1&a_2&a_3\\0&a_0&a_1&a_2\\0&0&a_0&a_1\\0&0&0&a_0\end{pmatrix}.$$

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

Theorem 13. *Let any integer $\ell\geq 2$:*

1. *the orbit of the identity matrix $I=N^0$ for the action of $\mathrm{Stab}(T)$ is the set of invertible matrices of T;*
2. *the orbit of N for the action of $\mathrm{Stab}(T)\cap\mathrm{Stab}(I)$ is the set of nilpotent matrices of T;*
3. *for any pair (Ψ,Ψ') of elements of T such that $\mathrm{rk}(\Psi)=\ell$ and $\mathrm{rk}(\Psi')=\ell-1$, there exists $\sigma\in\mathrm{Stab}(T)$ such that*
$$(\Psi\circ\sigma,\Psi'\circ\sigma)=(I,N);$$
4. *we have $\mathrm{Stab}(I)\cap\mathrm{Stab}(N)\subset\mathrm{Stab}(T)$ and the cardinality of $\mathrm{Stab}(T)$ is $(\#K)^{3\ell-4}(\#K-1)^3$.*

Proof.

- First, we prove that, for any element $M\in T$ of rank ℓ, there exists $R\in K[N]$ a polynomial of degree at most $\ell-1$ such that $R(0)\neq 0$ and $R(N)=M$, and that
$$\exists M_1\in\mathrm{Stab}(T),\ I_\ell\cdot M_1=R(N).$$
Any element in the orbit of I_ℓ has rank ℓ and any element of rank ℓ in T is associated to a polynomial $R\in K[N]$ evaluated in N of degree $\ell-1$ such that $R(0)\neq 0$. It remains to prove that the orbit of I_ℓ corresponds exactly to the set of rank-ℓ elements. Given $R\in K[N]$ such that $R(0)\neq 0$, we denote by $M_1(R)$ the element $(I_\ell,R(N))$. This element is in $\mathrm{Stab}(T)$ because, for any S, we have $R(N)S(N)=(RS \bmod X^\ell)(N)$, which is a polynomial evaluated in N of degree at most $\ell-1$. We have:
$$I_\ell\cdot M_1(R)=(I_\ell)^{\mathrm{T}}\cdot I_\ell\cdot R(N)=R(N).$$

- We prove that, for any element $M\in T$ of rank $\ell-1$, there exists $R\in K[N]$ a polynomial of degree at most $\ell-1$ such that $R(0)=0$, $R'(0)\neq 0$ and $R(N)=M$, and that
$$\exists M_2\in\mathrm{Stab}(I_\ell)\cap\mathrm{Stab}(T),\ N\cdot M_2=R(N).$$
An element of the orbit of N is an element of rank $\ell-1$ and an element of rank $\ell-1$ in T is associated to a polynomial $R\in K[N]$ evaluated in N of degree at most $\ell-1$ such that $R(0)=0$ and $R'(0)\neq 0$. It remains to prove that N can mapped to any element of rank $\ell-1$ via the action of $\mathrm{Stab}(I_\ell)\cap\mathrm{Stab}(T)$.

  Let e_ℓ be the vector $(0,\cdots,0,1)$, such that $R(N)\cdot e_\ell$ corresponds to the last colum of $R(N)$. We have $R(N)^{\ell-1}e_\ell\neq 0$. Thus, let $P(N)$ be the matrix whose columns are given by the tuple $(R(N)^{\ell-1}\cdot e_\ell,R(N)^{\ell-2}\cdot e_\ell,\ldots,R(N)\cdot e_\ell,e_\ell)$. We have $R(N)P(N)=(0,R(N)^{\ell-1}\cdot e_\ell,\ldots,R(N)^2\cdot e_\ell,R(N)\cdot e_\ell)=R(N)$. For $i<\ell-1$, the i-th column of $P(N)$ is the $(i+1)$-th column of $R(N)$ by construction. Thus, $P(N)N=R(N)$. Consequently We have $R(N)P(N)=P(N)N$ and $P(N)^{-1}R(N)P(N)=N$. We take $M_2(R)=(P(N)^{\mathrm{T}},P(N)^{-1})$:
$$N\cdot M_2(R)=R(N)\text{ and }M_2(R)\in\mathrm{Stab}(I_\ell)\cap\mathrm{Stab}(T).$$

