# ON A CONJECTURE FROM A FAILED CRYPTOANALYSIS

SHENGTONG ZHANG

## 1. Introduction

Let $P(x, y)$ be a bivariate polynomial with coefficients in $\mathbb{C}$. Form the $n \times n$ matrices $L_n$ whose elements are defined by $P(i, j)$. Define the matrices $M_n = I_n - L_n$.

We show that $\mu_n = \det(M_n)$ is a polynomial in $n$, thus answering a conjecture of Naccache and Yifrach.

## 2. The Proof

Our proof is based on the folklore identity of Sylvester.

**Theorem 2.1.** *Let $A$ be an $n \times m$ matrix, and $B$ be an $m \times n$ matrix. Then*

$$\det(I_n - AB) = \det(I_m - BA).$$

In our case, there exists a constant $D$ such that

$$P(x, y) = \sum_{i=0}^{D} \sum_{j=0}^{D} a_{ij} x^i y^j$$

where $a_{ij} \in \mathbb{C}$ are coefficients. If we let $A(n)$ be the $(D + 1) \times n$ matrix given by

$$A(n)_{ij} = j^i$$

for $0 \leq i \leq D$ and $1 \leq j \leq n$, and let $C$ be the $(D + 1) \times (D + 1)$ matrix given by $C_{ij} = a_{ij}$, then we can compute that

$$L_n = A(n)^T C A(n).$$

Thus by Sylvestor's identity, we have

$$\mu_n = \det(I_n - L_n) = \det(I - CA(n)A(n)^T).$$

The matrix $A(n)A(n)^T$ is a $(D + 1) \times (D + 1)$ matrix with entries

$$(A(n)A(n)^T)_{ij} = \sum_{k=1}^{n} k^{i+j}$$

which is a polynomial in $n$ by Faulhaber's formula [1]. Thus, the dimensions of $CA(n)A(n)^T$ is independent of $n$, and each entry of $CA(n)A(n)^T$ is a polynomial in $n$. As the determinant of a constant size matrix is a polynomial in the entries, we conclude that $\mu_n$ is a polynomial in $n$.

*Date*: September 2022.

## References

[1] Carl Jacob, *De usu legitimo formulae summatoriae Maclaurinianae*. Journal für die reine und angewandte Mathematik. Vol. 12. pp. 263–72 (1834)

[2] David Naccache and Ofer Yifrach-Stav, *A Conjecture From a Failed Cryptanalysis*. Cryptology ePrint Archive, Paper 2022/1273. https://eprint.iacr.org/2022/1273

Stanford University, Stanford, CA, USA

*Email address*: stzh1555@stanford.edu