On Rank Properties of Toeplitz Matrices over Finite Fields*

E. KALTOFEN[1] and A. LOBO[2]

[1]Department of Mathematics, North Carolina State University
Raleigh, North Carolina 27695-8205, USA; email: kaltofen@math.ncsu.edu

[2]Department of Computer and Information Sciences, The University of Delaware
Newark, Delaware 19711-1501, USA; email: alobo@cis.udel.edu

Abstract

Out of all the $n \times n$ Toeplitz matrices over a finite field of q elements, a fraction of exactly $(1-1/q)$ is non-singular. Also a fraction of exactly $(1/q)(1-1/q)^2(1-(q-1)/q^2)^{r-1}$ has generic rank $0 < r < n$. These statements are proven with the extended Euclidean algorithm and the theory of subresultants. A matrix has generic rank r when all its leading principal minors up to dimension r are non-zero, and r is maximal. Our results have implications to the probability of success of the block Wiedemann linear system solver algorithm, which is an open question at the present time.

1 Introduction

Let $\mathbb{F}_q$ be a finite field of q elements. An $n \times n$ matrix $T_n = (t_{i-j})$, $i, j = 1, \ldots, n$ over $\mathbb{F}_q$ has Toeplitz structure when all the elements along the diagonal are equal, and those along each line parallel to the diagonal, are also equal. So

$$T_n = \begin{bmatrix} t_0 & t_{-1} & \ldots & t_{2-n} & t_{1-n} \\ t_1 & t_0 & \ldots & t_{3-n} & t_{2-n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ t_{n-2} & t_{n-3} & \ldots & t_0 & t_{-1} \\ t_{n-1} & t_{n-2} & \ldots & t_1 & t_0 \end{bmatrix} \tag{1}$$

is uniquely specified by the $2n-1$ elements of its first row and column.

An alternate representation for T_n is the polynomial

$$\mathcal{T}_n(x) = a_{2n-2} + a_{2n-3}x + \cdots + a_1 x^{2n-3} + a_0 x^{2n-2} \tag{2}$$

over $\mathbb{F}_q[x]$, the polynomial ring over $\mathbb{F}_q$ in the indeterminate x, with coefficients $(a_{i-j+n-1}) = (t_{i-j})$ where $i, j = 1, \ldots, n$.

*This material is based on work supported in part by the National Science Foundation under Grant No. CCR-9319776. An early report of this work was made in a poster presentation at ISSAC '95 in Montreal, Canada. Authors' previous address: Department of Computer Science, Rensselaer Polytechnic Institute, Troy, New York 12180-3590.

1.1 Statement of Results

In this paper we exploit the connection between the condition under which a Toeplitz matrix $T_n \in \mathsf{K}^{n \times n}$ is non-singular, and the extended Euclidean algorithm over the associated polynomial $T_n(x)$ and x^{2n-1}. We have two results to report.

First, out of all the $n \times n$ matrices T_n over $\mathbb{F}_q$, a fraction of exactly $(1-1/q)$ is non-singular. This means that there are $(q-1)q^{2n-2}$ non-singular Toeplitz matrices T_n. It follows that T_n is non-singular with probability $1-1/q$ when the entries in its first row and column are chosen uniformly at random from the set of elements of $\mathbb{F}_q$.

Second, again for $n \times n$ Toeplitz matrices over $\mathbb{F}_q$, there are $(q-1)(q^2-q+1)^{r-1}$ matrices that have generic rank r.

We say that a matrix A has *generic rank profile* when all its leading $k \times k$ principal submatrices of dimension $k = 1, 2, \ldots, \mathrm{rank}(A)$ have full rank. The *generic rank* of a matrix is the dimension of its largest leading principal submatrix that has generic rank profile.

For $0 < r < n$ the probability that T_n has generic rank r is

$$p_{r,n} = \frac{1}{q}(1-\frac{1}{q})^2(1-\frac{q-1}{q^2})^{r-1}.$$

The probability that T_n has generic rank n is

$$p_{n,n} = (1-\frac{1}{q})(1-\frac{q-1}{q^2})^{n-1}.$$

The significance of these results is that a randomly selected $n \times n$ Toeplitz matrix has full generic rank with probability almost $(1-1/q) \cdot e^{(1-n)/q}$, a quantity that approaches zero as n tends to infinity.

1.2 Relevance to Symbolic Computation

Much research has focussed on solving Toeplitz and Toeplitz-like systems of equations. The coefficient matrices of linear systems encountered in numerical analysis, coding theory, and symbolic mathematical computing, frequently have this structure.

Toeplitz matrices also see usage as pre-conditioners in the process of solving linear systems having unstructured coefficient matrices. They are especially attractive as pre-conditioners because they can be stored in linear space and the product of a Toeplitz matrix and a column vector can be computed in superlinear time by convolution using fast Fourier transform techniques.

Pre-conditioning gives the generic rank profile property to a coefficient matrix. When Gaussian elimination is performed on a matrix in generic rank profile, there is no need for row or column permutations for the purpose of avoiding a zero pivot element.

Our interest in Toeplitz matrices was motivated by their role as pre-conditioners. In the only available analysis of the block Wiedemann algorithm (Coppersmith 1994), Kaltofen (1995) employed Toeplitz pre-conditioner matrices $\mathcal{P}, \mathcal{Q}$ with entries chosen uniformly at random from the field K. He proved that provided K was large enough, $\mathcal{B} = \mathcal{P}B\mathcal{Q}$ acquired generic rank profile with a certain high probability, and then the linear system $Bx = 0$ with coefficient matrix B could be successfully solved, also with high probability.

Kaltofen's analysis uses the fact that the degree of the minimum polynomial of a matrix in generic rank profile exceeds by one, the matrix's actual rank. His approach is based upon earlier work by Kaltofen and Saunders, (1991), on Wiedemann's coordinate recurrence algorithm (Wiedemann, 1985). There unimodular, triangular Toeplitz matrices are used as pre-conditioners.

The event that $\mathcal{B}$ has generic profile, occurs with high probability if the field from which the entries of $\mathcal{P}$ and $\mathcal{Q}$ are taken has cardinality $O(n^2)$. If K is not large enough then arithmetic must be performed in an extension of K, of degree $O(\log n)$. Hence Kaltofen's analysis is meaningful only for fields of sufficiently large cardinality.

Recent experiments on very high dimensional matrices over $\mathbb{F}_2$ (Lobo, 1995) give strong evidence that the block Wiedemann algorithm is indeed successful even in fields of small cardinality. Hence, our long-term goal is to refine the earlier analysis and justify the success probability without placing any restrictions on the cardinality of the field and to avoid computationally expensive arithmetic in field extensions.