- Let (Ψ, Ψ') be a couple of elements of T such that $\mathrm{rk}(\Psi) = \ell$ and $\mathrm{rk}(\Psi') = \ell - 1$. Let (P, P') be the corresponding matrices. According to the previous points, there exist $M_1 \in \mathrm{Stab}(T)$ such that $I_\ell \cdot M_1 = P$ and $M_2 \in \mathrm{Stab}(T) \cap \mathrm{Stab}(I_\ell)$ such that $N \cdot M_2 = P' \cdot M_1^{-1}$. Consequently, we have

$$(I_\ell, N) = (P \cdot M_1^{-1} \cdot M_2^{-1}, P' \cdot M_1^{-1} \cdot M_2^{-1}).$$

- We prove that we have $\mathrm{Stab}(I_\ell) \cap \mathrm{Stab}(N) \subset \mathrm{Stab}(T)$ and that, for any $M_3 \in \mathrm{Stab}(I_\ell) \cap \mathrm{Stab}(N)$, there exists $R \in K[N]$ a polynomial of degree at most $\ell - 1$ such that $R(0) \neq 0$ and

$$M_3 = ((R(N)^{-1})^{\mathrm{T}}, R(N)).$$

  Let $M_3 \in \mathrm{Stab}(I_\ell) \cap \mathrm{Stab}(N)$. Since $M_3 \in \mathrm{Stab}(I_\ell)$, there exists $P \in \mathrm{GL}_\ell$ such that $M_3 = ((P^{-1})^{\mathrm{T}}, P)$ and, since $M_3 \in \mathrm{Stab}(N)$, $P^{-1}NP = N$. We have $PN = NP$.

  Multiplying a matrix by N on the left shifts the rows upward and multiplying N 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 is equal to the evaluation in N of a polynomial R such that $R(0) \neq 0$, from which we deduce that

$$M_3 = ((R(N)^{-1})^{\mathrm{T}}, R(N)) \text{ and } M_3 \in \mathrm{Stab}(T).$$

  Given the form of the elements of $\mathrm{Stab}(I_\ell) \cap \mathrm{Stab}(N)$, its cardinality is equal to the number of polynomials R of degree at most $\ell - 1$ such that $R(0) \neq 0$, which is $\#K^{\ell-1}(K-1)$. Combining with the fact that there are $\#K^{\ell-1}(K-1) \cdot \#K^{\ell-2}(K-1)$ pairs (Ψ, Ψ') of elements of T such that $\mathrm{rk}(\Psi) = \ell$ and $\mathrm{rk}(\Psi') = \ell - 1$, we have $\#\mathrm{Stab}(T) = \#K^{3\ell-4}(\#K - 1)^3$.

□

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 $M \cdot (X, Y) \mapsto X^{\mathrm{T}}MY$, we want to prove Theorem 15.

Theorem 15. *For the group action $M \cdot (X, Y) \mapsto X^{\mathrm{T}}MY$, the subgroup stabilizing the vector space $T_{p,q,r}$ can be described as the group given by the pairs $(P \otimes R^{\mathrm{T}}, Q \otimes (R^{-1}))$ for $P \in \mathrm{GL}_p$, $R \in \mathrm{GL}_q$, and $Q \in \mathrm{GL}_r$.*

Proof. 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 the Hamming weight for the matrix product

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 still denote by T the subspace of $\mathcal{L}(K^6, K^6; K)$ corresponding to the coefficients of the product of 3×2 by 2×3 matrices. We recall the stem of T that we consider:

$$\mathcal{C} = \{\mathrm{Span}(\{\Phi_{0,0}+\Phi_{1,1}+\Phi_{2,2}\}), \mathrm{Span}(\{\Phi_{0,0}+\Phi_{1,1}, \Phi_{0,1}+\Phi_{2,2}\}), \mathrm{Span}(\{\Phi_{0,0}+\Phi_{1,1}, \Phi_{1,1}+\Phi_{2,2}\}),$$
$$\mathrm{Span}(\{\Phi_{0,0}+\Phi_{1,1}, \Phi_{2,2}\}), \mathrm{Span}(\{\Phi_{0,0}, \Phi_{1,1}, \Phi_{2,2}\})\}.$$

We define the following sets:

