Trisymmetric Multiplication Formulae in Finite Fields

Hugues Randriambololona, Édouard Rousseau

Trisymmetric Multiplication Formulae in Finite Fields

Hugues Randriambololona[1,2] and Édouard Rousseau[2,3](✉)

[1] ANSSI, Paris, France
[2] Institut Polytechnique de Paris / Télécom Paris, Palaiseau, France
{randriam,erousseau}@telecom-paris.fr
[3] Université Paris-Saclay / UVSQ, Versailles, France

Abstract. Multiplication is an expensive arithmetic operation, therefore there has been extensive research to find Karatsuba-like formulae reducing the number of multiplications involved when computing a bilinear map. The minimal number of multiplications in such formulae is called the *bilinear complexity*, and it is also of theoretical interest to asymptotically understand it. Moreover, when the bilinear maps admit some kind of invariance, it is also desirable to find formulae keeping the same invariance. In this work, we study *trisymmetric*, *hypersymmetric*, and *Galois invariant* multiplication formulae over finite fields, and we give an algorithm to find such formulae. We also generalize the result that the bilinear complexity and symmetric bilinear complexity of the two-variable multiplication in an extension field are linear in the degree of the extension, to trisymmetric bilinear complexity, and to the complexity of t-variable multiplication for any $t \geq 3$.

1 Introduction

Given an algorithm that computes a polynomial map over a field $\mathbf{k}$ (or a family of such polynomial maps, with entries of length going to infinity), one is usually interested in the (asymptotic) cost of the algorithm. In order to understand this cost, one studies the *complexity* of the algorithm, *i.e.* the number of operations needed by the algorithm. We can for example count the number of bit operations, or the number of algebraic operations $(+, \times)$ in $\mathbf{k}$. The latter is called the *algebraic complexity* and in this model it is supposed that all algebraic operations have the same cost. Nevertheless, multiplication of two variable quantities in $\mathbf{k}$ is arguably more expensive than addition, or than multiplication of a variable by a fixed constant. In the context of the computation of bilinear maps, extensive work has been done to reduce the number of two-variable multiplications involved. Notable examples are Karatsuba's algorithm [11] and Strassen's algorithm [19]. Karatsuba's algorithm is based on the fact that the bilinear map associated to the product of two polynomials of degree 1

$$A = a_1X + a_0 \text{ and } B = b_1X + b_0$$

can be computed with three products $a_0b_0, (a_0+a_1)(b_0+b_1), a_1b_1$ instead of the four classic ones $a_0b_0, a_0b_1, a_1b_0, a_1b_1$. Strassen's algorithm exploits a similar idea in the case of 2×2 matrices: only 7 products are used instead of 8 in order to compute a matrix product. Both these algorithms have very practical consequences. The *bilinear complexity* $\mu(\Phi)$ of a bilinear map Φ over $\mathbf{k}$ represents the minimum number of two-variable multiplications in a formula that computes Φ, discarding the cost of other operations such as addition or multiplication by a constant. In particular when $\mathcal{A}$ is a finite dimensional algebra over $\mathbf{k}$, we define the bilinear complexity of $\mathcal{A}$ as $\mu(\mathcal{A}/\mathbf{k}) = \mu(m_{\mathcal{A}})$ where $m_{\mathcal{A}} : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ is the multiplication map in $\mathcal{A}$ seen as a $\mathbf{k}$-bilinear map.

Let $\mathbf{k}^{2\times2}$ be the algebra of 2×2 matrices over $\mathbf{k}$. We know thanks to Strassen's algorithm that

$$\mu(\mathbf{k}^{2\times2}/\mathbf{k}) \leq 7.$$

In fact, this is optimal, so we have exactly $\mu(\mathbf{k}^{2\times 2}/\mathbf{k}) = 7$ [20, Thm. 3.1]. In general, it seems to be hard to find the bilinear complexity of a given algebra, for example the bilinear complexity of $\mathbf{k}^{3\times 3}$ is not known. In the litterature, work has been done both to algorithmically find the bilinear complexity of small algebras [5,10] and to understand how the bilinear complexity asymptotically grows [9,2]. Chudnovsky and Chudnovsky proved in 1988 that the bilinear complexity of an extension field $\mathbb{F}_{q^k}/\mathbb{F}_q$ is linear in the degree k of the extension, using an evaluation-interpolation method on curves. As the main contribution of this article, we investigate both questions for *trisymmetric* bilinear complexity, and solve a certain number of the open problems stated in [2, §5.2].

When a bilinear map admits certain invariance properties, it can be interesting, both for theoretical and for practical reasons, to find formulae for it that exhibit these same properties. For symmetric bilinear maps, and in particular for commutative algebras, this leads to the notion of symmetric bilinear complexity. A further refinement, the trisymmetric bilinear complexity of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, was first introduced in [16], and rediscovered independently in [14, App. A].

In Section 2 we recall the definition of symmetric and trisymmetric formulae, and discuss further generalizations such as hypersymmetric formulae for higher multilinear maps, and Galois-invariant formulae. In Section 3 we describe algorithms to compute trisymmetric decompositions in small dimension. In all examples we were able to compute, the trisymmetric bilinear complexity is equal to the symmetric bilinear complexity. However we found an example where the Galois-invariant trisymmetric bilinear complexity is strictly larger. Finally, in Section 4, we prove that for all $q \geq 3$, the trisymmetric bilinear complexity of an extension of $\mathbb{F}_q$ is again linear in the degree, as well as similar results for higher multiplication maps.

2 Multiplication formulae with symmetries

Although we are mainly interested in bilinear multiplication formulae, the notions we will consider naturally involve higher multilinear maps.

Multilinear complexity. Let $\Phi : V_1 \times \cdots \times V_t \to W$ be a t-multilinear map between finite dimensional vector spaces over $\mathbf{k}$. A *multilinear algorithm*, or *multilinear decomposition*, or *multilinear formula* of length n for Φ is a collection of linear forms $(\varphi_i^{(j)})_{\substack{1\leq i\leq n\\ 1\leq j\leq t}}$, where $\varphi_i^{(j)}$ is in $V_j^\vee$, the dual vector space of V_j, and elements $(w_i)_{1\leq i\leq n}$ in W, such that for all $v_1, \ldots, v_t$ we have

$$\Phi(v_1, \ldots, v_t) = \sum_{i=1}^{n} \varphi_i^{(1)}(v_1) \cdots \varphi_i^{(t)}(v_t) w_i.$$

The *multilinear complexity* $\mu(\Phi)$ is then defined as the smallest length n of such a decomposition. Equivalently, it is the rank of the tensor in $V_1^\vee \otimes \cdots \otimes V_t^\vee \otimes W$ corresponding to Φ.

Symmetric multilinear complexity. When $V_1 = \cdots = V_t = V$ and Φ is a *symmetric* multilinear map, it is natural to search for *symmetric multilinear decompositions*, *i.e.* formulae of the form

$$\Phi(v_1, \ldots, v_t) = \sum_{i=1}^{n} \varphi_i(v_1) \cdots \varphi_i(v_t) w_i$$

with $\varphi_i^{(1)} = \cdots = \varphi_i^{(t)} = \varphi_i \in V^\vee$ for all i. It is more space-efficient, since symmetric formulae admit a shorter description. From an algorithmic point of view, it should also be simpler to find symmetric formulae, because the search space is smaller. We define $\mu^{\mathrm{sym}}(\Phi)$, the *symmetric*

multilinear complexity of Φ, as the minimal length n of such a symmetric decomposition, if it exists (otherwise we set $\mu^{\mathrm{sym}}(\Phi) = \infty$).

In the case $t = 2$, a symmetric bilinear map always admits a symmetric decomposition. However, when $t \geq 3$ and $\mathbf{k} = \mathbb{F}_q$ is a finite field, this can fail. When $t = 3$ and $q > 2$, it is shown in [16, Lemma 7] that a symmetric trilinear map Φ over $\mathbb{F}_q$ always admits a symmetric algorithm, while in the remaining case $t = 3$ and $q = 2$, as observed by Cascudo, a necessary condition is that Φ should satisfy $\Phi(x, x, y) = \Phi(x, y, y)$ for all entries x, y. These results were then combined and generalized into the following necessary and sufficient criterion:

Theorem 1 ([14, Thm. A.7]). *Let $\Phi : V^t \to W$ be a t-multilinear map between finite dimensional vector spaces over $\mathbb{F}_q$. Then Φ admits a symmetric decomposition if and only if Φ is* Frobenius-symmetric*, i.e. if and only if it is symmetric and one of the following two conditions holds:*

- $t \leq q$
- $t \geq q + 1$ *and for all $u, v, z_1, \ldots, z_{t-q-1}$ in V,*

$$\Phi(\underbrace{u, \ldots, u}_{q \text{ times}}, v, z_1, \ldots, z_{t-q-1}) = \Phi(u, \underbrace{v, \ldots, v}_{q \text{ times}}, z_1, \ldots, z_{t-q-1}).$$

Observe that this criterion involves the *cardinality* of the field, not its characteristic.

