On a matrix product question in cryptography *†

Mei-Chu Chang‡
Department of Mathematics
University of California, Riverside
mcc@math.ucr.edu

Abstract

Let A, B be invertible $n \times n$ matrices with irreducible characteristic polynomials. For $k \in \mathbb{Z}^+$, denote

$$M_k(A, B) := \{f(A)g(B) : f, g \in \mathbb{F}_q[x], \text{ with } \deg f, \deg g < k\}.$$

Assume $q \geq 2n$, we prove that

$$|M_k(A, B)| > 4^{-k-1} q^{\min(n, 2k-1)}.$$

Moreover, let $d = \dim \operatorname{Ker}(AB - BA)$, we prove

$$|M_k(A, B)| > \frac{1}{16\binom{n}{d}\big(2(n-d)\big)^{\frac{n-d}{2}}}\ q^{k+\min(\frac{k}{2}, \frac{n-d}{2})}.$$

Inspired by a question of Maze, Monico and Rosenthal [MMR], I. Shparlinski [S] proposed the following problem:

---

*2000 *Mathematics Subject Classification*: 15B33, 11C .

†*Key words*: matrices over finite fields, product sets, additive combinatorics, cryptography.

‡Research partially financed by the National Science Foundation.

Given three $n \times n$ matrices A, B, S over $\mathbb{F}_q$, obtain a nontrivial lower bound on the size of the set of the matrix products

$$M_k(A,B,S) = \{f(A)Sg(B) : f, g \in \mathbb{F}_q[x], \text{ with } \deg f, \deg g < k\}.$$

Apparently, a trivial lower (respectively, upper) bound is q^k (resp. q^{2k}).

Assume S is invertible. We can consider

$$f(A)Sg(B)S^{-1} = f(A)g(B_1) \text{ with } B_1 = SBS^{-1}.$$

Thus we may drop S and consider obtaining a lower bound on the size of the set of the matrix products $f(A)g(B)$. We start with some notations.

Given $A, B \in GL_n(q)$. For $h \in \mathbb{Z}^+$, we denote

$$\mathcal{P}_h = \{f \in \mathbb{F}_q[x] : \deg f \leq h\}.$$

Fix a positive integer $k \leq n$. Let

$$M_k(A,B) = \{f(A)g(B) : f, g \in \mathcal{P}_{k-1}\}.$$

We have the following lower bound on $|M_k(A,B)|$.

Proposition 1. *Assume $q \geq 2n$. Let $r'_* = \min(r', 2k-1)$, where r' is the number of distinct eigenvalues of A. Similarly, we have r''_* for B. Then*

$$|M_k(A,B)| > 4^{-k-1} q^{\frac{1}{2}(r'_* + r''_*)} \tag{1}$$

Remark 1.1. If eigenvalues of A (respectively, B) are distinct, we get

$$|M_k(A,B)| > 4^{-k+1-\epsilon} q^{\min(n,2k-1)}. \tag{2}$$

Suppose the characteristic polynomials of A and B are irreducible over $\mathbb{F}_q$. Then for any $f \in \mathcal{P}_{k-1} \setminus \{0\}$ with $k \leq n$, f does not vanish on any eigenvalue of A. Therefore the assumption $q \geq 2n$ is unnecessary. Note that in this situation (2) is also of interest for q fixed and $n \to \infty$. On the other hand, (2) is poor, if $k \sim n$. Indeed, assume A, B can be diagonalized simultaneously, then $|M_k(A,B)| \leq n! q^{n+1}$.

Next we give some estimates exploiting that A and B are far from commuting and will prove the following theorem.

Theorem 2. *Let $A, B \in GL_n(q)$ and let $d = \dim Ker(AB - BA)$. If the characteristic polynomials of A and B are irreducible, then*

$$M_k(A,B) > \frac{1}{16\binom{n}{d}\big(2(n-d)\big)^{\frac{n-d}{2}}}\, q^{k+\min(\frac{k}{2},\frac{n-d}{2})}. \qquad (3)$$

Remark 2.1. For almost all $A, B \in GL_n(q)$, we have $d = 0$. Indeed, the probability of being singular of a matrix in the space of $n \times n$ matrices with zero diagonal is less than $2/q$.