- $\mathcal{E}_0 = \mathscr{S}_7(\mathrm{Span}(\Phi_{0,0}+\Phi_{1,1}+\Phi_{2,2}))$,
- $\mathcal{E}_1 = \mathscr{S}_8(\mathrm{Span}(\Phi_{0,0}+\Phi_{1,1}, \Phi_{0,1}+\Phi_{2,2}))$,
- $\mathcal{E}_2 = \mathscr{S}_8(\mathrm{Span}(\Phi_{0,0}+\Phi_{1,1}, \Phi_{1,1}+\Phi_{2,2}))$,
- $\mathcal{E}_3 = \mathscr{S}_8(\mathrm{Span}(\Phi_{0,0}+\Phi_{1,1}, \Phi_{2,2}))$ and
- $\mathcal{E}_4 = \mathscr{S}_9(\mathrm{Span}(\Phi_{0,0}, \Phi_{1,1}, \Phi_{2,2}))$.

In theory, we have to enumerate the elements of the sets $\tilde{\mathscr{S}_7}(\{\Phi_{0,0}+\Phi_{1,1}+\Phi_{2,2}\})$, $\tilde{\mathscr{S}_8}(\{\Phi_{0,0}+\Phi_{1,1}, \Phi_{0,1}+\Phi_{2,2}\})$, $\tilde{\mathscr{S}_8}(\{\Phi_{0,0}+\Phi_{1,1}, \Phi_{1,1}+\Phi_{2,2}\})$, $\tilde{\mathscr{S}_8}(\{\Phi_{0,0}+\Phi_{1,1}, \Phi_{2,2}\})$ and $\tilde{\mathscr{S}_9}(\{\Phi_{0,0}, \Phi_{1,1}, \Phi_{2,2}\})$, denoted by $\tilde{\mathcal{E}}_0$, $\tilde{\mathcal{E}}_1$, $\tilde{\mathcal{E}}_2$, $\tilde{\mathcal{E}}_3$ and $\tilde{\mathcal{E}}_4$, respectively. However, one can notice that, given $V \in \mathscr{S}_{15}(T)$ such that

$$\exists W \in \tilde{\mathcal{E}}_4, \sigma \in \mathrm{Stab}(\{\Phi_{0,0}, \Phi_{1,1}, \Phi_{2,2}\}),\ V = T + W \circ \sigma,$$

it may happen that there exists $W' \subset V$ such that

$$V = T + W'$$

and

$$\exists \sigma \in \mathrm{Stab}(T),\ W' \circ \sigma \in \begin{cases} \mathscr{S}_7(\mathrm{Span}(\Phi_{0,0}+\Phi_{1,1}+\Phi_{2,2})) \\ \qquad \text{or} \\ \mathscr{S}_8(\mathrm{Span}(\Phi_{0,0}+\Phi_{1,1}, \Phi_{0,1}+\Phi_{2,2})) \\ \qquad \text{or} \\ \mathscr{S}_8(\mathrm{Span}(\Phi_{0,0}+\Phi_{1,1}, \Phi_{1,1}+\Phi_{2,2})) \\ \qquad \text{or} \\ \mathscr{S}_8(\mathrm{Span}(\Phi_{0,0}+\Phi_{1,1}, \Phi_{2,2})) \end{cases}.$$

In other terms, the V's corresponding to the5 sets to enumerate do not form a partition of $\mathscr{S}_{15}(T)$.

Thus, we propose, if possible, to enumerate a subset of $\mathcal{E}_4$, rather than the whole set, without losing exhaustivity. The strategy that is proposed is related to the notion of Hamming weight of the elements $\Phi_{0,0}$, $\Phi_{1,1}$ and $\Phi_{2,2}$.

Definition 29 (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 $\mathcal{B}$:*

$$x = \sum_{0 \le t < d} \lambda_t \cdot \psi_t.$$

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:

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

The Hamming weight over some basis has a useful property related to the bilinear rank stated in Lemma 30.

Lemma 30. *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*

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

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

We describe in Theorem 31 what is the subset of $\tilde{\mathcal{E}}_4$ that we consider.

