A Conjecture From a Failed Cryptanalysis

David Naccache[1] and Ofer Yifrach-Stav[1]

DIÉNS, ÉNS, CNRS, PSL University, Paris, France
45 rue d'Ulm, 75230, Paris CEDEX 05, France
ofer.friedman@ens.fr, david.naccache@ens.fr

Abstract. This note describes an observation discovered during a failed cryptanalysis attempt.
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 $M_n = L_n - \mathrm{ID}_n$.
It appears that $\mu(n) = (-1)^n \det(M_n)$ is a polynomial in n that we did not characterize.
We provide a numerical example.

1 Introduction

During a failed cryptanalysis of multivariate signature scheme we stumbled on the following observation.

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 $M_n = L_n - \mathrm{ID}_n$.

It appears that $\mu(n) = (-1)^n \det(M_n)$ is a polynomial in n that we did not characterize.

If we replace the definition of μ by $\mu(n) = (-1)^{n+1} \det(M_n)$ then a similar phenomenon occurs with $M_n = L_n + \mathrm{ID}_n$.

We did not research the reasons for this behavior but note it for those who wish to further investigate it.

2 Example

Let

$$P(x,y) = hx^2y + gy^2x + fy^2 + ex^2 + dxy + ax + by + c$$

Then

$$\mu(n) = (-1)^n \det(M_n) = \sum_{i=0}^{9} \eta_i n^i$$

$$\eta_9 = \frac{def + cgh - afh - beg}{2160}$$

$$\eta_8 = -\frac{gh}{240}$$

$$\eta_7 = -\frac{\rho}{60} - 6\eta_9$$

$$\eta_6 = \frac{\kappa}{72} - \frac{4ef + 2\rho}{45} - 6\eta_8$$

$$\eta_5 = \frac{\kappa}{24} + \frac{cg + ch - af - be - 2ef}{12} + 9\eta_9$$

$$\eta_4 = \frac{\kappa - 7ef + 2\rho}{36} + 9\eta_8 - \frac{g+h}{4} - \tau$$

$$\eta_3 = -2\sigma - \frac{g+h}{2} - \eta_5 - \eta_9 - \eta_7$$

$$\eta_2 = \alpha - \frac{19ef + 2\rho}{180} - 4\eta_8 - \frac{g+h}{4} + \frac{\kappa}{72} - 2\sigma + \tau$$

$$\eta_1 = \alpha - c$$

$$\eta_0 = 1$$

$$\text{Where } \sigma = \frac{d+e+f}{6}, \quad \tau = \frac{ab - cd}{12} + 9\eta_9 - \eta_5, \quad \alpha = -\frac{a+b}{2} - \sigma$$

$$\kappa = ah + bg - de - df - eg - fh \quad \text{and} \quad \rho = eg + fh + gh$$

The Mathematica code generating those polynomials is very simple:

```
M := Function[n,
  P := Function[{x, y},
    h x^2 y + g y^2 x + f y^2 + e x^2 + d x y + a x + b y + c];
  Table[P[i, j] , {i, 1, n}, {j, 1, n}] - IdentityMatrix[n]]

t = Table[ Det[(-1)^(k) M[k]], {k, 1, 20}];
mu = Collect[Expand[InterpolatingPolynomial[t, n]], n];
```

The formulae were simplified (?) by hand using $\sigma, \tau, \alpha, \kappa, \rho$ and machine-tested.

3 Further Remarks

3.1 Extending the Example

Adding to the example the coefficients:

$$P(x,y) = c_1y^3 + c_2x^3 + hx^2y + gy^2x + fy^2 + ex^2 + dxy + ax + by + c$$

the formal interpolation offered by Mathematica runs out of resources.

Nonetheless, it is possible to disassemble the effect of c_1, c_2 by assigning to those coefficients notable values such as 10^6 and solving locally a system of linear equations assuming that the missing terms are linear combinations of c_1, c_2 and c_1c_2.

The resulting coefficients are very large and have additional terms with respect to the η_i. For instance, the new value of η_2 becomes:

$$\eta_2' = \eta_2 + \frac{ac_1 + bc_2}{30} + \frac{d(c_1 + c_2)}{60} + \frac{c_1g + c_2h}{180} - \frac{c_1c_2}{42} - \frac{c_1 + c_2}{4}$$

3.2 An Identity

We observed that $\forall q \in \mathbb{N}$, $\forall u \leq q$ all $P(x,y) = x^u y^{q-u}$ have the same μ.

3.3 A Related Application

In a private communication, Éric Brier notes that taking $P(x,y) = 1$ it is possible to prove that the number of even derangements is equal to:

$$\frac{\left\lfloor \frac{n!}{e} \right\rceil + (-1)^n(n-1)}{2}$$

Which is indeed a new explicit formula for oeis.org sequence A000387.