Trisymmetric and hypersymmetric complexity. Now suppose furthermore that $V = W$, and that this space is equipped with a non-degenerate symmetric bilinear form, written as a scalar product

$$\begin{aligned} V \times V &\to \mathbf{k} \\ (v, w) &\mapsto \langle v, w \rangle . \end{aligned}$$

This allows to identify V and $V^\vee$, *i.e.* any linear form $\varphi \in V^\vee$ is of the form $\varphi(x) = \langle a, x \rangle$ for a uniquely determined $a \in V$. As a consequence, a symmetric decomposition for $\Phi : V^t \to V$ can also be described as the data of elements $(a_i)_{1 \leq i \leq n}$ and $(b_i)_{1 \leq i \leq n}$ in V such that for all $v_1, \ldots, v_t$ in V, we have $\Phi(v_1, \ldots, v_t) = \sum_{i=1}^n \langle a_i, v_1 \rangle \cdots \langle a_i, v_t \rangle \, b_i$. In order to have an even more compact description, one could ask for b_i to be proportional to a_i, leading to the following:

Definition 1. *Let V be a finite dimensional $\mathbf{k}$-vector space equipped with a scalar product, and $\Phi : V^t \to V$ a symmetric t-multilinear map. Then a* hypersymmetric *formula for Φ is the data of elements $(a_i)_{1 \leq i \leq n}$ in V and scalars $(\lambda_i)_{1 \leq i \leq n}$ in $\mathbf{k}$ such that, for all $v_1, \ldots, v_t \in V$,*

$$\Phi(v_1, \ldots, v_t) = \sum_{i=1}^{n} \lambda_i \langle a_i, v_1 \rangle \cdots \langle a_i, v_t \rangle \, a_i.$$

The hypersymmetric complexity $\mu^{hyp}(\Phi)$ is then the minimal length n of such a hypersymmetric decomposition, if it exists. Obviously we always have $\mu^{sym}(\Phi) \leq \mu^{hyp}(\Phi)$.

When $t = 2$, we will say trisymmetric *for hypersymmetric, and write $\mu^{tri}(\Phi)$ for $\mu^{hyp}(\Phi)$.*

As a further motivation, observe that to any t-multilinear map $\Phi : V^t \to V$ one can associate a $(t+1)$-multilinear *form* $\widetilde{\Phi} : V^{t+1} \to \mathbf{k}$, defined by

$$\widetilde{\Phi}(v_1, \ldots, v_t, v_{t+1}) = \langle \Phi(v_1, \ldots, v_t), v_{t+1} \rangle .$$

We then say that Φ is hypersymmetric (as a t-multilinear map) if $\widetilde{\Phi}$ is symmetric (as a $(t+1)$-multilinear form). It is easily seen that Φ hypersymmetric is a necessary condition for it to admit a hypersymmetric decomposition, and more precisely:

Lemma 1. *Elements $(a_i)_{1\le i\le n}$ in V and scalars $(\lambda_i)_{1\le i\le n}$ in $\mathbf{k}$ define a hypersymmetric formula for the t-multilinear map Φ,*

$$\Phi(v_1,\dots,v_t)=\sum_{i=1}^{n}\lambda_i\,\langle a_i,v_1\rangle\cdots\langle a_i,v_t\rangle\,a_i,$$

if and only if they define a symmetric formula for the $(t+1)$-multilinear form $\widetilde{\Phi}$,

$$\widetilde{\Phi}(v_1,\dots,v_s,v_{t+1})=\sum_{i=1}^{n}\lambda_i\,\langle a_i,v_1\rangle\cdots\langle a_i,v_t\rangle\,\langle a_i,v_{t+1}\rangle\,.$$

Thus, Φ admits a hypersymmetric formula if and only if $\widetilde{\Phi}$ is Frobenius-symmetric (in the sense of Theorem 1), and we have

$$\mu^{hyp}(\Phi)=\mu^{sym}\left(\widetilde{\Phi}\right).$$

In particular, if $q\ge t+1$, then any hypersymmetric t-multilinear map over $\mathbb{F}_q$ admits a hypersymmetric formula.

Proof. For the *only if* part in the first assertion, take scalar product with v_{t+1}. For the *if* part, use the fact that the scalar product is non-degenerate. The other assertions follow. □

Galois invariance. Last we consider another type of symmetry. Let $\sigma : v\mapsto v^\sigma$ be a $\mathbf{k}$-linear automorphism of V that respects the scalar product: $\langle v^\sigma,w^\sigma\rangle=\langle v,w\rangle$ for all v,w in V.

Lemma 2. *Let $\Phi : V^t\to V$ be a symmetric t-multilinear map that is compatible with σ,* i.e.

$$\Phi(v_1^\sigma,\dots,v_t^\sigma)=\Phi(v_1,\dots,v_t)^\sigma$$

for all $v_1,\dots,v_t$ in V, and let $(a_i)_{1\le i\le n}$ and $(b_i)_{1\le i\le n}$ in V define a symmetric formula for Φ,

$$\Phi(v_1,\dots,v_t)=\sum_{i=1}^{n}\langle a_i,v_1\rangle\cdots\langle a_i,v_t\rangle\,b_i.$$

Then $(a_i^\sigma)_{1\le i\le n}$ and $(b_i^\sigma)_{1\le i\le n}$ also define a symmetric formula for Φ,

$$\Phi(v_1,\dots,v_t)=\sum_{i=1}^{n}\langle a_i^\sigma,v_1\rangle\cdots\langle a_i^\sigma,v_t\rangle\,b_i^\sigma.$$

Proof. Write $\Phi(v_1,\dots,v_t)=\Phi(v_1^{\sigma^{-1}},\dots,v_t^{\sigma^{-1}})^\sigma$ and apply the formula. □

We then say that the symmetric formula given by $(a_i)_{1\le i\le n}$ and $(b_i)_{1\le i\le n}$ is σ-invariant if it is the same as the formula given by $(a_i^\sigma)_{1\le i\le n}$ and $(b_i^\sigma)_{1\le i\le n}$, *i.e.* if there is a permutation π of $\{1,\dots,n\}$ such that $(a_i^\sigma,b_i^\sigma)=(a_{\pi(i)},b_{\pi(i)})$ for all i. This applies also to hypersymmetric formulae, setting $b_i=\lambda_i a_i$.

If G is a group of $\mathbf{k}$-linear automorphisms of V that respect the scalar product, and if $\Phi : V^t\to V$ is a symmetric t-multilinear map that is compatible with all elements in G, we then define $\mu^{\mathrm{sym},G}(\Phi)$ (resp. $\mu^{\mathrm{hyp},G}(\Phi)$), the *$G$-invariant* symmetric (resp. hypersymmetric) multilinear complexity of Φ, as the minimal length n of a symmetric (resp. hypersymmetric) multilinear formula for Φ that is G-invariant, *i.e.* σ-invariant for all σ in G.

Multiplication formulae in algebras. Let $\mathcal{A}$ be a finite dimensional commutative algebra over $\mathbf{k}$. We say a linear form $\tau : \mathcal{A} \to \mathbf{k}$ is trace-like if the symmetric bilinear form $\mathcal{A} \times \mathcal{A} \to \mathbf{k}$, $(x, y) \mapsto \tau(xy)$ is non-degenerate. If so, we set $\langle x, y\rangle = \tau(xy)$, which defines a scalar product on $\mathcal{A}$. In this work we will take $\mathbf{k} = \mathbb{F}_q$, and either:

- $\mathcal{A} = \mathbb{F}_{q^k}$ a finite field extension, and $\tau = \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ the usual trace map; indeed it is well known that the trace bilinear form $\langle x, y\rangle = \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(xy)$ is non-degenerate
- $\mathcal{A} = \mathbb{F}_q[T]/(T^k)$ an algebra of truncated polynomials, and τ defined by $\tau(x) = x_{k-1}$ for $x = x_0 + x_1T + \cdots + x_{k-1}T^{k-1}$ in $\mathcal{A}$; indeed, observe that for $x = x_0 + x_1T + \cdots + x_{k-1}T^{k-1}$, $y = y_0 + y_1T + \cdots + y_{k-1}T^{k-1}$, we then have $\langle x, y\rangle = \tau(xy) = x_0y_{k-1} + x_1y_{k-2} + \cdots + x_{k-1}y_0$, which is non-degenerate.