This type of result fits in the general 'sum-product' philosophy, in the sense that the set of products of additively stable sets in a ring is usually large, unless for some algebraic reason. But in this problem ad hoc arguments perform better than invoking more general theorems. (See [T].)

Denote

$$\mathcal{P}' = \{f \in \mathcal{P}_{k-1} : f(A) \in GL_n(q)\},$$
$$\mathcal{P}'' = \{g \in \mathcal{P}_{k-1} : g(B) \in GL_n(q)\}.$$

First, we prove the following

Lemma 3. Assume $q \geq 2n$. Then $|\mathcal{P}'|\,|\mathcal{P}''| > \frac{1}{4}q^{2k}$.

Proof. Let $\xi_1, \ldots, \xi_n$ be the eigenvalues of A (in some extension $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$). Since for any $f \in \mathcal{P}'$,

$$f(\xi_i) \neq 0, \text{ for } i = 1, \ldots, n, \qquad (4)$$

we have $|\mathcal{P}'| \geq q^k - nq^{k-1} > \frac{1}{2}q^k$. Similarly, $|\mathcal{P}''| > \frac{1}{2}q^k$. $\square$

Remark 3.1. Suppose the characteristic polynomials of A and B are irreducible over $\mathbb{F}_q$. Then for any $f \in \mathcal{P}_{k-1} \setminus \{0\}$ with $k \leq n$, f does not vanish on any eigenvalue of A. Therefore the assumption $q \geq 2n$ is unnecessary and we have $\mathcal{P}' = \mathcal{P}'' = \mathcal{P}_{k-1} \setminus \{0\}$.

Proof of Proposition 1.

We want to give a lower bound on

$$M := |M_k(A,B)|.$$

For $x \in GL_n(q)$, denote

$$\eta(x) = \big|\{(f,g) \in \mathcal{P}' \times \mathcal{P}'' : x = f(A)g(B)\}\big|.$$

Since

$$M \geq \big|\{f(A)g(B) : f \in \mathcal{P}', g \in \mathcal{P}''\}\big|,$$

by Cauchy-Schwarz, we have

$$|\mathcal{P}'|\,|\mathcal{P}''| = \sum_x \eta(x) \leq \Big(\sum_x \eta(x)^2\Big)^{1/2} M^{1/2}.$$

Combining with Lemma 3, we have

$$M > \frac{q^{4k}}{16E}\,, \tag{5}$$

where

$$\begin{aligned} E =& \sum_x \eta(x)^2 \\ =& \big|\{(f,g,F,G) \in \mathcal{P}' \times \mathcal{P}'' \times \mathcal{P}' \times \mathcal{P}'' : f(A)g(B) = F(A)G(B)\}\big|. \end{aligned} \tag{6}$$

We note that the identity in (6) is equivalent to

$$F(A)^{-1}f(A) = G(B)g(B)^{-1}. \tag{7}$$

Therefore, denoting

$$\alpha(x) = |\{(f,F) \in \mathcal{P}' \times \mathcal{P}' : x = F(A)^{-1}f(A)\}|$$

and

$$\beta(x) = |\{(g,G) \in \mathcal{P}'' \times \mathcal{P}'' : x = G(B)g(B)^{-1}\}|,$$

we have

$$E = \sum_x \alpha(x)\beta(x) \leq \sqrt{\sum \alpha(x)^2}\sqrt{\sum \beta(x)^2}. \tag{8}$$

Therefore, we are estimating $E_1 := \sum_x \alpha(x)^2$.

$$\begin{aligned} E_1 =& \left|\{(f,F,\tilde{f},\tilde{F}) \in \mathcal{P}' \times \cdots \times \mathcal{P}' : F(A)^{-1}f(A) = \tilde{F}(A)^{-1}\tilde{f}(A)\}\right| \\ \le& \left|\{(f,F,\tilde{f},\tilde{F}) \in \mathcal{P}_{k-1} \times \cdots \times \mathcal{P}_{k-1} : (f\tilde{F})(A) = (\tilde{f}F)(A)\}\right| \\ =& \left|\{(f,F,\tilde{f},\tilde{F}) \in \mathcal{P}_{k-1} \times \cdots \times \mathcal{P}_{k-1} : f\tilde{F} - \tilde{f}F \in I\}\right|, \end{aligned}$$

where

$$I = \{h \in \mathbb{F}_q[x] : h \text{ vanishes on the eigenvalues of } A\}\big|.$$

Since A has r' distinct eigenvalues,

$$|I \cap \mathcal{P}_{2k-2}| \le q^{2k-1-r'_*},$$

with $r'_* = \min(r', 2k-1)$.