With an approach somewhat along the lines of (Borodin *et al.*,1982), we sought to determine the probability that $\mathcal{B} = \mathcal{W}_n^{(v)} \cdot X(I_r \oplus \mathbf{0}_{n-r})Y \cdot \mathcal{W}_n^{(t)}$ has generic rank profile, where X and Y are non-singular matrices from the factorization of B, r is the rank of B, and $\mathcal{W}_n^{(v)}$ and $\mathcal{W}_n^{(t)}$ are random Toeplitz matrices. The matrices $\mathcal{W}_n^{(v)}X$ and $Y\mathcal{W}_n^{(t)}$ are themselves Toeplitz-like (Gohberg *et al.*, 1986). We examined the the rank and generic rank probabilities of the matrices $\mathcal{W}$ and obtained both our stated results.

After proving the theorem on the number of non-singular Toeplitz matrices of a given dimension, over a finite field, we were informed by David G. Cantor[1] that that fact was known to Daykin (1960). Our approach is entirely different from Daykin's, and relies upon the Euclidean algorithm and the theory of subresultants. The second result, relating to the number of Toeplitz matrices having a given generic rank, is our own work.

Our results have implications to the general problem of solving linear systems. There are really two issues namely, the analysis of the block Wiedemann algorithm in fields of small cardinality, and the solution of block Toeplitz matrices over small fields. It is an open problem, at the present time, to give the proof of success of the block Wiedemann algorithm for small fields. The problem of solving Toeplitz-like systems in small fields is also open. It should be noted that the block Wiedemann algorithm converts an unstructured, possibly sparse, linear system to a block Toeplitz linear system.

Our results also apply to the use of random Toeplitz preconditioners in the LU factorization of matrices and might assist in the choice of blocksize in block-Schur triangularization algorithms.

1.3 Motivation – the 2×2 case

Let us consider 2×2 matrices of the form

$$T_2 = \begin{bmatrix} a & b \\ c & a \end{bmatrix}.$$

Let N_2 denote the number of such matrices that are non-singular. If $\mathbb{F}_q$ has odd characteristic and $a = 0$, then either $b = 0$ thereby permitting q choices for c, or $c = 0$ and there are $q-1$ more choices for b. This gives $2q-1$ singular matrices with $a = 0$. If $a \neq 0$ then b and c must be simultaneously, either quadratic residues or quadratic nonresidues. When b and c are both quadratic residues, there are $(q-1)/2$ choices for each, and 2 roots to the equation

$$a^2 = y$$

in $\mathbb{F}_q$, where $y = bc$. Similarly, when b and c are each not a quadratic residue, there are $(q-1)^2/2$ singular matrices like of the form of T_2. There are q^3 matrices in total. Therefore,

$$\begin{aligned} N_2 &= q^3 - (2q-1) - (q-1)^2/2 - (q-1)^2/2 \\ &= (q-1)q^2 \end{aligned}$$

Alternatively, if q is even, every $\alpha \in \mathbb{F}_q$ is a quadratic residue, because $(\alpha^{\frac{q}{2}})^2 = \alpha$ in $\mathbb{F}_q$, and there is only one root to the equation $a^2 = bc$. So if $a \neq 0$, there are $(q-1)^2$ triples. As before, if $a = 0$ there are $2q-1$ choices for b and c. Thus there are

$$\begin{aligned} N_2 &= q^3 - (2q-1) - (q-1)^2 \\ &= (q-1)q^2 \end{aligned}$$

non-singular 2×2 matrices. Our proof for $n > 2$ is much more involved.

1.4 Outline of Approach

We will first use the extended Euclidean algorithm on the polynomial pair $(x^{2n-1}, \mathcal{T}_n(x))$, to prove with the help of the theory of subresultants (Brown and Traub, 1971), that T_n is non-singular if and only if there is a remainder polynomial in the Euclidean reduction sequence for $(x^{2n-1}, \mathcal{T}_n(x))$ with degree exactly $n-1$. This particular result was first proven, using Padé Approximants, in Brent *et al.*, (1980).

Next we will count pairs (u, v) of polynomials in $\mathbb{F}_q[x]$ where $\deg(u) = n-1$ and $\deg(v) \leq \deg(u)$ and u/v is a valid Padé approximant (Gragg, 1972) for some $\mathcal{T}_n(x)$. There is a many-to-one correspondence between the set of non-singular $\mathcal{T}_n$ and the set of valid Padé pairs (u, v). We will demonstrate that for a particular (u, v) with $\gcd(u, v) = x^\beta$ and $\beta > 0$ there are $(q-1)q^{\beta-1}$ non-singular T_n, and that there is a unique T_n when $\beta = 0$.

With this Counting Lemma and a result from Gathen and Ma (1990), we will determine the number of non-singular $n \times n$ Toeplitz matrices over $\mathbb{F}_q$.

To count the number of Toeplitz matrices of a given generic rank, we will employ a lemma due to Sylvester (Gantmacher, 1990).

[1] Private communication, March 1995

2 The Extended Euclidean Algorithm

In this section we will present certain details of the extended Euclidean algorithm and of Padé approximation that are relevant to the proof of our main theorem. It should be noted that these theoretical properties are valid in any abstract field K.

Let $f_{-1}(x), f_0(x) \in \mathsf{K}[x]$, $f_{-1} \neq 0$, $f_0 \neq 0$. For all i with $1 \leq i \leq k$, the Euclidean polynomial remainder sequence, is defined by

$$f_i = f_{i-2} - q_i f_{i-1}, \quad \deg(f_{i-1}) > \deg(f_i), \quad f_{k+1} = 0.$$

Where $f_i, q_i \in \mathsf{K}[x]$ are the ith remainder and quotient respectively. Note that $f_k = \gcd(f_{-1}, f_0) \neq 0$.

The Extended Euclidean Scheme maintains multipliers $s_i(x), h_i(x) \in \mathsf{K}[x]$ where

$$\begin{aligned} s_i f_{-1} + h_i f_0 &= f_i \\ s_{i-2} - q_i s_{i-1} &= s_i \\ h_{i-2} - q_i h_{i-1} &= h_i \end{aligned}$$

where $s_{-1} = h_0 = 1, s_0 = h_{-1} = 0$. It follows by induction on i that for all $1 \leq i \leq k+1$,

$$\begin{aligned} s_i h_{i-1} - s_{i-1} h_i &= (-1)^{i+1} \\ \gcd(s_i, h_i) &= 1, \\ \deg(f_0) - \deg(f_{i-1}) &= \deg(s_i) \\ \deg(f_{-1}) - \deg(f_{i-1}) &= \deg(h_i). \end{aligned}$$

Note that if $\deg(f-1) < \deg(f_0)$ then $q_1 = 0$, and hence $h_1 = 0$ is designated to be of degree $\deg(f_{-1}) - \deg(f_0) < 0$.