Theorem 31. *Let W be a subspace such that $W \in \tilde{\mathcal{E}}_4$ and $T_{3,2,3} + W \in \mathscr{S}_{15}$ and let $\mathcal{B}$ be a basis of W composed of rank-one bilinear forms. Let $\tilde{\mathcal{E}}'$ be the subset of elements $W \in \tilde{\mathcal{E}}_4$ such that*

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

We obtain all the elements of $\mathscr{S}_{15}(T)$ via the enumeration of $\tilde{\mathcal{E}}_0$, $\tilde{\mathcal{E}}_1$, $\tilde{\mathcal{E}}_2$, $\tilde{\mathcal{E}}_3$ and $\tilde{\mathcal{E}}'$.

We prove Theorem 31 within 2 steps:

1. We prove in Lemma 32 that if $\mathbb{H}_{\mathcal{B}}(\Phi_{0,0} + \Phi_{1,1} + \Phi_{2,2}) \neq \mathbb{H}_{\mathcal{B}}(\Phi_{0,0}) + \mathbb{H}_{\mathcal{B}}(\Phi_{1,1}) + \mathbb{H}_{\mathcal{B}}(\Phi_{2,2})$, a subspace V obtained as $V = T + W \circ \sigma$ can also be obtained as $V = T + W' \circ \sigma$, with $W' \in \tilde{\mathcal{E}}_0$, $\tilde{\mathcal{E}}_1$ or $\tilde{\mathcal{E}}_3$.
2. Otherwise, if $\mathbb{H}_{\mathcal{B}}(\Phi_{0,0} + \Phi_{1,1} + \Phi_{2,2}) = \mathbb{H}_{\mathcal{B}}(\Phi_{0,0}) + \mathbb{H}_{\mathcal{B}}(\Phi_{1,1}) + \mathbb{H}_{\mathcal{B}}(\Phi_{2,2})$, it remains to prove that we do not lose in generality if we assume that $\mathbb{H}_{\mathcal{B}}(\Phi_{0,0} + \Phi_{1,1} + \Phi_{2,2}) > 6$, which is done in Lemma 33.

Lemma 32. *Let $W \in \mathscr{S}_9$ and let $V = T + W$. We assume that $T + W \in \mathscr{S}_{15}(T)$ and $\mathrm{Span}(\{\Phi_{0,0}, \Phi_{1,1}, \Phi_{2,2}\}) \subset W$. Let $\mathcal{B}$ be a basis of rank-one bilinear forms of W. If $\mathbb{H}_{\mathcal{B}}(\Phi_{0,0} + \Phi_{1,1} + \Phi_{2,2}) \neq \mathbb{H}_{\mathcal{B}}(\Phi_{0,0}) + \mathbb{H}_{\mathcal{B}}(\Phi_{1,1}) + \mathbb{H}_{\mathcal{B}}(\Phi_{2,2})$, there exists $W' \subset W$ such that $V = T + W'$ and there exists $\sigma' \in \mathrm{Stab}(T)$ such that $W' \circ \sigma' \in \mathcal{E}_0, \mathcal{E}_1$ or $\mathcal{E}_3$.*

Proof. We have by hypothesis $\mathbb{H}_{\mathcal{B}}(\Phi_{0,0}+\Phi_{1,1}+\Phi_{2,2}) < \mathbb{H}_{\mathcal{B}}(\Phi_{0,0})+\mathbb{H}_{\mathcal{B}}(\Phi_{1,1})+\mathbb{H}_{\mathcal{B}}(\Phi_{2,2})$. Thus, there exist two elements $\Psi \in \mathcal{B}$ and $\Phi \in \{\Phi_{0,0}, \Phi_{1,1}, \Phi_{2,2}\}$ such that the coordinate of Φ on Ψ is not zero and the coordinates of $\Phi_{0,0}+\Phi_{1,1}+\Phi_{2,2}$ on Ψ is zero. By considering the vector space $W' = \mathrm{Span}(\mathcal{B} - \{\Psi\})$, we have $W' \in \mathscr{S}_8$. Moreover, we have $W = \mathrm{Span}(\{\Psi\}) \oplus W' = \mathrm{Span}(\{\Phi\}) \oplus W'$ and $T + (\mathrm{Span}(\{\Phi\}) \oplus W') =\subset T+W'$. Thus, $\dim(T+W') = \dim(T+W) = 15$. Consequently, $\dim(T \cap W') = 2$.