To estimate E_1, we fix $\tilde{f}$ and F. Since

$$f\tilde{F} \in \tilde{f}F + (I \cap \mathcal{P}_{2k-2}),$$

there are at most $q^{2k-1-r'_*}$ choices of $f\tilde{F}$. Given $g = f\tilde{F}$, factorizations of g over $\overline{\mathbb{F}_q}$ gives at most $q\binom{2k-2}{k-1}$ choices of $(f, \tilde{F})$.

Since there are q^{2k} choices of $(\tilde{f}, F)$, we have

$$E_1 := \sum_x \alpha(x)^2 \le q^{2k}\, q^{2k-1-r'_*}\ \ q\binom{2k-2}{k-1} < 4^{k-1}q^{4k-r'_*}. \tag{9}$$

Similarly,

$$E_2 < 4^{k-1}q^{4k-r''_*}.$$

Putting (5), (8) and (9) together, we have (1). $\square$

For the rest of the paper, we assume that the characteristic polynomials of A and B are irreducible over $\mathbb{F}_q$ and

$$k < n \ll q.$$

Denote

$$\mathcal{P} = \mathcal{P}' = \mathcal{P}'' = \mathcal{P}_{k-1} \setminus \{0\}.$$

Returning to the definition of E in (6), we let

$$\mathcal{E} = \{(f, g, F, G) \in \mathcal{P}^4 : F(A)^{-1} f(A) = G(B) g(B)^{-1}\},$$

and let $\mathcal{E}_1 = \pi_{(f,F)}(\mathcal{E}) \subset \mathcal{P} \times \mathcal{P}$ be the projection. We denote by $\mathcal{M} = \mathcal{M}(B)$ the algebra of $n \times n$ mtrices that commute with B. Clearly,

$$F(A)^{-1} f(A) \in \mathcal{M}, \text{ if } (f, F) \in \mathcal{E}_1, \tag{10}$$

and also,

$$|\mathcal{E}_1| \geq \frac{E}{q^k}. \tag{11}$$

Lemma 4. *Let $(f, F) \in \mathcal{E}_1$. If $F(A)^{-1} f(A)$ has m distinct eigenvalues with $m > \frac{n}{2}$, then*

$$\dim Ker(AB - BA) \geq 2m - n. \tag{12}$$

Proof. We diagonalize

$$A = \sum_{j=1}^{n} \xi_j \, e_j \otimes e_j \quad \text{with} \quad \xi_j \in \overline{\mathbb{F}_q}.$$

Then

$$\bar{A} := F(A)^{-1} f(A) = \sum_{j=1}^{n} \lambda_j \, e_j \otimes e_j \in \mathcal{M}, \text{ where } \lambda_j = \frac{f(\xi_j)}{F(\xi_j)}.$$

Also,

$$\bar{A}^r := \sum_{j=1}^{n} \lambda_j^r \, e_j \otimes e_j \in \mathcal{M}, \quad \text{for all } r \in \mathbb{Z}^+.$$

We partition $\{1, \cdots, n\} = \bigcup_{\alpha=1}^{m} I_\alpha$ with $\lambda_j = \lambda_{j'} = \lambda_\alpha$ for all $j, j' \in I_\alpha$ and $\lambda_\alpha \neq \lambda_\beta$ for $\alpha \neq \beta$ and denote

$$V_\alpha := \sum_{j \in I_\alpha} e_j \otimes e_j.$$

It follows that

$$\sum_{\alpha=1}^{m} \lambda_\alpha^r V_\alpha \in \mathcal{M}, \quad \text{for } r = 0, 1, \cdots, m-1.$$