Lemma 1 *Let $g(x) = \gcd(s_j, f_j)$, $0 \leq j \leq n-1$ in the Extended Euclidean Scheme*

$$s_j f_{-1} + h_j x^{2n-1} = f_j$$

with $\deg(f_{-1}) \leq 2n-2$. Then either $g(x) = 1$ or $g(x) = x^\beta$ where $1 \leq \beta < 2n-1$.

Proof. Suppose $g(x) = \gcd(f_j, s_j)$. Rearranging the the scheme, since $g(x)$ divides the left hand side of $s_j f_{-1} - f_j = h_j x^{2n-1}$, $g(x)$ divides $h_j x^{2n-1}$. However $\gcd(s_j, h_j) = 1$ so $g(x)$ divides x^{2n-1}. Therefore $g(x) = 1$ or $g(x) = x^\beta$ and $1 \leq \beta < 2n-1$. □

Lemma 2 *Let $S(x), T(x)$, $F(x) \in \mathsf{K}[x]$ be such that for some j with $0 \leq j \leq k$,*

$$\begin{aligned} S f_{-1} + T f_0 &= F, \\ \deg(S) &< \deg(f_0) - \deg(f_j), \\ \deg(F) &< \deg(f_{j-1}). \end{aligned}$$

Then there exists a polynomial $w(x) \in \mathsf{K}[x]$ such that

$$F = w\, f_j, \; S = w\, s_j, \; \text{and } T = w\, h_j.$$

Proof. By induction on the degree of $F(x)$. If $\deg(F) < \deg(f_k)$, then $F = 0$ since F must be divisible by $f_k = \gcd(f_{-1}, f_0)$. Thus

$$S \frac{f_{-1}}{f_k} = -T \frac{f_0}{f_k}$$

which implies that f_0/f_k divides S. However, $\deg(f_0) - \deg(f_k) \geq \deg(f_0) - \deg(f_j) > \deg(S)$, which means that $S = 0$, and therefore also $T = 0$. In this case the statement holds with $w = 0$. Now, let $\deg(F) = \deg(f_l) + e$ with $j \leq l \leq k$ and $0 \leq e < \deg(f_{l-1}) - \deg(f_l)$. If $Q(x)$ is the polynomial quotient of $F(x)$ and $f_l(x)$, we have

$$\underbrace{(S - Q s_l)}_{=\widehat{S}} f_{-1} + \underbrace{(T - Q h_l)}_{=\widehat{T}} f_0 = \underbrace{F - Q f_l}_{=\widehat{F}}.$$

The polynomials $\widehat{S}, \widehat{T}$, and $\widehat{F}$, now satisfy the conditions of the lemma with l in place of j. In particular,

$$\begin{aligned} \deg(\widehat{S}) &= \max\{\deg(S), \deg(f_0) - \deg(f_{l-1}) + e\} \\ &< \deg(f_0) - \deg(f_l), \end{aligned}$$

and $\deg(\widehat{F}) < \deg(f_l) < \deg(f_{l-1})$. Because $\deg(\widehat{F}) < \deg(F)$, the induction hypothesis can be applied to the triple $\widehat{S}, \widehat{T}, \widehat{F}$, leading to the existence of a polynomial $\widehat{w}$ such that

$$\widehat{S} = \widehat{w}\, s_l, \; \widehat{T} = \widehat{w}\, h_l, \text{ and } \widehat{F} = \widehat{w}\, f_l.$$

Since $\deg(\widehat{F}) < \deg(f_l)$, the last of the above equalities implies that $\widehat{w} = 0$. It remains to prove that $l = j$; suppose that $l > j$, that is, $\deg(f_j) \geq \deg(f_{l-1})$. Then $\deg(S) < \deg(f_0) - \deg(f_j) \leq \deg(f_0) - \deg(f_{l-1}) \leq \deg(Q s_l)$, which contradicts $S - Q s_l = \widehat{w} s_l = 0$. □

Note that Lemma 2 remains true for $j = k+1$ with $w = 0$. Again $\deg(f_{k+1})$ can be set to any integer ≤ 0.

We now treat a special case of Lemma 2. Let

$$\mathcal{F}(x) = a_0 + a_1 x + a_2 x^2 + \cdots \in \mathsf{K}[[x]]$$

be a power series over K, and define

$$\mathcal{F}_n(x) = \mathcal{F}(x) \bmod x^{n+1} = a_0 + a_1 x + \cdots + a_n x^n \in \mathsf{K}[x]$$

be the part truncated at order $n+1$, $n \geq 0$. For each pair of non-negative integers d and e, consider the problem of solving the congruence equation

$$G \equiv H \mathcal{F}_{d+e} \bmod x^{d+e+1}, \tag{3}$$

where $G, H \in \mathsf{K}[x]$, $\deg(G) \leq d$, $\deg(H) \leq e$, and $H \neq 0$.

Lemma 3 *For any pair $d \geq 0$ and $e \geq 0$, and any $\mathcal{F}_{d+e}(x) \in \mathsf{K}[x]$, there exists a solution G, H to equation (3). Furthermore, if G_2, H_2 is another solution to equation (3), then $G/H = G_2/H_2$.*

Proof. Let $f_{-1}(x) = \mathcal{F}_{d+e}(x)$ and $f_0(x) = x^{d+e+1}$; note that $\deg(f_0) = d + e + 1$. If $f_{-1} = 0$, we must have $G = 0$, which with $H = 1$ solves (3). In that case $G/H = 0$. Assume now that $f_{-1} \neq 0$ and consider the polynomial remainder f_j of f_{-1} and f_0, $1 \leq j \leq k+1$, whose degree satisfies $\deg(f_j) \leq d < \deg(f_{j-1})$. Since $f_{k+1} = 0$, such a remainder can always be found. We have

$$s_j f_{-1} \equiv f_j \bmod f_0, \quad \deg(s_j) = \deg(f_0) - \deg(f_{j-1}) \leq e.$$

Also, $s_j \neq 0$, because $\deg(s_j) > 0$ for $j > 1$ and $s_1 = 1$. Therefore $G = f_j$ and $H = s_j$ solve (3). For any pair G_2, H_2 solving (3), there exists a polynomial H_2 such that

$$H_2 f_{-1} + H_2 f_0 = G_2,$$

where $\deg(G_2) \leq d < \deg(f_{j-1})$, and where $\deg(H_2) \leq e < \deg(f_0) - \deg(f_j)$. By Lemma 2, there exists a $w(x) \in \mathsf{K}[x]$ such that $G_2 = wf_j$ and $H_2 = ws_j$, proving $G_2/H_2 = f_j/s_j$, which is thus uniquely determined. □

Therefore, for every $\mathcal{F}(x) \in \mathsf{K}[[x]]$ there exists an infinite matrix of rational functions $p_{d,e}(x) \in \mathsf{K}(x)$, $d, e \geq 0$, that correspond to G/H in (3). This matrix is referred to as the Padé table of $\mathcal{F}(x)$. Computing $p_{d,e}$ as f_j/s_j essentially fills in the entries

$$p_{d+e,0}, p_{d+e-1,1}, \ldots, p_{d,e}, \ldots, p_{0,d+e},$$

in that order. This is the Kronecker algorithm for completing the Padé table. Further details can be found in (Gragg, 1972).