Let $\Phi : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ be the multiplication map, $\Phi(x, y) = xy$. It is easily seen that Φ is trisymmetric. Indeed $\widetilde{\Phi}$ is the trilinear form $x, y, z \mapsto \tau(xyz)$, which is symmetric. A symmetric bilinear multiplication formula for $\mathcal{A}$ is thus the data of $(a_i)_{1\le i\le n}$ in $\mathcal{A}$ and $(\varphi_i)_{1\le i\le n}$ in $\mathcal{A}^\vee$ such that

$$\forall x, y \in \mathcal{A},\ xy = \sum_{i=1}^{n} \varphi_i(x)\varphi_i(y)a_i, \tag{1}$$

and a trisymmetric formula is the data of $(a_i)_{1\le i\le n}$ in $\mathcal{A}$ and $(\lambda_i)_{1\le i\le n}$ in $\mathbb{F}_q$ such that

$$\forall x, y \in \mathcal{A},\ xy = \sum_{i=1}^{n} \lambda_i \langle a_i, x\rangle \langle a_i, y\rangle a_i. \tag{2}$$

We will write $\mu_q(k)$ (resp. $\hat{\mu}_q(k)$) for the bilinear complexity of multiplication in $\mathbb{F}_{q^k}$ (resp. in $\mathbb{F}_q[T]/(T^k)$) over $\mathbb{F}_q$, and we will write likewise $\mu_q^{\mathrm{sym}}(k)$, $\hat{\mu}_q^{\mathrm{sym}}(k)$, $\mu_q^{\mathrm{tri}}(k)$, $\hat{\mu}_q^{\mathrm{tri}}(k)$, $\mu_q^{\mathrm{sym},G}(k)$, $\hat{\mu}_q^{\mathrm{sym},G}(k)$, $\mu_q^{\mathrm{tri},G}(k)$, $\hat{\mu}_q^{\mathrm{tri},G}(k)$, etc. for the similar quantities with the corresponding symmetry conditions.

For $q \ge 3$ we have $\mu_q^{\mathrm{tri}}(k) < \infty$ and $\hat{\mu}_q^{\mathrm{tri}}(k) < \infty$ for all k, while for $q = 2$ we have $\mu_2^{\mathrm{tri}}(1) = \hat{\mu}_2^{\mathrm{tri}}(1) = 1$ and $\mu_2^{\mathrm{tri}}(2) = 3$, but $\mu_2^{\mathrm{tri}}(k) = \infty$ for $k \ge 3$ and $\hat{\mu}_2^{\mathrm{tri}}(k) = \infty$ for $k \ge 2$. This follows essentially from Theorem 1 and Lemma 1 (see also [14, Prop. A.14]).

Obviously we have $\mu_q(k) \le \mu_q^{\mathrm{sym}}(k) \le \mu_q^{\mathrm{tri}}(k)$ and $\hat{\mu}_q(k) \le \hat{\mu}_q^{\mathrm{sym}}(k) \le \hat{\mu}_q^{\mathrm{tri}}(k)$ for all q and k. But when all these quantities are finite, e.g. when $q \ge 3$, no example of strict inequality is known.

In the other direction, when $q \ge 4$ is not divisible by 3, [16, Thm. 2] gives $\mu_q^{\mathrm{tri}}(k) \le 4\mu_q^{\mathrm{sym}}(k)$ and $\hat{\mu}_q^{\mathrm{tri}}(k) \le 4\hat{\mu}_q^{\mathrm{sym}}(k)$. This allows to translate the many known upper bounds on symmetric complexity [2] into upper bounds on trisymmetric complexity. However the resulting upper bounds do not seem to be tight, so it would be desirable to have better estimates, and especially upper bounds that work also for q divisible by 3.

3 Finding trisymmetric decompositions

Algorithmic search. Barbulescu *et al.* [5] and later Covanov [10] found clever ways of exhaustively searching for formulae for (symmetric) bilinear maps. Their method eliminates redundancy in the search but strongly relies on the fact that the vectors $a_i \in \mathcal{A}$ in the symmetric formulae (1) can be chosen independently of the linear forms $\varphi_i \in \mathcal{A}^\vee$, which is no longer the case when searching for trisymmetric decompositions. For this reason, we use another method that

is once again a variant of an exhaustive search and thus still leads to an exponential complexity algorithm. Let Φ be the two-variable product in $\mathcal{A}$. Recall that we are looking for a trisymmetric decomposition:

$$\forall x, y \in \mathcal{A},\, \Phi(x, y) = xy = \sum_{i=1}^{n} \lambda_i \langle x, a_i \rangle \langle y, a_i \rangle a_i,$$

with $a_i \in \mathcal{A}$ and $\lambda_i \in \mathbf{k}$ for all $1 \leq i \leq n$. Because we are allowed to use scalars $\lambda_i \in \mathbf{k}$, we can limit our search to "normalized" elements in $\mathcal{A}$, as follows. Choose a basis of $\mathcal{A}$, which gives an identification $\mathcal{A} \simeq \mathbf{k}^k$ as vector spaces. Then for all $1 \leq i \leq k$, let

$$\mathcal{E}_i = \left\{ x = (x_1, \ldots, x_k) \in \mathcal{A} \simeq \mathbf{k}^k \,|\, \forall j \leq i-1,\, x_j = 0 \text{ and } x_i = 1 \right\}$$

and

$$\mathcal{E} = \bigcup_{i=1}^{k} \mathcal{E}_i.$$

We search for elements a_i in $\mathcal{E}$ instead of $\mathcal{A}$. We further use the vector space structure of $\mathcal{A}$ by searching for solutions on each coordinate. Let

$$xy = (\pi_1(x, y), \ldots, \pi_k(x, y)) \in \mathcal{A} \simeq \mathbf{k}^k,$$

where, for all $1 \leq i \leq k$, π_i is the bilinear form corresponding to the i-th coordinate of the product in $\mathbb{F}_{p^k}$. In other words,

$$\Phi = (\pi_1, \ldots, \pi_k).$$

We let $\mathcal{B}$ be the space of bilinear forms on $\mathcal{A}$ and we let f be the application mapping an element in $\mathcal{A}$ to its associated bilinear symmetric form:

$$\begin{array}{rccc} f : \mathcal{A} \to & & & \mathcal{B} \\ a & \mapsto (x, y) & \mapsto & \langle x, a \rangle \langle y, a \rangle . \end{array}$$

We then search for elements $a_1, \ldots, a_{n_1}$ in $\mathcal{E}_1$ and $\lambda_1, \ldots, \lambda_{n_1}$ in $\mathbf{k}$ such that

$$\pi_1 = \sum_{j=1}^{n_1} \lambda_j f(a_j), \tag{3}$$

and we obtain

$$\Phi - \sum_{j=1}^{n_1} \lambda_j f(a_j) a_j = (0, \pi_2', \ldots, \pi_k'),$$

where for $2 \leq i \leq k$, π_i' is some other bilinear form. We then continue the operation with π_2' and elements $a_{n_1+1}, \ldots, a_{n_2}$ in $\mathcal{E}_2$, then with π_3'' and elements in $\mathcal{E}_3$, and so on. In the end, we have n elements $a_1, \ldots, a_n \in \mathcal{E}$ and $\lambda_1, \ldots, \lambda_n \in \mathbf{k}$ such that

$$\Phi = \sum_{j=1}^{n} \lambda_j f(a_j) a_j.$$

Now, there is left to see how we compute the elements $a_1, \ldots, a_{n_1} \in \mathcal{E}_1$ and $\lambda_1, \ldots, \lambda_{n_1} \in \mathbf{k}$ in order to obtain (3). Let r_1 be the rank of π_1. We know that the number n_1 of elements in $\mathcal{E}_1$ such that we have (3) is at least r_1, but there also exist some trisymmetric decompositions where we

need more than r_1 elements. To find these elements, we search through elements $a_1 \in \mathcal{E}_1$ such that there exists $\lambda_1 \in \mathbf{k}$ with

$$\operatorname{rank}(\pi_1 - \lambda_1 f(a_1)) < \operatorname{rank}(\pi_1),$$

then, for each such $a_1 \in \mathcal{E}_1$, we search through elements $a_2 \in \mathcal{E}_1$ such that there exists λ_2 with

$$\operatorname{rank}(\pi_1 - \lambda_1 f(a_1) - \lambda_2 f(a_2)) < \operatorname{rank}(\pi_1 - \lambda_1 f(a_1)),$$

and so on, eliminating a lot of unsuitable elements along the way. This method allows us to find decompositions of π_1 into a sum of exactly r_1 bilinear forms of rank 1. In order to find decompositions containing $r_1 + m_1$ bilinear forms, we repeat the same process, except that we allow the rank not to decrease m_1 times. Let m_j be the number of times we allow the rank not to decrease when dealing with the j-th coordinate in the algorithm. We let $\mathcal{M} = (m_1, \ldots, m_k)$ and we call *margin* this k-tuple. This strategy was implemented in the Julia programming language [1] and a package searching for trisymmetric decompositions is available online[4], along with the source code.