If there exists in $T \cap W'$ two elements Φ_1 and Φ_2 of rank smaller or equal to 4 such that $\Phi_1 + \Phi_2 = \Phi_{0,0}+\Phi_{1,1}+\Phi_{2,2}$, then

$$\exists \sigma \in \mathrm{Stab}(T),\ W' \circ \sigma \in \begin{cases} \mathscr{S}_8(\mathrm{Span}(\Phi_{0,0}+\Phi_{1,1}, \Phi_{0,1}+\Phi_{2,2})) \\ \text{or} \\ \mathscr{S}_8(\mathrm{Span}(\Phi_{0,0}+\Phi_{1,1}, \Phi_{2,2})) \end{cases}.$$

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

$$\exists \sigma \in \mathrm{Stab}(T),\ W'' \circ \sigma \in \mathscr{S}_7(\mathrm{Span}(\Phi_{0,0}+\Phi_{1,1}+\Phi_{2,2}))$$

and $T + W'' \in \mathscr{S}_{15}$, which concludes. □

Lemma 33. *Let $V \in \mathscr{S}_{15}(T)$. The subspace V satisfies hypotheses **H1** and **H2** state as follows.*

H1: *For any $W \subset V$ such that there exists $\sigma \in \mathrm{Stab}(T)$ satisfying $W \circ \sigma \in \mathscr{S}_9(\mathrm{Span}(\Phi_{0,0}, \Phi_{1,1}, \Phi_{2,2}))$ and $T + W \in \mathscr{S}_{15}$, we have, for any basis $\mathcal{B}$ of rank-one bilinear forms of W,*

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

H2: *There do not exist $W \subset V$ and $\sigma \in \mathrm{Stab}(T)$ such that $W \circ \sigma \in \mathcal{E}_0, \mathcal{E}_1$, $\mathcal{E}_2$ or $\mathcal{E}_3$ and $V = T + W$ (in other terms, V can not be obtained via the enumeration of $\tilde{\mathcal{E}}_0$, $\tilde{\mathcal{E}}_1$, $\tilde{\mathcal{E}}_2$ or $\tilde{\mathcal{E}}_3$).*

Then, there exists $W' \subset V$ and $\sigma' \in \mathrm{Stab}(T)$ such that $W' \circ \sigma' \in \mathscr{S}_9(\mathrm{Span}(\Phi_{0,0}, \Phi_{1,1}, \Phi_{2,2}))$, $T + W' \in \mathscr{S}_{15}$, and W' has a basis $\mathcal{B}'$ of rank-one bilinear forms such that

$$\mathbb{H}_{\mathcal{B}' \circ \sigma'}(\Phi_{0,0}+\Phi_{1,1}+\Phi_{2,2}) > 6.$$

Proof. Let $W \in \mathscr{S}_6$ be such that $T \oplus W \in \mathscr{S}_{15}$. Take a basis $\mathcal{W}$ of W, and complete it into a basis $\mathcal{B}$ of $T \oplus W$ using 9 rank-one bilinear forms, denoted by $\{\psi_i\}_{0 \le i < 9}$. For all $i \in \{0, \ldots, 8\}$, write $\psi_i = \Phi_i + \Psi_i$, with $\Phi_i \in T$ and $\Psi_i \in W$. The Φ_i's form a basis of T. In our context, we are concerned by the case $\mathrm{rk}(\Phi_i) = 2$ for any i (otherwise **H2** is not satisfied). Since we assume Hypothesis **H1**, it is enough to prove that there exists i such that $\mathbb{H}_{\mathcal{B}}(\Phi_i) > 2$.

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 $\#\mathcal{B} \ge 2 \cdot 9 = 18 \ne 15 = \mathrm{rk}(T)$.

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

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

and, by Lemma 30, $\mathrm{rk}(\{\Phi_i, \Phi_{i'}\}) \le 3$. Henceforth, we prove that this is contradictory, because $\mathrm{rk}(\{\Phi_i, \Phi_{i'}\}) = 4$. Indeed, there are two cases.

- If $\Phi_i + \Phi_{i'}$ has rank 4, the conclusion follows.
- If $\mathrm{Span}(\Phi_i, \Phi_{i'})$ 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.

Consequently, $\mathbb{H}_{\mathcal{B}}(\Phi_i) > 2$ or $\mathbb{H}_{\mathcal{B}}(\Phi_{i'}) > 2$. □