3 Subresultants

Let $G, H \in \mathsf{K}[x], \deg(G) = m, \deg(H) = l$. The jth subresultant of G and H is a polynomial of formal degree j, defined as the determinant $S_j(G, H)$ given by

$$\begin{vmatrix}
g_m & \cdots & g_0 & & & x^{l-j-1}G \\
& \ddots & & \ddots & & \\
& g_m & & & g_0 & \vdots \\
& & \ddots & & \vdots & \\
& & g_m & \cdots & g_{j+1} & G \\
h_l & \cdots & h_{j+1} & \cdots\ h_0 & & x^{m-j-1}H \\
& \ddots & & \ddots & \ddots & \\
& h_l & & h_{j+1} & h_0 & \vdots \\
& & \ddots & & \ddots & \\
& & h_l & \cdots & h_{j+1} & H
\end{vmatrix}.$$

From this, it can be shown that

$$S_j = U_j G + V_j H$$

with $U_j, V_j \in \mathsf{K}[x]$ and $\deg(U_j) \leq l - j - 1, \deg(V_j) \leq m - j - 1$. Corresponding to the Euclidean remainder sequence $(f_1, f_2, \ldots, f_k)$ where $f_{-1} = G(x)$ and $f_0 = H(x)$ and $\gcd(G, H) = f_k$, is a chain $(S_{i_1}, \ldots, S_{i_k})$ of subresultants, where the remainder f_l and the subresultant S_{i_l} are identical upto multiplication by a constant from $\mathbb{F}_q$. This can be seen from the following theorem.

Theorem 1 *Let* D *denote an integral domain, let* $f_1, f_2 \in \mathsf{D}[x]$ *and let*

$$\alpha_i f_{i-2} = q_i f_{i-1} + \beta_i f_i$$

with $\deg(f_i) = \eta_i < \eta_{i-1}$; $\delta_{i-2} = \eta_{i-2} - \eta_{i-1}$; $c_{i-1} = \mathrm{ldcf}(f_{i-1})$; $\alpha_i, \beta_i \in \mathrm{QF}(\mathsf{D})$; $q_i \in \mathrm{QF}(\mathsf{D})[x]$. *Let* k *be such that* $f_{k+1} = 0$ *and let* $S_j(f_1, f_2)$ *denote the* jth *subresultant of* f_1 *and* f_2. *Then for* $i = 3, \ldots, k$

$$\begin{aligned}
S_{\eta_{i-1}-1}(f_1, f_2) &= \gamma_i f_i \quad \text{with} \quad 0 \neq \gamma_i \in \mathrm{QF}(\mathsf{D}) \\
S_{\eta_i}(f_1, f_2) &= \theta_i f_i \quad \text{with}
\end{aligned}$$

$$\begin{aligned}
\theta_i &= (-1)^{\tau_i} c_{i-1}^{\delta_{i-1}-1} \prod_{l=3}^{i} c_{l-1}^{\delta_{l-2}+\delta_{l-1}} \left(\frac{\beta_l}{\alpha_l}\right)^{\eta_{l-1}-\eta_i} \\
\text{and} & \\
\tau_i &= \sum_{l=3}^{i} (\eta_{l-2} - \eta_i)(\eta_{l-1} - \eta_i) \\
S_j(f_1, f_2) &= 0 \quad \text{for both } \eta_{i-1} - 1 > j > \eta_i \text{ and } \eta_k > j \geq 0
\end{aligned}$$

Proof. See (Brown and Traub, 1971) □

The reason for introducing subresultants is that when $S_{n-1}\left(\mathcal{T}(x), x^{2n-1}\right)$ is written out as a polynomial in x, the coefficients are certain minors of S_{n-1} and in particular, the leading coefficient is $\det(T_n)$. We now present an alternative proof for the theorem of Brent *et al.* (1980).

Theorem 2 *Let* T_n *be an* $n \times n$ *Toeplitz matrix over* K *and let* $\mathcal{T}_n(x)$ *be its associated polynomial. With* $f_{-1}(x) = \mathcal{T}_n(x)$, $f_0(x) = x^{2n-1}$, *let* $0 \leq \mu \leq k$ *be that index where* $\deg(f_{\mu-1}) > n - 1 \geq \deg(f_\mu)$ *in the Extended Euclidean Scheme*

$$s_j f_{-1} + t_j f_0 = f_j, \quad \gcd(f_{-1}, f_0) = f_k.$$

T_n *is nonsingular if and only if* $\deg(f_\mu) = n - 1$.

Proof. Let $(f_1, f_2, \ldots, f_k, 0)$ be the remainders obtained by applying the Extended Euclidean algorithm with $f_{-1} = \mathcal{T}_n(x)$ and $f_0 = x^{2n-1}$. Let $\eta_i = \deg(f_i), i = 0, \ldots, k$ and consider $S_{n-1}(f_0, f_{-1})$ as a polynomial in x. Then

$$\begin{aligned}
S_{n-1}(f_0, f_{-1}) &= \sum_{i=0}^{2n-2} \mathrm{Det}(\mathcal{M}_{i,n-1}) x^i \\
&= \sum_{i=0}^{n-1} \mathrm{Det}(\mathcal{M}_{i,n-1}) x^i
\end{aligned}$$

where $\mathcal{M}_{i,j}$ is the matrix obtained after replacing the last column of the matrix shown in the definition of S_j, with the vector $[g_{i+j-l+1}, \ldots, g_i, h_{i+j-m+1}, \ldots, h_i]^{\mathrm{tr}}$. The second equation due to the fact that for $i > j$, $\mathcal{M}_{i,j}$ has two repeated columns and $\det(\mathcal{M}_{i,j}) = 0$

The leading coefficient of $S_{n-1}(f_0, f_{-1})$ is the determinant of $\mathcal{M}_{n-1,n-1}$ which is the matrix

$$\begin{bmatrix}
1 & 0 & \cdots & 0 & & & 0 \\
& \ddots & & & \ddots & & \vdots \\
& & 1 & & & & 0 \\
& & & \ddots & & & \vdots \\
0 & & \cdots & 1 & 0 & \cdots & 0 \\
a_0 & & & \cdots & a_{n-1} & & a_{2n-2} \\
& \ddots & & & & & \\
& & a_0 & & \vdots & \ddots & \vdots \\
& & & \ddots & & & \\
& & & & a_0 & \cdots & a_{n-1}
\end{bmatrix}$$

where T_n^{tr} is the $n \times n$ submatrix in the bottom right corner. Expansion of the determinant along the top rows shows that $\det(\mathcal{M}_{n-1,n-1}) = \det(T_n)$. If $\mathrm{Det}(T_n) = 0$ then