This allowed us to compute $\mu_3^{\text{tri}}(3) = 6$, $\mu_p^{\text{tri}}(3) = 5$ for all primes $5 \leq p \leq 257$, $\mu_3^{\text{tri}}(4) = 9$, $\mu_5^{\text{tri}}(4) = 8$, and $\mu_p^{\text{tri}}(4) = 7$ for all primes $7 \leq p \leq 23$. Details about the computation can be found in Table 1, while examples of formulae obtained via our algorithm are given in Table 2 (actually the formulae in this table are *normalized* in the sense of [14, Def. A.16], *i.e.* they satisfy all $\lambda_i = 1$).

Field	Margin	Solutions	Length	Time (s)	Field	Margin	Solutions	Length	Time (s)
$\mathbb{F}_{3^2}$	$(0,0)$	1	3	$1.8 \cdot 10^{-4}$	$\mathbb{F}_{7^3}$	$(0,0,0)$	8	5	$7.0 \cdot 10^{-3}$
$\mathbb{F}_{3^3}$	$(0,0,0)$	1	6	$4.4 \cdot 10^{-4}$	$\mathbb{F}_{13^3}$	$(0,0,0)$	100	5	$2.9 \cdot 10^{-1}$
$\mathbb{F}_{3^4}$	$(0,0,0,0)$	2	9	$5.3 \cdot 10^{-3}$	$\mathbb{F}_{19^3}$	$(0,0,0)$	415	5	1.8
$\mathbb{F}_{3^4}$	$(2,1,0,0)$	18	9	$3.8 \cdot 10^{-1}$	$\mathbb{F}_{31^3}$	$(0,0,0)$	2031	5	29
$\mathbb{F}_{3^4}$	$(3,2,1,1)$	25	9	1.1	$\mathbb{F}_{47^3}$	$(0,0,0)$	7590	5	360

Table 1. Algorithmic results with various degrees, base fields and margins.

Galois invariant formulae. Let $\mathcal{A} = \mathbb{F}_{q^k}$ and G be the cyclic group generated by σ, the Frobenius automorphism over $\mathbb{F}_q$. In order to find G-invariant decompositions, we exhaustively search through orbits in $\mathbb{F}_{q^k}$, which is fast because the search space is smaller. This allows us to find Galois invariant trisymmetric formulae of length 11 for $\mathbb{F}_{3^5}$, and of length 10 for $\mathbb{F}_{5^5}$ and $\mathbb{F}_{7^5}$. Joint with the obvious inequalities $\mu_q(k) \leq \mu_q^{\text{sym}}(k) \leq \mu_q^{\text{tri}}(k) \leq \mu_q^{\text{tri},G}(k)$ and with known lower bounds from [2, Thm. 2.2] and [5], this gives $10 \leq \mu_3(5) \leq \mu_3^{\text{sym}}(5) = \mu_3^{\text{tri}}(5) = \mu_3^{\text{tri},G}(5) = 11$, $\mu_5(5) = \mu_5^{\text{sym}}(5) = \mu_5^{\text{tri}}(5) = \mu_5^{\text{tri},G}(5) = 10$, and $\mu_7(5) = \mu_7^{\text{sym}}(5) = \mu_7^{\text{tri}}(5) = \mu_7^{\text{tri},G}(5) = 10$. Some examples of Galois invariant formulae can be found in Table 2.

For $q \geq 3$ we know no example where one of the inequalities in $\mu_q(k) \leq \mu_q^{\text{sym}}(k) \leq \mu_q^{\text{tri}}(k)$ is strict. However, it turns out that the inequality with $\mu_q^{\text{tri},G}(k)$ can be strict. Indeed, let $q = 3$ and $k = 7$. In this setting our exhaustive search found no G-invariant decomposition of length up to 15. Since all orbits are of length 7, except the trivial orbit of length 1, the minimal length for a G-invariant decomposition is congruent to 0 or 1 modulo 7, so we deduce that it is at least 21. Furthermore, we know [2, table 2] that $\mu_3^{\text{sym}}(7) \leq 19$, so we have

$$\mu_3(7) \leq \mu_3^{\text{sym}}(7) \leq 19 < 21 \leq \mu_3^{\text{tri},G}(7).$$

Field	n	Field elements $a_1, \ldots, a_n$ such that $xy = \sum_{i=1}^{n} \langle a_i, x\rangle \langle a_i, y\rangle a_i$
$\mathbb{F}_{3^3} = \mathbb{F}_3[\alpha]/(\alpha^3-\alpha+1)$	6	$a_1 = \alpha$, $a_2 = a_1^\sigma$, $a_3 = a_2^\sigma$, $a_4 = 1-\alpha^2$, $a_5 = a_4^\sigma$, $a_6 = a_5^\sigma$
$\mathbb{F}_{3^4} = \mathbb{F}_3[\alpha]/(\alpha^4-\alpha^3-1)$	9	$a_1 = -1$, $a_2 = -\alpha$, $a_3 = a_2^\sigma$, $a_4 = a_3^\sigma$, $a_5 = a_4^\sigma$, $a_6 = \alpha^2+\alpha+1$, $a_7 = a_6^\sigma$, $a_8 = a_7^\sigma$, $a_9 = a_8^\sigma$
$\mathbb{F}_{3^5} = \mathbb{F}_3[\alpha]/(\alpha^5-\alpha+1)$	11	$a_1 = 1$, $a_2 = \alpha-1$, $a_3 = a_2^\sigma$, $a_4 = a_3^\sigma$, $a_5 = a_4^\sigma$, $a_6 = a_5^\sigma$, $a_7 = 1-\alpha-\alpha^2$, $a_8 = a_7^\sigma$, $a_9 = a_8^\sigma$, $a_{10} = a_9^\sigma$, $a_{11} = a_{10}^\sigma$
$\mathbb{F}_{5^3} = \mathbb{F}_5[\alpha]/(\alpha^3+3\alpha+3)$	5	$a_1 = 3\alpha+2$, $a_2 = -\alpha^2-\alpha-1$, $a_3 = 3\alpha^2+2\alpha+2$, $a_4 = -\alpha$, $a_5 = 3\alpha^2+2\alpha$
$\mathbb{F}_{5^4} = \mathbb{F}_5[\alpha]/(\alpha^4-\alpha^2-\alpha+2)$	8	$a_1 = -1$, $a_2 = 3\alpha^2+3\alpha+3$, $a_3 = 3\alpha^3-\alpha^2+2\alpha-1$, $a_4 = 2\alpha^3-\alpha^2-\alpha+1$, $a_5 = \alpha$, $a_6 = -\alpha^2+\alpha$, $a_7 = \alpha^3+\alpha^2+\alpha$, $a_8 = \alpha^3+\alpha^2$

Table 2. Examples of trisymmetric multiplication formulae (the first three are Galois invariant).

Universal formulae. As mentioned in Section 2, for $q \geq 3$, we do not know any example of algebra $\mathcal{A} = \mathbb{F}_{q^k}$ or $\mathcal{A} = \mathbb{F}_q[T]/(T^k)$ where the bilinear complexity and the trisymmetric bilinear complexity are different. We can even prove that these quantities are the same in small dimension, by exhibiting trisymmetric *universal formulae*, *i.e.* trisymmetric decompositions that are true for (almost) any choice of $q \geq 3$. In order to obtain such formulae, it is useful to change our point of view on the problem. Assume we want to compute a trisymmetric decomposition of the product Φ in $\mathcal{A}$, a commutative algebra of degree k. After the choice of a basis of $\mathcal{A}$ and a basis of the space $\mathcal{B}$ of the bilinear forms on $\mathcal{A}$, we can represent

$$\Phi = (\pi_1, \ldots, \pi_k)$$

as a column vector B of length k^3. The first k^2 coordinates corresponding to π_1, the next k^2 coordinates corresponding to π_2 and so on up to π_k. Now, for each $a \in \mathcal{E}$, we note

$$\mathbf{f}(a) = a \otimes f(a),$$

where a is the column vector of length k corresponding to a in the basis of $\mathcal{A}$, $f(a)$ is the column vector of length k^2 corresponding to $f(a) \in \mathcal{B}$, and $\otimes$ is the Kronecker product. With these notations, finding a trisymmetric decomposition of the product in $\mathcal{A}$ is the same as finding elements $a_1 \ldots, a_n \in \mathcal{E}$ and $\lambda_1, \ldots, \lambda_n \in \mathbf{k}$ with

$$B = \sum_{j=1}^{n} \lambda_j \mathbf{f}(a).$$

Let A be the matrix which columns are the $\mathbf{f}(a)$ for all $a \in \mathcal{E}$, then the problem is to find a solution X of

$$AX = B$$

with the smallest possible number of nonzero entries in X.

