ON RYSTOV’S GENERALIZATION OF THE ČERNÝ CONJECTURE

NOAM LIFSHITZ, CIARAN MULLAN, AND BOAZ TSABAN

Abstract. We resolve a conjecture of Rystov concerning products of matrices, that generalizes the Černý Conjecture. This is a preliminary announcement. Later versions will include additional results and details.

The following conjecture is a generalization of the celebrated, and still open, Černý Conjecture. By product in $A_1, \ldots, A_k$ of length $l$ we mean a product

$$A_{i_1}A_{i_2}\cdots A_{i_l}$$

with $1 \leq i_1, \ldots, i_l \leq k$ not necessarily distinct.

**Conjecture 1** (Rystov). Let $A_1, \ldots, A_k \in M_n(\mathbb{F})$, $k$ arbitrary. If the semigroup generated by $A_1, \ldots, A_k$ is finite and contains the zero matrix $O$, then there is a product in $A_1, \ldots, A_k$ of length at most $n^2$ that is equal to $O$.

Over finite fields, the condition that the generated semigroup is finite is satisfied automatically, and the conjecture asserts that if any product in matrices $A_1, \ldots, A_k$ equals $O$, then there is one of length at most $n^2$. As there are no zero divisors in a field, the conjecture is true when $n = 1$. We prove that this conjecture fails for all $n > 1$. In the language of semigroup theory, the following lemma is equivalent to the assertion that the semigroup of all singular matrices in $M_2(\mathbb{F})$ is categorical at 0.

**Lemma 2** (folklore). Let $A, B, C \in M_2(\mathbb{F})$, $B$ singular. If $ABC = O$, then $AB = O$ or $BC = O$.

**Proof.** If $C$ is invertible we are done. Thus, assume that $C$ is singular. If $C = O$ we are done, so assume $C$ is nonzero. Then 0 is an eigenvalue of $C$, and the characteristic polynomial of $C$ is $x(x - \gamma) = 0$. If $\gamma = 0$ then the Jordan form of $C$ is

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

If $\gamma \neq 0$, then $C$ is conjugate to a nonzero diagonal matrix of the form

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

Since scalar multiplication does not affect our problem, we may assume in this case that $C$ is conjugate to

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

Conjugate $A, B, C$ by the same matrix (and multiply $C$ by a nonzero scalar, if needed), such that $C$ obtains one of the two above-mentioned forms.
As $B$ is singular, there is $v$ such that the columns of $B$ are $(v, \beta v)$ or $(\vec{0}, v)$. If $B = (v, \beta v)$, then
\[
O = ABC = A(v, \beta v)C = (Av, \beta Av)C = (Av, \vec{0}) \text{ or } (\vec{0}, Av),
\]
depending on the form of $C$. Then $Av = \vec{0}$, and therefore $AB = (Av, \beta Av) = O$. And if $B = (\vec{0}, v)$, then
\[
BC = (\vec{0}, v) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = O. \quad \Box
\]

Lemma 2 has the following consequence. Assume, in general, that
\[
A_1 \cdots A_k = O
\]
in $M_2(\mathbb{F})$. By cancelling off the regular matrices on the edges, We may then assume that $A_1$ and $A_k$ are singular. Next, if any $A_i$ is singular, $1 < i < k$, we can apply Lemma 2 to
\[
(A_1 \cdots A_{i-1})A_i(A_{i+1} \cdots A_{k-1}A_k)
\]
and conclude that
\[
(A_1 \cdots A_{i-1})A_i = O \text{ or } A_i(A_{i+1} \cdots A_{k-1}A_k) = O.
\]
We can continue this procedure until we arrive at a word of the form
\[
A_1 \cdots A_k = O
\]
where $A_1$ and $A_k$ are singular, and all other matrices are invertible.

**Corollary 3.** Let $A, B \in M_2(\mathbb{F})$ with $B$ invertible. If any product in $A, B$ equals $O$, then there is a unique shortest product in $A, B$ that equals $O$. The shortest product is of the form $AB^nA = O$. \quad \Box

We are now ready to prove the main result.

**Theorem 4.** Let $n \geq 2$. For each $N$, there is a finite field $\mathbb{F}$ and matrices $A, B \in M_n(\mathbb{F})$ such that the minimal length of a product in $A, B$ that equals $O$ exists, and its length is greater than $N$.

**Proof.** If $A, B \in M_2(\mathbb{F})$ exemplify the assertion for $n = 2$, then for every larger $n$, the block matrices
\[
\begin{pmatrix} A & O \\ O & O \end{pmatrix}, \begin{pmatrix} B & O \\ O & O \end{pmatrix} \in M_n(\mathbb{F})
\]
exemplify the same assertion. Thus, we may assume that $n = 2$.

Take
\[
A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},
\]
and note that $B$ is invertible and $A$ is idempotent. As
\[
B \begin{pmatrix} y \\ x \end{pmatrix} = \begin{pmatrix} x + y \\ y \end{pmatrix},
\]
we have that
\[
B^k \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} F_{k+1} \\ F_k \end{pmatrix}
\]
for all \( k = 0, 1, \ldots \), where \( F_0 = 0, F_1 = 1 \), and \( F_{k+1} = F_k + F_{k-1} \) for all \( k > 1 \), that is, \( F_k \) is the \( k \)-th element of the Fibonacci sequence. Thus,

\[
AB^k A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} B^k \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} F_{k+1} & 0 \\ F_k & 0 \end{pmatrix} = F_{k+1}
\]

for all \( k \). Fix a prime number \( p \geq F_{N+1} \). Let \( k \) be minimal such that \( F_{k+1} = 0 \) (mod \( p \)). Necessarily, \( k \geq N \). Then, in \( M_2(\mathbb{F}_p) \),

\[
AB^k A = O,
\]

and \( AB^m A \neq O \) for all \( 0 \leq m < k \). By Corollary 3 the length of the shortest \( O \) product is \( k + 2 \geq N + 2 > N \). \( \Box \)

**Acknowledgments.** We learned of the Rystov Conjecture from Benjamin Steinberg, who presented it in an open problem session during a recent conference in honor of Stuart Margolis. We thank Ben and Stuart for stimulating discussions on this problem.

**Department of Mathematics, Bar Ilan University, 5290002 Ramat Gan, Israel**  
*E-mail address: noamlifshitz@gmail.com*

**Technische Universität Darmstadt, Fachbereich Informatik, Kryptographie und Computeralgebra, Hochschulstrasse 10, 64289 Darmstadt, Germany**

**Department of Mathematics, Bar Ilan University, 5290002 Ramat Gan, Israel**  
*E-mail address: tsaban@math.biu.ac.il*  
*URL: http://www.cs.biu.ac.il/~tsaban*