$\deg(S_{n-1}) < n-1$. By theorem 1, there is no i, where $2 \le i \le k$ for which $\deg(f_i) = n-1$. In other words, $\deg(f_{\mu-1}) > n-1 > \deg(f_\mu)$. Hence $\deg(f_\mu) < n-1$. Conversely if $\deg(f_\mu) < n-1$ then $\deg(f_{\mu-1}) - \deg(f_\mu) \ge 2$. From theorem 1 it follows that $\mathrm{ldcf}(S_{n-1}) = 0 = \mathrm{Det}(T_n)$. □

4 The Counting Lemma

Theorem 2 establishes a link from non-singular Toeplitz matrices to remainders in a Euclidean reduction scheme. In particular, T_n is non-singular if $\deg(f_\mu) = n-1$. We now seek a link in the opposite direction. Is it possible to construct a non-singular Toeplitz matrix for a given triple (f_μ, s_μ, h_μ) from some valid Euclidean scheme? In fact, we shall be interested in the number of different polynomials $\mathcal{T}_n(x)$ whose $(n-1, n-1)$ Padé approximant is $F(x)/S(x)$ for a given pair (F, S). We will then restrict ourselves to only those $\mathcal{T}_n(x)$ that are non-singular.

Lemma 4 (Counting Lemma) *Let $\hat{f}(x), \hat{s}(x) \in \mathbb{F}_q[x]$ be such that $\deg(\hat{f}) \le n-1$, $\deg(\hat{s}) \le \deg(\hat{f})$ and $\hat{s}(0) \ne 0$. Let $\beta = n-1-\deg(\hat{f})$, also let $F = x^\beta \hat{f}$ and $S = x^\beta \hat{s}$. If $\beta = 0$ then there is exactly one polynomial $\mathcal{T}_n(x)$ that satisfies*

$$S\mathcal{T}_n \equiv F \bmod x^{2n-1}$$

subject to $\gcd(S, H) = 1$. If $\beta \ge 1$, then there are $(q-1)q^{\beta-1}$ polynomials $\mathcal{T}_n$ that satisfy this congruence. Furthermore, these polynomials are identical in all but their β highest-order coefficients.

Proof. Suppose $\hat{f}$ and $\hat{s}$ are two relatively prime polynomials in $\mathbb{F}_q[x]$ with $\deg(\hat{f}) \le n-1$, $\deg(\hat{s}) \le \deg(\hat{f})$ and $\hat{s}(0) \ne 0$. Let $F = x^\beta \hat{f}$ and $S = x^\beta \hat{s}$ where $\beta = n-1-\deg(\hat{f})$ and consider solving

$$Sf_{-1} + Hx^{2n-1} = F \tag{4}$$

subject to $\gcd(S, H) = 1$, for H and f_{-1} in $\mathbb{F}_q[x]$. By lemma 2, $F = wf_\kappa, S = ws_\kappa$, and $H = wt_\kappa$, for some $0 \le \kappa < k$ in the extended Euclidean scheme for f_{-1} and x^{2n-1}, where $\gcd(f_{-1}, f_0) = f_k$. Since S and H are relatively prime, $w(x) = 1$. From this, f_{-1} is the solution to the congruence

$$Sf_{-1} \equiv F \bmod x^{2n-1} \tag{5}$$

and not a solution to equation (5) modulo $x^{2n-1-\beta}$ for $\beta \ge 1$.

By theorem 2, $\deg(f_\kappa) = n-1$ if and only if $\mathcal{T}_n(x)$ is non-singular in the scheme where $f_{-1}(x) = \mathcal{T}_n(x)$. Hence the pair $(\hat{f}, \hat{s})$, corresponds to some non-singular T_n.

Now let $S = \sum_{i=0}^{n-1} \sigma_i x^i, H = \sum_{i=0}^{n-2} \tau_i x^i, F = \sum_{i=0}^{n-1} \gamma_i x^i$, and let $\mathcal{T}_n(x) = \sum_{i=0}^{2n-2} a_i x^{2n-2-i}$. Comparison of the coefficients of x^i for $0 \le i \le 3n-3$ yields the following system of $3n-2$ equations in $3n-2$ unknowns:

$$\begin{bmatrix} \sigma_0 & 0 & \cdots & & 0 & 0 \\ \vdots & \ddots & 0 & \ddots & & \vdots \\ \sigma_{n-1} & \cdots & \sigma_0 & 0 & 0 & 0 \\ 0 & \sigma_{n-1} & \cdots & \sigma_0 & 0 & 0 \\ & & \ddots & & \ddots & \vdots \\ \vdots & & 0 & \sigma_{n-1} & \cdots & \sigma_0 \\ & & & 0 & \sigma_{n-1} & \vdots \\ 0 & \cdots & & & 0 & \sigma_{n-1} \end{bmatrix} \vec{a} = \begin{bmatrix} \gamma_0 \\ \vdots \\ \gamma_{n-1} \\ 0 \\ \vdots \\ 0 \\ -\tau_0 \\ \vdots \\ -\tau_{n-2} \end{bmatrix} \tag{6}$$

where $\vec{a} = [a_{2n-2}, a_{2n-1}, \ldots, a_1, a_0]^{\mathrm{tr}}$. If $\beta = 0$, the block consisting of the first $2n-1$ equations has a lower triangular coefficient matrix of full rank since the diagonal element σ_0 is non-zero. Thus there is a unique solution vector $\vec{a}$. The unknowns $\tau_0, \ldots, \tau_{n-1}$ can be found by forward substitution.

If $\beta = 1$, then $\sigma_0 = \gamma_0 = 0$ but $\tau_0 \ne 0$, otherwise $\gcd(S, H) \ne 1$ and one of the conditions (see lemma 1) of the extended Euclidean scheme is violated. The system of equation (6) reduces to

$$\begin{bmatrix} \sigma_1 & 0 & \cdots & & 0 & 0 \\ \vdots & \ddots & 0 & & & \vdots \\ \sigma_{n-1} & \cdots & \sigma_1 & 0 & 0 & 0 \\ 0 & \sigma_{n-1} & \cdots & \sigma_1 & 0 & 0 \\ & & \ddots & & \ddots & \vdots \\ \vdots & & 0 & \sigma_{n-1} & \cdots & \sigma_1 \end{bmatrix} \vec{a} = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_{n-1} \\ 0 \\ \vdots \\ 0 \\ -\tau_0 \end{bmatrix}$$

These $2n-2$ equations involving unknowns $a_1, \ldots, a_{2n-2}$ (obtained by comparing the coefficients of $x, x^2, \ldots, x^{2n-2}$ in equation (4) form a full-rank, lower triangular system which can be solved to yield $[a_{2n-2}, \ldots, a_1]^{\mathrm{tr}}$ uniquely. The coefficient a_0 is found in the $(2n)$th equation which is of the form

$$\sigma_1 a_0 = -\tau_0 + c$$

where $c \in \mathbb{F}_q$ is determined by $a_1, \ldots, a_{2n-2}$. There are $q-1$ possible choices for τ_0 and hence $q-1$ polynomials $\mathcal{T}_n(x)$ which match in all coefficients but a_0.