We first consider the case $\mathcal{A} = \mathbb{F}_{q^2}$ over $\mathbf{k} = \mathbb{F}_q$, where the characteristic of $\mathbf{k}$ is not 2.

Proposition 1. *For any odd q we have*

$$\mu_q(2) = \mu_q^{tri}(2) = 3.$$

Proof. That $\mu_q(2) = 3$ follows e.g. from [2, Thm. 2.2]. In order to prove that $\mu_q^{\text{tri}}(2) = 3$, we find an *universal* trisymmetric formula of length 3. We know that we can find a non-square element ζ in $\mathbb{F}_q$, we can then define

$$\mathbb{F}_{q^2} \cong \mathbb{F}_q[T]/(T^2 - \zeta) = \mathbb{F}_q(\alpha),$$

[4] https://github.com/erou/TriSym.jl

where $\alpha = \bar{T}$ is the canonical generator of $\mathbb{F}_{q^2}$. Let $x = x_0 + x_1\alpha$ and $y = y_0 + y_1\alpha$ be two elements of $\mathbb{F}_{q^2}$, we have

$$xy = (x_0 + x_1\alpha)(y_0 + y_1\alpha) = x_0y_0 + \zeta x_1y_1 + (x_0y_1 + x_1y_0)\alpha.$$

We can lift the matrix B coming from the multiplication formula, that has coefficients in $\mathbb{F}_q$, to a matrix with coefficients in $\mathbb{Q}(\zeta)$, where ζ is an indeterminate. We can also lift the matrix A, because the map f (and therefore $\mathbf{f}$) has the same expression for all q not divisible by 2. Indeed, one can check that the map f is given by

$$f(x_0 + x_1\alpha) = \left(S\begin{bmatrix}x_0\\x_1\end{bmatrix}\right)\left(S\begin{bmatrix}x_0\\x_1\end{bmatrix}\right)^{\mathsf{T}} = 4\begin{bmatrix}x_0^2 & \zeta x_0x_1\\ \zeta x_0x_1 & \zeta^2x_1^2\end{bmatrix}.$$

where

$$S = \left[\langle \alpha^i, \alpha^j\rangle\right]_{0\le i,j\le 1} = \left[\mathrm{Tr}(\alpha^{i+j})\right]_{0\le i,j\le 1} = \begin{bmatrix}2 & 0\\ 0 & 2\zeta\end{bmatrix}.$$

We can then solve $AX = B$ over $\mathbb{Q}(\zeta)$ and finally check that

$$B = (1-\zeta^{-1})4^{-1}\mathbf{f}(1) + (8\zeta)^{-1}\mathbf{f}(1+\alpha) + (8\zeta)^{-1}\mathbf{f}(1-\alpha),$$

so that the trisymmetric bilinear complexity of $\mathbb{F}_{q^2}/\mathbb{F}_q$ is 3. □

Using the same strategy, we can also find universal formulae for another type of algebra $\mathcal{A} = \mathbb{F}_q[T]/(T^k)$, namely the truncated polynomials. In that context, we first observe that we have

$$\hat{\mu}_q^{\mathrm{tri}}(k) \ge \hat{\mu}_q(k) \ge 2k-1$$

for all q and k. Indeed this is a special case of [21, Thm. 4], which holds for any polynomial that is a power of an irreducible polynomial. Conversely we are able to find formulae for $2 \le k \le 4$ that match this lower bound.

Proposition 2. *For any odd q we have*

$$\hat{\mu}_q^{tri}(2) = 3.$$

Proof. Let $\mathcal{A} = \mathbb{F}_q[T]/(T^2) = \mathbb{F}_q[\alpha]$ with $\alpha = \bar{T}$, so $\alpha^2 = 0$. If $x = x_0 + x_1\alpha$ and $y = y_0 + y_1\alpha$ are two elements of $\mathcal{A}$, we have

$$xy = (x_0 + x_1\alpha)(y_0 + y_1\alpha) = x_0y_0 + (x_0y_1 + x_1y_0)\alpha.$$

We can again construct the matrix B and A, and solve $AX = B$, this time simply over $\mathbb{Q}$. We obtain

$$B = -\mathbf{f}(1) + 2^{-1}\mathbf{f}(1+\alpha) + 2^{-1}\mathbf{f}(1-\alpha)$$

so that the trisymmetric bilinear complexity of $\mathcal{A} = \mathbb{F}_q[T]/(T^2)$ is at least 3, which concludes. □

Proposition 3. *For any q not divisible by 2 nor 3 we have*

$$\hat{\mu}_q^{tri}(3) = 5 \qquad \textit{and} \qquad \hat{\mu}_q^{tri}(4) = 7.$$

Proof. We use the same notations as before. For $\mathcal{A} = \mathbb{F}_q[T]/(T^3)$, we obtain

$$B = -\mathbf{f}(1-\alpha-\alpha^2) + 3^{-1}\mathbf{f}(\alpha+2\alpha^2) + 2^{-1}\mathbf{f}(1-\alpha-2\alpha^2) - 3^{-1}\mathbf{f}(\alpha-\alpha^2) + 2^{-1}\mathbf{f}(1-\alpha).$$

Therefore the trisymmetric bilinear complexity of $\mathcal{A} = \mathbb{F}_q[T]/(T^3)$ is 5.

Finally, for $\mathcal{A} = \mathbb{F}_q[T]/(T^4)$, we obtain

$$\begin{aligned}B = \;& 2^{-1}\mathbf{f}(1-\alpha^2+\alpha^3) - \mathbf{f}(1-\alpha^2) + 12^{-1}\mathbf{f}(\alpha+2\alpha^2+2\alpha^3) - 12^{-1}\mathbf{f}(\alpha-2\alpha^2+2\alpha^3)\\ & - 6^{-1}\mathbf{f}(\alpha+\alpha^2-\alpha^3) + 6^{-1}\mathbf{f}(\alpha-\alpha^2-\alpha^3) + 2^{-1}\mathbf{f}(1-\alpha^2-\alpha^3)\cdot(1-\alpha^2-\alpha^3).\end{aligned}$$

The trisymmetric bilinear complexity of $\mathcal{A} = \mathbb{F}_q[T]/(T^4)$ is then 7. □

4 Asymptotic bounds

In this section, we work with $\mathcal{A} = \mathbb{F}_{q^k}$ or $\mathbb{F}_q[T]/(T^k)$, seen as an algebra over $\mathbf{k} = \mathbb{F}_q$, and equipped with the trace-like linear form τ introduced at the end of Section 2. Our aim is to show that the trisymmetric bilinear complexities $\mu_q^{\mathrm{tri}}(k)$ and $\hat{\mu}_q^{\mathrm{tri}}(k)$ grow linearly as $k \to \infty$. Our proof will involve higher multilinear maps, and in turn, give results for them as well.

For any t we define the t-multilinear multiplication map in $\mathcal{A}$ over $\mathbf{k}$

$$\begin{array}{rccc} m_t : & \mathcal{A}^t & \to & \mathcal{A} \\ & (x_1, \ldots, x_t) & \mapsto & x_1 \cdots x_t \end{array}$$

and the t-multilinear trace form

$$\begin{array}{rccc} \tau_t = \tau \circ m_t : & \mathcal{A}^t & \to & \mathcal{A} \\ & (x_1, \ldots, x_t) & \mapsto & \tau(x_1 \cdots x_t). \end{array}$$

If needed, we will write ${m_t}^{\mathcal{A}/\mathbf{k}}$ or ${\tau_t}^{\mathcal{A}/\mathbf{k}}$ to keep $\mathcal{A}$ and $\mathbf{k}$ explicit.

The (symmetric) multilinear complexity of m_t has been considered in [7] in relation with the theory of testers.