Therefore,

$$V_\alpha \in \mathcal{M} \ \text{ for } \alpha = 1, \ldots, m. \tag{13}$$

The vectors in (13) can be extended to a basis of the space generated by $\{e_j \otimes e_j : j = 1, \ldots, n\}$. Therefore, A has a decomposition

$$A = A_0 + A_1 \ \text{ with } A_0 \in \mathcal{M}, A_1 \notin \mathcal{M}.$$

Obviously, $\operatorname{rank} A_1 \leq n - \left|\{V_\alpha\}_\alpha\right| = n - m$. Since

$$AB - BA = A_1 B - BA_1,$$

$\dim \operatorname{Ker}(AB - BA) = n - \operatorname{rank}(A_1 B - BA_1) \geq n - 2(n-m) = 2m - n.$ $\square$

Lemma 5. *Let $m \geq n - \frac{k}{2}$ and assume that for all $(f, F) \in \mathcal{E}_1$, $F(A)^{-1} f(A)$ has fewer than m distinct eigenvalues, then*

$$E < \binom{n}{2(n-m)} \big(4(n-m)\big)^{n-m} q^{3k - \min(k, n-m)}. \tag{14}$$

Proof. For $(f, F) \in \mathcal{E}_1$, we write

$$F(A)^{-1} f(A) = \sum_{j=1}^{n} \frac{f(\xi_j)}{F(\xi_j)} \, e_j \otimes e_j,$$

where $\xi_1, \cdots, \xi_n$ are the eigenvalues of A.

Let $S \subset \{1, \ldots, n\}$ be maximal such that all elements in $\left\{\frac{f(\xi_j)}{F(\xi_j)} : j \in S\right\}$ are distinct. Hence $|S| < m$.

Take $S_1 \subset \{1, \ldots, n\} \setminus S$, with $|S_1| = n - m$. Then we take $S_2 \subset \{1, \ldots, n\}$, such that $S_1 \cap S_2 = \emptyset, |S_2| = n - m$ and

$$\left\{\frac{f(\xi_j)}{F(\xi_j)} : j \in S_1\right\} \subset \left\{\frac{f(\xi_j)}{F(\xi_j)} : j \in S_2\right\}.$$

Such S_2 exists, because $S \cap S_1 = \emptyset$ and $m > \frac{n}{2}$.

Thus there is a map $S_1 \to S_2$ sending j to j' such that

$$f(\xi_j) - \frac{F(\xi_j)}{F(\xi_{j'})} f(\xi_{j'}) = 0 \quad \text{for } j \in S_1. \tag{15}$$

Once S_1, S_2 and the map $j \mapsto j'$ are specified, (15) gives $n-m$ linearly independent conditions on f (with F fixed), and the number of $(f, F) \in \mathcal{P} \times \mathcal{P}$ satisfying (15) is at most $q^{2k-(n-m)}$. Let $b_j = \frac{F(\xi_j)}{F(\xi_{j'})}$. Here we have used that the matrix having $(\xi_1^j, \ldots, \xi_{n-m}^j) - b_j(\xi_{1'}^j, \ldots, \xi_{n-m'}^j)$ as the jth column has the maximal rank $n-m$, since all $\xi_i, \xi_{i'}$ are distinct.

The number of $(S_1, S_2, j \to j')$ is bounded by

$$\binom{n}{2(n-m)} \binom{2(n-m)}{n-m} (n-m)^{n-m}.$$

Therefore,

$$|\mathcal{E}_1| < \binom{n}{2(n-m)} \big(4(n-m)\big)^{n-m} q^{2k-n+m}$$

and (11) implies (14). $\square$

Therefore, under the assumption of Lemma 5, by (5)

$$M_k(A, B) > \frac{1}{16 \binom{n}{2(n-m)} \big(4(n-m)\big)^{n-m}} \, q^{k+n-m}. \tag{16}$$

By Lemma 4 and Lemma 5, given $m > \max(\frac{d+n}{2}, n - \frac{k}{2})$, we see that (16) holds. Thus, Theorem 2 is proved.

Acknowledgement. The author would like to thank the mathematics department of University of California at Berkeley for hospitality.

References

[MMR] G. Maze, C. Monico and J. Rosenthal, *Public key cryptography based on semigroup actions*, Adv. Math. of Commun., 1 (2007), 489507.

[S] I. E. Shparlinski, *Additive Combinatorics over Finite Fields: New Results and Applications*, (preprint).

[T] T. Tao, *The sum-product phenomenon in arbitrary rings*, Contrib. Discrete Math. 4 (2009), 5982.