Generalizing for $\beta \ge 1$. We have $\sigma_0 = \cdots = \sigma_{\beta-1} = 0$ and $\gamma_0 = \cdots = \gamma_{\beta-1} = 0$, and $\tau_0 \ne 0$. The first $2n-1-\beta$ equations of the system

$$\begin{bmatrix} \sigma_\beta & 0 & \cdots & & 0 & 0 \\ \vdots & \ddots & & \ddots & & \vdots \\ \sigma_{n-1} & \cdots & \sigma_\beta & & 0 & 0 \\ 0 & \sigma_{n-1} & \cdots & \sigma_\beta & 0 & 0 \\ & & \ddots & & \ddots & \vdots \\ \vdots & & 0 & \sigma_{n-1} & \cdots & \sigma_\beta \end{bmatrix} \vec{a} = \begin{bmatrix} \gamma_1 \\ \vdots \\ 0 \\ -\tau_0 \\ \vdots \\ -\tau_{\beta-1} \end{bmatrix}$$

involving unknowns $a_\beta, \ldots, a_{2n-2}$ is of full rank since it is lower triangular with diagonal element, $\sigma_\beta \ne 0$. Hence $a_{2n-2}, \ldots, a_\beta$ are unique. The next β equations are of the form

$$\sigma_{\beta+i-1} a_{\beta-i-1} = -\tau_i + c_i$$

where $i = 0, \ldots, \beta-1$ and $c_i \in \mathbb{F}_q$. It is clear that $a_{\beta-1}$ depends upon the value of τ_0, for which there are $q-1$ possible choices. For each of $\tau_1, \ldots, \tau_{\beta-1}$ there are q choices.

Hence there are $(q-1)q^{\beta-1}$ different solution vectors $\vec{a}$. □

Our strategy for counting non-singular Toeplitz matrices is to find the number of pairs (F,S) which are Padé Approximants to a non-singular $\mathcal{T}_n$. By theorem 2, $\deg(F)=n-1$, and we must have $\deg(S)\le\deg(F)$. If $\gcd(F,S)\neq 1$ we can apply lemma 4. Finally we will take a weighted sum of the counts. This discussion is summarized in the corollary below.

Corollary 1 *Let* $N_n = \mathrm{card}(\{T_n \mid T_n \text{ is non-singular}\})$. *Let* $\mathcal{P}_i$ *be the set of all polynomial pairs* $(x^i\hat{g}, x^i\hat{h})$ *such that* $\deg(\hat{g})=n-i-1$, $\deg(\hat{h})\le\deg(\hat{g})$, $\hat{h}(0)\neq 0$, *and with* $\hat{g},\hat{h}\in\mathsf{K}[x]$. *Then*

$$N_n = \mathrm{card}(\mathcal{P}_0) + \sum_{\beta=1}^{n-1}(q-1)q^{\beta}\mathrm{card}(\mathcal{P}_\beta).$$

□

5 Count of Non-Singular Toeplitz Matrices

Once again, let $\mathbb{F}_q$ be a finite field with q elements where q is a power of a prime, and let $\mathbb{F}_q[x]$ denote the polynomial ring over $\mathbb{F}_q$ in the indeterminate x. For $r,s,b\in\mathsf{N}, 0\le m,b\le r$ let $P_r=\{g\in\mathbb{F}_q[x] \mid \deg(g)=r\}$ and $\widetilde{P}_r=\{g \mid g\in P_r \text{ and } g(0)\neq 0\}$. Let $C_{r,m}=\mathrm{card}(\Gamma_{r,m})$, $D_{r,m}=\mathrm{card}(\Delta_{r,m})$ and $M_{r,b}=\mathrm{card}(\Omega_{r,b})$ where

$$\begin{aligned}
\Gamma_{r,m} &= \{(u,v)\in P_r\times\widetilde{P}_m \mid \gcd(u,v)=1\}\\
\Delta_{r,m} &= \{(u,v)\in \widetilde{P}_r\times\widetilde{P}_m \mid \gcd(u,v)=1\}\\
\Omega_{r,b} &= \{(u,v)\in P_{r-b}\times\widetilde{P}_k \mid \gcd(u,v)=1 \text{ and } 0\le k\le r-b\}
\end{aligned}$$

When $d=0$, both u and v are constant polynomials and either $u=1$ or $v=1$. Consequently $D_{0,0}=q-1$. For $1\le m\le r$ we have

$$\begin{aligned}
D_{r,0} &= (q-1)^2q^{r-1} \quad \text{and}\\
D(r,r) &= (q-1)^2(q^{2r}-q^{2r-1}-2)/(q+1) \quad \text{and}\\
D(r,m) &= q^{r-1}(q-1)^3(q^{2m}-1)/(q^{m+1}+q^m), \qquad (7)
\end{aligned}$$

where we have made use of the following result:

Theorem 3 *Let* $1\le m\le r$ *and* (u,v) *be uniformly distributed in* $\widetilde{P}_r\times\widetilde{P}_m$. *Then we have* $\Pr[\gcd(u,v)=1]$

$$= \begin{cases}(1-1/(p+1))(1-p^{-2m}) & \text{if } r>m\\ (1-1/(p+1))(1-2p^{1-2m})/(p-1)) & \text{if } r=m.\end{cases}$$

Proof. See Ma and Gathen (1990). □

We will now determine the total number of non-singular T_n over $\mathbb{F}_q$. For each β with $0\le\beta\le n-1$ we will count the $M_{n-1,\beta}$ pairs of relatively prime $(x^\beta\hat{u}, x^\beta\hat{v})$ for which $\deg(\hat{u})=n-1-\beta, \deg(\hat{v})\le\deg(\hat{u})$, and $\hat{v}(0)\neq 0$. Then we will apply lemma 4 and take the sum over all d with $\beta=n-1-d$.