Lemma 3. *The map m_t is hypersymmetric, and we have*

$$\mu^{hyp}(m_t) = \mu^{sym}(\tau_{t+1}) \leq \mu^{sym}(m_{t+1}).$$

Proof. Indeed we have $\widetilde{m}_t = \tau_{t+1}$, and the equality on the left is a special case of Lemma 1. For the inequality on the right, take a symmetric formula for m_{t+1} and apply τ. □

When studying the variation with the degree of the extension field $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, we will write $\mu_q^{\mathrm{sym}}(k, m_t)$ for $\mu^{\mathrm{sym}}\left({m_t}^{\mathbb{F}_{q^k}/\mathbb{F}_q}\right)$, and we will also use the similar notations $\mu_q^{\mathrm{hyp}}(k, m_t)$, $\mu_q^{\mathrm{sym}}(k, \tau_t)$, etc. In particular for $t = 2$ we have

$$\mu_q^{\mathrm{tri}}(k) = \mu_q^{\mathrm{tri}}(k, m_2) = \mu_q^{\mathrm{sym}}(k, \tau_3).$$

When working in $\mathbb{F}_q[T]/(T^k)$ over $\mathbb{F}_q$, we will write likewise $\hat{\mu}_q^{\mathrm{sym}}(k, m_t)$, $\hat{\mu}_q^{\mathrm{hyp}}(k, m_t)$, etc.

Our aim is, for fixed q and t with $q \geq t + 1$, to show that $\mu_q^{\mathrm{hyp}}(k, m_t)$ and $\hat{\mu}_q^{\mathrm{hyp}}(k, m_t)$ grow linearly with $k \to \infty$. Thanks to Lemma 3, it suffices to show that $\mu_q^{\mathrm{sym}}(k, m_{t+1})$ and $\hat{\mu}_q^{\mathrm{sym}}(k, m_{t+1})$ grow linearly with $k \to \infty$. To ease notations we will set

$$M_{q,t}^{\mathrm{sym}} = \limsup_{k\to\infty} \frac{1}{k} \mu_q^{\mathrm{sym}}(k, m_t), \qquad M_{q,t}^{\mathrm{hyp}} = \limsup_{k\to\infty} \frac{1}{k} \mu_q^{\mathrm{hyp}}(k, m_t),$$
$$M_q^{\mathrm{tri}} = \limsup_{k\to\infty} \frac{1}{k} \mu_q^{\mathrm{tri}}(k) = M_{q,2}^{\mathrm{hyp}},$$

and likewise for $\hat{M}_{q,t}^{\mathrm{sym}}$, $\hat{M}_{q,t}^{\mathrm{hyp}}$, $\hat{M}_q^{\mathrm{tri}}$, etc.

Evaluation-interpolation method. We use the function field terminology and notations presented in [18]. Let $F/\mathbb{F}_q$ be an algebraic function field of one variable over $\mathbb{F}_q$ and let $\mathbb{P}_F$ be the set of places of F. Let $\mathcal{D}_F$ the set of divisors on F, and if $D \in \mathcal{D}_F$ is a divisor on F, we denote by $L(D)$ its Riemann-Roch space and $\ell(D) = \dim L(D)$.

Proposition 4. *Assume there exist a place $Q \in \mathbb{P}_F$ of F of degree k, $P_1, \ldots, P_n \in \mathbb{P}_F$ places of F of degree 1, and a divisor $D \in \mathcal{D}_F$ of F such that the places Q and $P_1, \ldots, P_n$ are not in the support of D and such that the following conditions hold.*

(i) The evaluation map

$$\begin{aligned} \mathrm{ev}_{Q,D} : L(D) &\to \mathbb{F}_{q^k} \\ f &\mapsto f(Q) \end{aligned}$$

is surjective.

(ii) The evaluation map

$$\begin{aligned} \mathrm{ev}_{\mathcal{P},tD} : L(tD) &\to (\mathbb{F}_q)^n \\ h &\mapsto (h(P_1), \ldots, h(P_n)) \end{aligned}$$

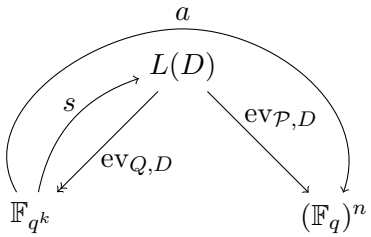
is injective.

Then $m_t^{\mathbb{F}_{q^k}/\mathbb{F}_q}$ *admits a symmetric formula of length* n, i.e. *we have* $\mu_q^{sym}(k, m_t) \leq n$.

Proof. Since the map $\mathrm{ev}_{Q,D}$ is surjective, it admits a right inverse, *i.e.* a linear map $s : \mathbb{F}_{q^k} \to L(D)$ such that $\mathrm{ev}_{Q,D} \circ s = \mathrm{Id}_{\mathbb{F}_{q^k}}$. For all $x \in \mathbb{F}_{q^k}$, we denote $s(x) \in L(D)$ by f_x, so the map $x \mapsto f_x$ is linear, and $f_x(Q) = x$. We also let

$$\begin{aligned} a : \mathbb{F}_{q^k} &\to (\mathbb{F}_q)^n \\ x &\mapsto (f_x(P_1), \ldots, f_x(P_n)) \end{aligned}$$

be the composite map $a = \mathrm{ev}_{\mathcal{P},D} \circ s$. The situation is sumed up in the following drawing.

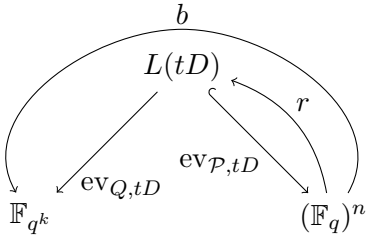


Observe that a is linear, so we can write

$$a(x) = (\varphi_1(x), \ldots, \varphi_n(x))$$

where $\varphi_i : \mathbb{F}_{q^k} \to \mathbb{F}_q$ is a linear form, namely $\varphi_i(x) = f_x(P_i)$.

Similarly, since the map $\mathrm{ev}_{\mathcal{P},tD}$ is injective, it admits a left inverse, *i.e.* a linear map $r : (\mathbb{F}_q)^n \to L(tD)$ such that $r \circ \mathrm{ev}_{\mathcal{P},tD} = \mathrm{Id}_{L(tD)}$. We also let $b : (\mathbb{F}_q)^n \to \mathbb{F}_{q^k}$ be the composite map $b = \mathrm{ev}_{Q,tD} \circ r$. The situation is sumed up in the following drawing.



The map b is linear, so there are $b_1, \ldots, b_n$ in $\mathbb{F}_{q^k}$ such that, for all $y = (y_1, \ldots, y_n) \in (\mathbb{F}_q)^n$,

$$b(y) = \sum_{i=1}^{n} y_i b_i.$$

Now for $x, \dots, x_t \in \mathbb{F}_{q^k}$, let

$$p = (p_1, \dots, p_n) = ((\prod_{j=1}^{t} f_{x_j})(P_1), \dots, (\prod_{j=1}^{t} f_{x_j})(P_n))$$

in $(\mathbb{F}_q)^n$ be the coordinatewise product of the vectors $a(x_1)$, ..., $a(x_t)$. Then

$$h = r(p)$$

is an element of $L(tD)$ such that $h(P_i) = p_i = (\prod_{j=1}^{t} f_{x_j})(P_i)$ for all i. Since the map $\mathrm{ev}_{\mathcal{P},tD}$ is injective, this forces

$$h = \prod_{j=1}^{t} f_{x_j}.$$

Then, we have

$$b(p) = \mathrm{ev}_{Q,tD}(r(p)) = \mathrm{ev}_{Q,tD}(h) = h(Q) = \prod_{j=1}^{t} f_{x_j}(Q) = \prod_{j=1}^{t} x_j.$$

But we also have

$$b(p) = \sum_{i=1}^{n} p_i b_i = \sum_{i=1}^{n} (\prod_{j=1}^{t} f_{x_j}(P_i)) b_i = \sum_{i=1}^{n} (\prod_{j=1}^{t} \varphi_i(x_j)) b_i$$

and finally we get a symmetric formula for m_t:

$$\prod_{j=1}^{t} x_j = \sum_{i=1}^{n} (\prod_{j=1}^{t} \varphi_i(x_j)) b_i.$$

□

Proposition 5. *Let $F/\mathbb{F}_q$ be an algebraic function field of genus g. Assume that F admits a place Q of degree k, and a set $\mathcal{S}$ of places of degree 1 of cardinality*

$$|\mathcal{S}| \geq (k + g - 1)t + 1.$$

Then we have

$$\mu_q^{sym}(k, m_t) \leq kt + (g-1)(t-1).$$

Proof. Set $n = kt + (g-1)(t-1)$. We will show that there are places $P_1, \dots, P_n$ in $\mathcal{S}$, and a divisor D on F, such that Proposition 4 applies, which gives $\mu_q^{\mathrm{sym}}(k, m_t) \leq n$ as desired.

Using e.g. [3, Lemma 2.1] we know F admits a non-special divisor R of degree $g-1$. By the strong approximation theorem [18, Thm. 1.6.5] we can then find a divisor D linearly equivalent to $R + Q$ and of support disjoint from Q and $\mathcal{S}$.

Then $D - Q$ and D are non-special, with $\ell(D - Q) = 0$ and $\ell(D) = k$. We thus find

$$\mathrm{Ker}(\mathrm{ev}_{Q,D} : L(D) \to \mathbb{F}_{q^k}) = L(D - Q) = 0,$$

so $\mathrm{ev}_{Q,D}$ is injective, hence also surjective by equality of dimensions, *i.e.* the surjectivity condition (i) in Proposition 4 is satisfied.

Likewise, tD is non-special, with $\deg(tD) = (k+g-1)t$ and $\ell(tD) = kt + (g-1)(t-1)$. Then the evaluation map

$$\begin{aligned} \mathrm{ev}_{\mathcal{S},tD} : L(tD) &\to (\mathbb{F}_q)^{|\mathcal{S}|} \\ h &\mapsto (h(P))_{P\in\mathcal{S}} \end{aligned}$$

has kernel $L(tD - \sum_{P\in\mathcal{S}} P) = 0$, because $\deg(tD - \sum_{P\in\mathcal{S}} P) = (k+g-1)t - |\mathcal{S}| < 0$. So $\mathrm{ev}_{\mathcal{S},tD}$ is injective, with image of dimension $\dim \mathrm{Im}(\mathrm{ev}_{\mathcal{S},tD}) = \ell(tD) = n$. Then we can find a subset $\mathcal{P} = \{P_1, \dots, P_n\} \subset \mathcal{S}$ of cardinality n, such that $\mathrm{ev}_{\mathcal{P},tD} : L(tD) \to (\mathbb{F}_q)^n$ is an isomorphism, and the injectivity condition (ii) in Proposition 4 is also satisfied. □

Choice of the curves for q a large enough square.

Proposition 6. *Let t be given, and assume q is a square, $q \geq (t+2)^2$. Then we have*

$$M_{q,t}^{sym} \leq (1 + \epsilon_t(q))t$$

with $\epsilon_t(q) = \frac{t-1}{\sqrt{q}-t-1}$.

Proof. We know [17] that there exists a family of function fields $F_i/\mathbb{F}_q$ of genus $g_i \to \infty$ such that

(i) $\frac{g_{i+1}}{g_i} \to 1$
(ii) $N_i \sim (\sqrt{q}-1)g_i$

where $N_i = \mathrm{Card}\,\{P \in \mathbb{P}_{F_i} \mid \deg P = 1\}$ is the number of places of degree 1 of F_i. We can also assume that the sequence g_i is increasing.

For any k let $i(k)$ be the smallest index such that

$$N_{i(k)} \geq (k + g_{i(k)} - 1)t + 1.$$

Such an $i(k)$ always exists since by (ii) we have $N_i \sim (\sqrt{q}-1)g_i$, with $\sqrt{q}-1 > t$.

By definition we thus have

$$N_{i(k)} \geq (k + g_{i(k)} - 1)t + 1 > (k + g_{i(k)-1} - 1)t + 1 > N_{i(k)-1}.$$

As $k \to \infty$ we have $i(k) \to \infty$, and by (i) we get $g_{i(k)} \sim g_{i(k)-1}$, so by (ii) we also get $N_{i(k)} \sim N_{i(k)-1}$. This then gives

$$\begin{aligned} N_{i(k)} &\sim (k + g_{i(k)} - 1)t + 1 \\ &\sim (k + g_{i(k)})t \end{aligned}$$

while by (ii),

$$N_{i(k)} \sim (\sqrt{q}-1)g_{i(k)}.$$

From these two relations we deduce

$$g_{i(k)} \sim \frac{t}{\sqrt{q}-1-t}k.$$

For k large enough this implies in particular $2g_{i(k)} + 1 \leq q^{(k-1)/2}(\sqrt{q}-1)$, so $F_{i(k)}$ admits a place of degree k by [18, Cor. 5.2.10].

From this we are allowed to apply Proposition 5 to $F_{i(k)}$, which gives

$$\mu_q^{\mathrm{sym}}(k, m_t) \;\leq\; kt + (g_{i(k)} - 1)(t-1) \;\sim\; kt + g_{i(k)}(t-1) \;\sim\; kt(1 + \epsilon_t(q))$$

as desired. □

Corollary 1. *For q a square, $q \geq (t+3)^2$ we have*

$$M_{q,t}^{hyp} \leq (1+\epsilon_{t+1}(q))(t+1),$$

and in particular we have

$$M_q^{tri} \leq 3\left(1+\frac{2}{\sqrt{q}-4}\right)$$

for q a square, $q \geq 25$.

Conclusion for arbitrary q.

Lemma 4. *Let q be a prime power. Then for any integers t, d, k we have*

$$\mu_q^{sym}(k, m_t) \leq \mu_q^{sym}(dk, m_t) \leq \mu_q^{sym}(d, m_t)\mu_{q^d}^{sym}(k, m_t).$$

Proof. For the inequality on the left, there is nothing to prove if $\mu_q^{\mathrm{sym}}(dk, m_t) = \infty$. So let us assume $m_t^{\mathbb{F}_{q^{dk}}/\mathbb{F}_q}$ admits a symmetric multiplication formula of length $n = \mu_q^{\mathrm{sym}}(dk, m_t)$, *i.e.*

$$\forall x_1, \ldots, x_t \in \mathbb{F}_{q^{dk}}, \quad x_1 \cdots x_t = \sum_{i=1}^{n} \varphi_i(x_1) \cdots \varphi_i(x_t) a_i$$

for linear forms $\varphi_i : \mathbb{F}_{q^{dk}} \to \mathbb{F}_q$ and elements $a_i \in \mathbb{F}_{q^{dk}}$. Choose a linear projection

$$p : \mathbb{F}_{q^{dk}} \to \mathbb{F}_{q^k}$$

left inverse for the inclusion $\mathbb{F}_{q^k} \subseteq \mathbb{F}_{q^{dk}}$. Then we get

$$\forall x_1, \ldots, x_t \in \mathbb{F}_{q^k}, \quad x_1 \cdots x_t = p(x_1, \ldots, x_t) = \sum_{i=1}^{n} \varphi_i(x_1) \cdots \varphi_i(x_t) p(a_i)$$

which is a symmetric multiplication formula of length n for $m_t^{\mathbb{F}_{q^k}/\mathbb{F}_q}$.

Likewise, for the inequality on the right, there is nothing to prove if $\mu_q^{\mathrm{sym}}(d, m_t) = \infty$ or $\mu_{q^d}^{\mathrm{sym}}(k, m_t) = \infty$. So let us assume $m_t^{\mathbb{F}_{q^d}/\mathbb{F}_q}$ and $m_t^{\mathbb{F}_{q^{dk}}/\mathbb{F}_{q^d}}$ admit symmetric multiplication formulae of length $r = \mu_q^{\mathrm{sym}}(d, m_t)$ and $s = \mu_{q^d}^{\mathrm{sym}}(k, m_t)$ respectively, so

$$\forall y_1, \ldots, y_t \in \mathbb{F}_{q^d}, \quad y_1 \cdots y_t = \sum_{u=1}^{r} \psi_u(y_1) \cdots \psi_u(y_t) b_u$$

$$\forall z_1, \ldots, z_t \in \mathbb{F}_{q^{dk}}, \quad z_1 \cdots z_t = \sum_{v=1}^{s} \chi_v(z_1) \cdots \chi_v(z_t) c_v$$

for linear forms $\psi_u : \mathbb{F}_{q^d} \to \mathbb{F}_q$, $\chi_v : \mathbb{F}_{q^{dk}} \to \mathbb{F}_{q^d}$ and elements $b_u \in \mathbb{F}_{q^d}$, $c_v \in \mathbb{F}_{q^{dk}}$. Then setting $y_1 = \chi_v(z_1)$, ..., $y_t = \chi_v(z_t)$ we find

$$\forall z_1, \ldots, z_t \in \mathbb{F}_{q^{dk}}, \quad z_1 \cdots z_t = \sum_{v=1}^{s} \sum_{u=1}^{r} (\psi_u \circ \chi_v)(z_1) \cdots (\psi_u \circ \chi_v)(z_t) \cdot (b_u c_v)$$

which is a symmetric multiplication formula of length rs for $m_t^{\mathbb{F}_{q^{dk}}/\mathbb{F}_q}$. □

Theorem 2. *Let $t \geq 2$ be an integer and q a prime power. If $q < t$, then $\mu_q^{sym}(k, m_t) = \infty$ for all $k \geq 2$.*

On the other hand, if $q \geq t$, then $\mu_q^{sym}(k, m_t)$ grows at most linearly with k, i.e. *we have*

$$M_{q,t}^{sym} \leq C_t(q)$$

for some real constant $C_t(q) < \infty$.