We will need to count the total number of pairs $C_{r,m}$ of relatively prime $(x^i\bar{u},\bar{v})\in\mathbb{F}_q[x]$ for which $\deg(\bar{u})+i=r$, $\deg(\bar{v})=m$, and $\bar{v}(0)\neq 0$. We will then sum over all $0\le i\le r$. Note that the formulas from theorem 3 which give us the values of $D_{r,s}$ are applicable only when $\bar{u}(0)\neq 0$ and $\bar{v}(0)\neq 0$. Thus

$$\begin{aligned}
C_{r,m} &= \sum_{i=0}^{r} D_{i,m}\\
&= \left(\sum_{i=m+1}^{r} D_{i,m}\right) + D_{m,m} + \left(\sum_{j=1}^{m-1} D_{j,m}\right) + D_{0,m}\\
&= \left(\sum_{i=m+1}^{r} D_{i,m}\right) + D_{m,m} + \left(\sum_{j=1}^{m-1} D_{m,j}\right) + D_{m,0}\\
&= q^{r-m}(q-1)(q^{2m}-1). \qquad (8)
\end{aligned}$$

where for the purpose of counting, $D_{0,m}=D_{m,0}$. It follows that

$$\begin{aligned}
M_{r,\beta} &= \sum_{d=0}^{r-\beta} C_{r-\beta,d}\\
&= (q-1)q^{r-\beta} + \sum_{d=1}^{r-\beta} C_{r-\beta,d}\\
&= (1+q^{2r-2\beta+1})(q-1)/(q+1) \qquad (9)
\end{aligned}$$

We are now able to prove our main result.

Theorem 4 *Let* $\mathbb{F}_q$ *be a finite field with* q *elements where* q *is a power of a prime. The number of non-singular* $n\times n$ *Toeplitz matrices over* $\mathbb{F}_q$ *is* $(q-1)q^{2n-2}$.

Proof. Let $N_n=\mathrm{card}(\{T_n \mid T_n \text{ is non-singular}\})$. Applying corollary 1 to lemma 4 we count the $M_{n-1,\beta}$ pairs of relatively prime $(x^\beta\hat{u}, x^\beta\hat{v})$ for which $\deg(\hat{u})=n-1-\beta$, $\deg(\hat{v})\le\deg(\hat{u})$, and $\hat{v}(0)\neq 0$. This is the geometric sum of a finite number of terms, each of which is a finite geometric sum. Thus

$$\begin{aligned}
N_n &= M_{n-1,0} + \sum_{\beta=1}^{n-1}(q-1)q^{\beta-1}M_{n-1,\beta}\\
&= \left(\sum_{\beta=1}^{n-2}(q-1)q^{\beta-1}M_{n-1,\beta}\right) + \left(\sum_{d=1}^{n-1} C_{n-1,d}\right) +\\
&\quad (q-1)q^{n-1} + (q-1)^2q^{n-2}\\
&= (q-1)\Bigg((2q-1)q^{n-2} + \sum_{\beta=1}^{n-2} q^{\beta-1}M_{n-1,\beta} +\\
&\quad (q^{2n-1}-q^n-q^{n-1}+1)/(q+1)\Bigg)\\
&= (q-1)q^{2n-2}
\end{aligned}$$

This concludes the proof of the theorem. □

Corollary 2 *For* $n>1$ *let* T_n *be an* $n\times n$ *Toeplitz matrix over* $\mathbb{F}_q$. *Further, let the elements in the topmost row and leftmost column of* T_n *be selected uniformly randomly from the elements of* $\mathbb{F}_q$. *Then* T_n *is non-singular with probability* $(1-1/q)$.

Proof. This follows readily from the fact that there is a total of q^{2n-1} matrices T_n out of which $(q-1)q^{2n-2}$ are non-singular. □

An $n \times n$ matrix exhibits Hankel structure if elements along the antidiagonal are equal, and those along each line parallel to the antidiagonal, are equal. Thus a Hankel matrix is a Toeplitz matrix whose columns have been re-arranged. The properties of Toeplitz matrices are applicable to Hankel matrices after some notational changes. In particular we have the following:

Corollary 3 *There are $(q-1)q^{2n-2}$ non-singular $n \times n$ Hankel matrices H_n over $\mathbb{F}_q$. Furthermore let the elements in the topmost row and rightmost column be selected uniformly randomly from the elements of $\mathbb{F}_q$. Then H_n is non-singular with probability $(1-1/q)$.* □

6 Count of Toeplitz Matrices with Generic Rank Profile

Now let $T_n = (t_{i-j})$, $i, j = 1, \ldots, n$ have Toeplitz structure as in equation (1). For notational convenience we denote by D_k the determinant of the $k \times k$ leading principal submatrix of T_n.

We say that a matrix $A \in \mathsf{K}^{n\times n}$ has *generic rank profile* if $\mathrm{rank}(A) = r \leq n$ and if $\mathrm{rank}(A_k) = k$, where A_k is that leading principal submatrix of A consisting of the first k rows and columns of A for $k = 1, \ldots, r$. The matrix A has *generic rank* r if A_r has generic rank profile. The following fact is a consequence of the well-known identity of Sylvester (Gantmacher,1990).

Lemma 5 *Let $A \in \mathsf{K}^{n\times n}$ and let L_t, R_t, L_b, R_b denote respectively the $(n-1) \times (n-1)$ submatrices at the left top, right top, left bottom and right bottom, corners of A. Let M_c be the central $(n-2) \times (n-2)$ submatrix obtained by deleting the first and last rows and first and last columns of A. Then*

$$\mathrm{Det}(A)\mathrm{Det}(M_c) = \mathrm{Det}(L_t)\mathrm{Det}(R_b) - \mathrm{Det}(R_t)\mathrm{Det}(L_b).$$

Proof. Let $\mathrm{Det}(A_k) = \begin{vmatrix} 1 & 2 & \ldots & k \\ 1 & 2 & \ldots & k \end{vmatrix}$ denote the $k \times k$ leading principal minor of A. Let $b_{s,t} = \begin{vmatrix} 1 & 2 & \ldots & k & s \\ 1 & 2 & \ldots & k & t \end{vmatrix}$, $s, t = k+1, \ldots, n$, be the minor obtained by bordering A_k by components of the s^{th} row and t^{th} column of A. Denote the matrix formed by the $b_{i,j}$ by $B = (b_{i,j})_{i,j=k+1}^{n}$. Then Sylvester's identity (also attributable to C. L. Dodgson) states that

$$\mathrm{Det}(B) = (\mathrm{Det}(A_k))^{n-k-1} \cdot \mathrm{Det}(A).$$

Our desired result follows by substituting $n-1$ for the value of k. □

Lemma 6 *Let $T_r \in {\mathbb{F}_q}^{r\times r}$ be a Toeplitz matrix with generic rank r. Let N_r denote the number of such T_r. Then,*