Proof. If $q < t$ and $k \geq 2$, then $\mu_q^{\mathrm{sym}}(k, m_t) = \infty$ follows from Theorem 1.

On the other hand, for $q \geq t$, we have $\mu_q^{\mathrm{sym}}(d, m_t) < \infty$ for any integer d. Choose d such that q^d is a square, $q^d \geq (t+2)^2$. Then Proposition 6 shows $\mu_{q^d}^{\mathrm{sym}}(k, m_t)$ grows linearly with k. The Theorem then follows thanks to Lemma 4, with $C_t(q) = \mu_q^{\mathrm{sym}}(d, m_t)(1 + \epsilon_t(q^d))t$. □

Corollary 2. *For $q \geq t+1$ we have*

$$M_{q,t}^{hyp} \leq C_{t+1}(q)$$

and in particular for $q \geq 3$ we have

$$M_q^{tri} \leq C_3(q).$$

Further remarks and possible improvements.

1. When $q \geq 4$ is not divisible by 3, [16, Thm. 2] gives $\mu_q^{\mathrm{tri}}(k) \leq 4\mu_q^{\mathrm{sym}}(k)$. On the other hand, [9] shows that $\mu_q^{\mathrm{sym}}(k)$ grows linearly with k (the result is stated for $\mu_q(k)$, but it is easily seen that the proof works for $\mu_q^{\mathrm{sym}}(k)$). Taken together, these results show that $\mu_q^{\mathrm{tri}}(k)$ grows linearly with k when $q \geq 4$ is not divisible by 3. One advantage of our method is that it works for all $q \geq 3$. Moreover it gives sharper bounds. For instance, when q is a square and large enough, joining [16, Thm. 2] with the best asymptotic upper bound known on $\mu_q^{\mathrm{sym}}(k)$ [12, Thm. 6.4] gives $M_q^{\mathrm{tri}} \leq 8\left(1 + \frac{1}{\sqrt{q}-2}\right)$, which is not as good as $M_q^{\mathrm{tri}} \leq 3\left(1 + \frac{2}{\sqrt{q}-4}\right)$ from Corollary 1.
2. *Open question*: Lemma 3 reduces (upper) bounds on $\mu^{\mathrm{hyp}}(m_t)$ to bounds on $\mu^{\mathrm{sym}}(m_{t+1})$, and in particular it reduces bounds on M_q^{tri} to bounds on $M_{q,3}^{\mathrm{hyp}}$, which does not seem optimal. Indeed we know no example where the inequality $\mu_q^{\mathrm{sym}}(k) \leq \mu_q^{\mathrm{tri}}(k)$ is strict. So, for instance for q square, $q \to \infty$, our method gives $M_q^{\mathrm{tri}} \leq 3(1 + o(1))$, but one could ask whether it is possible to get a bound of the form $M_q^{\mathrm{tri}} \leq 2(1 + o(1))$, as given by [12, Thm. 6.4] for M_q^{sym}.
3. *Open question*: The condition $|\mathcal{S}| \geq (k + g - 1)t + 1$ in Proposition 5 does not seem optimal since in the end we do evaluation-interpolation at only $kt + (g-1)(t-1)$ places. If one could relax this condition to $|\mathcal{S}| \geq kt + (g-1)(t-1)$, this would improve Proposition 6 to $M_{q,t}^{\mathrm{sym}} \leq (1 + \epsilon'_t(q))t$ for q square, $q \geq (t+1)^2$, with $\epsilon'_t(q) = \frac{t-1}{\sqrt{q}-t}$. For $t = 2$ this is done in [12,15] using techniques from [13]. However, as observed at the end of [13], a generalization to $t \geq 3$ would require new arguments.
4. Lemma 4, which generalizes [17, Lemma 1.2], is clearly not optimal. When deriving upper bounds on $\mu_q^{\mathrm{sym}}(k, m_t)$ for non-square q, it might be better to use evaluation-interpolation at places of higher degree, as first introduced in [4], and further developped e.g. in [8,12]. To do this in an optimal way one needs function fields F_i defined over $\mathbb{F}_q$, of genus $g_i \to \infty$, with $\frac{g_{i+1}}{g_i} \to 1$ and $N_i^{(d)} \sim \frac{q^{d/2}-1}{d} g_i$ where $N_i^{(d)}$ is the number of places of degree d in F_i, for a convenient d. This improves the bound on $M_{q,t}^{\mathrm{sym}}$ by a factor $\frac{1}{d}$. The existence of these function fields was first claimed in [8], but unfortunately with an incorrect proof. A corrected construction, based on Drinfeld modular curves, will be found in [6].

5. All our bounds for multiplication in extension fields also hold for truncated polynomials. For instance we have $\hat{M}_{q,t}^{\mathrm{sym}} \leq (1+\epsilon_t(q))t$ for q square, $q \geq (t+2)^2$, and $\hat{M}_{q,t}^{\mathrm{sym}} \leq C_t(q)$ for all $q \geq t$. This requires only minor changes in our constructions. In Proposition 4, instead of evaluation at a place Q of degree k, one uses evaluation at order k at an extra place P_0 of degree 1. Likewise in Proposition 5, one needs one more place of degree 1, but one does not need Q (then the proof of Proposition 6 is slightly simplified since one does not need to invoke [18, Cor. 5.2.10] anymore).

References

1. Julia : a high-level, high-performance dynamic language for technical computing. http://julialang.org.
2. Stéphane Ballet, Jean Chaumine, Julia Pieltant, Matthieu Rambaud, Hugues Randriambololona, and Robert Rolland. On the tensor rank of multiplication in finite extensions of finite fields and related issues in algebraic geometry. *Russian Mathematical Surveys*, to appear.
3. Stéphane Ballet. Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$. *Finite Fields and their Applications*, 5:364–377, 1999.
4. Stéphane Ballet and Robert Rolland. Multiplication algorithm in a finite field and tensor rank of the multiplication. *Journal of Algebra*, 272:173–185, 2004.
5. Razvan Barbulescu, Jérémie Detrey, Nicolas Estibals, and Paul Zimmermann. Finding optimal formulae for bilinear maps. In *International Workshop on the Arithmetic of Finite Fields*, pages 168–186. Springer, 2012.
6. Alp Bassa, Peter Beelen, Matthieu Rambaud, and Hugues Randriam. In preparation.
7. Nader H. Bshouty. Multilinear complexity is equivalent to optimal tester size. *Electronic Colloquium on Computational Complexity*, 20:11, 2013.
8. Ignacio Cascudo, Ronald Cramer, Chaoping Xing, and An Yang. Asymptotic bound for multiplication complexity in the extensions of small finite fields. *IEEE Transactions on Information Theory*, 58(7):4930–4935, 2012.
9. David V. Chudnovsky and Gregory V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4(4):285–316, 1988.
10. Svyatoslav Covanov. Improved method for finding optimal formulas for bilinear maps in a finite field. *Theoretical Computer Science*, 2019.
11. Anatolii Karatsuba. Multiplication of multidigit numbers on automata. In *Soviet Physics Doklady*, volume 7, pages 595–596, 1963.
12. Hugues Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *Journal of Complexity*, 28(4):489–517, 2012.
13. Hugues Randriambololona. $(2,1)$-separating systems beyond the probabilistic bound. *Israel Journal of Mathematics*, 195(1):171–186, 2013.
14. Hugues Randriambololona. On products and powers of linear codes under componentwise multiplication. In *Algorithmic Arithmetic, Geometry, and Coding Theory*, volume 637 of *Contemporary Mathematics*, pages 3–78. AMS, 2015.
15. Hugues Randriambololona. Gaps between prime numbers and tensor rank of multiplication in finite fields. *Designs, Codes and Cryptography*, 87(2/3):627–645, 2019.
16. Gadiel Seroussi and Abraham Lempel. On symmetric algorithms for bilinear forms over finite fields. *Journal of Algorithms*, 5:327–344, 1984.
17. Igor E. Shparlinski, Michael A. Tsfasman, and Serge G. Vladut. Curves with many points and multiplication in finite fileds. In *Coding Theory and Algebraic Geometry*, volume 1518 of *Lecture Notes in Mathematics*, pages 145–169. Springer, 1992.
18. Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.
19. Volker Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356, 1969.
20. Shmuel Winograd. On multiplication of 2×2 matrices. *Linear Algebra and its Applications*, 4:381–388, 1971.
21. Shmuel Winograd. Some bilinear forms whose multiplicative complexity depends on the field of constants. *Mathematical Systems Theory*, 10:169–180, 1977.