$$N_r = (q-1)\left(q^2 - q + 1\right)^{r-1}.$$

Proof. For $r \leq 2$ the result is clear. Assume $r \geq 3$. Let $T_r^{(x,y)}$ denote

$$T_r^{(x,y)} = \begin{bmatrix} t_0 & t_{-1} & \ldots & t_{2-r} & y \\ t_1 & t_0 & \ldots & t_{3-r} & t_{2-r} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ t_{r-2} & t_{r-3} & \ldots & t_0 & t_{-1} \\ x & t_{r-2} & \ldots & t_1 & t_0 \end{bmatrix}$$

where the leading $(r-1) \times (r-1)$ principal submatrix has generic rank $r-1$. Applying lemma 5 we have

$$\begin{aligned} \mathrm{Det}(T_r^{(x,y)})\mathrm{Det}(T_{r-2}) &= \mathrm{Det}(T_{r-1})\mathrm{Det}(T_{r-1}) - \\ &\quad \mathrm{Det}(R_t)\mathrm{Det}(L_b) \end{aligned}$$

where

$$R_t = \begin{bmatrix} t_{-1} & t_{-2} & \ldots & t_{2-r} & y \\ t_0 & t_{-1} & \ldots & t_{3-r} & t_{2-r} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ t_{r-4} & t_{r-5} & \ldots & t_{-1} & t_{-2} \\ t_{r-3} & t_{r-4} & \ldots & t_0 & t_{-1} \end{bmatrix}$$

and

$$L_b = \begin{bmatrix} t_1 & t_0 & \ldots & t_{4-r} & t_{3-r} \\ t_2 & t_1 & \ldots & t_{5-r} & t_{4-r} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ t_{r-2} & t_{r-3} & \ldots & t_1 & t_0 \\ x & t_{r-2} & \ldots & t_2 & t_1 \end{bmatrix}$$

Thus we may write

$$D_r D_{r-2} = D_{r-1}^2 - ((-1)^{r-1} D_{r-2} y + \alpha)((-1)^{r-1} D_{r-2} x + \beta)$$

where $\alpha, \beta \in \mathbb{F}_q$. Since T_{r-1} has generic rank profile, $D_{r-1} \neq 0$ and $D_{r-2} \neq 0$. Suppose now that $D_r = 0$. Then

$$D_{r-1}^2 = D_{r-2}^2 (y + (-1)^{r-1} D_{r-2}^{-1} \alpha)(x + (-1)^{r-1} D_{r-2}^{-1} \beta),$$

whence

$$x = \frac{(D_{r-1}/D_{r-2})^2}{y + (-1)^{r-1}\alpha/D_{r-2}} + (-1)^r \frac{\beta}{D_{r-2}}.$$

Consider now the first fraction in equation (10). The denominator term becomes 0 for exactly one value of y, and the numerator term is always non-zero. Hence there are $q-1$ pairs (x, y) which give a singular extension to T_{r-1}. Consequently,

$$\begin{aligned} N_r &= \left(q^2 - (q-1)\right) N_{r-1} \\ &= \left(q^2 - (q-1)\right)^2 N_{r-2} \\ &\vdots \\ &= \left(q^2 - (q-1)\right)^{r-1} N_1 \\ &= (q-1)\left(q^2 - q + 1\right)^{r-1}. \end{aligned}$$

This concludes the proof of the lemma. □

Theorem 5 *Let $T_n \in {\mathbb{F}_q}^{n\times n}$ have Toeplitz structure. For $0 < r < n$ the probability that T_n has generic rank r is*

$$p_{r,n} = \frac{1}{q}(1 - \frac{1}{q})^2 \left(1 - \frac{q-1}{q^2}\right)^{r-1}.$$

The probability that T_n has generic rank n is

$$p_{n,n} = (1 - \frac{1}{q})\left(1 - \frac{q-1}{q^2}\right)^{n-1}.$$

Proof.
Let $\mathcal{G}_{r,n} = \Big\{ T_n \mid T_{r+1} \text{ has generic rank } 0 < r < n \Big\}$. Then

$$\begin{aligned}
p_{r,n} &= q^{1-2n} \cdot \text{card}(\mathcal{G}_{r,n}) \\
&= N_r(q-1)q^{2(n-r+1)}q^{1-2n} \\
&= \frac{(q-1)^2}{q^3}\left(1-\frac{q-1}{q^2}\right)^{r-1} \\
&= \frac{1}{q}(1-\frac{1}{q})^2\left(1-\frac{q-1}{q^2}\right)^{r-1}. \\
p_{n,n} &= q^{1-2n} \cdot N_n \\
&= (q-1)q^{2n-2}\left(1-\frac{q-1}{q^2}\right)^{n-1} q^{1-2n} \\
&= (1-\frac{1}{q})\left(1-\frac{q-1}{q^2}\right)^{n-1}.
\end{aligned}$$

This concludes the proof of the theorem □

7 Conclusions

We have shown that there are $(q-1)q^{2n-2}$ non-singular $n \times n$ Toeplitz matrices over a finite field $\mathbb{F}_q$ containing q elements. The probability that an $n \times n$ random Toeplitz matrix is non-singular is $1 - 1/q$ and this value is independent of the dimension. For the field $\mathbb{F}_2$ containing 2 elements, it is $1/2$ exactly. In (Borodin *et al.*, 1982) it is shown for an arbitrary $n \times n$ matrix A_n over $\mathbb{F}_q$ that[2]

$$\Pr[\text{A is non-singular}] = v(1/q, n) = \prod_{1 \le i \le n} (1 - q^{-i}).$$

In particular in $\mathbb{F}_2$, $\lim_{n\to\infty} v(1/2, n) \approx 0.2889$. Thus there is a higher probability of being singular if the $n \times n$ matrix over $\mathbb{F}_q$ is unstructured, than if the matrix has Toeplitz structure.

For matrices with no special structure, it can be shown that $p_{r,n} = (1/q)(1-1/q)^r$, and that $p_{n,n} = (1-1/q)^n$. We conjectured that for $0 < r < n$ the number of $n \times n$ matrices over $\mathbb{F}_q$ with actual rank r is $N_r = (q^2-1)q^{2r-2}$. This last fact was proven by Daykin.

As mentioned earlier these results were obtained in our on-going investigation of the probability of success of the block Wiedemann algorithm for solving linear systems over finite fields of small cardinality. Along the lines of (Borodin *et al.*, 1982) we sought the probability that the matrices $Y = T_n A$ and $W = BT_n'$ over $\mathbb{F}_q$ have generic rank profile. Here A and B are non-singular Toeplitz-like matrices (Gohberg *et al.*, 1986) and T_n and T_n' are square, uniformly random Toeplitz matrices. We wish to put the coefficient matrix into generic rank profile, with the use of Toeplitz preconditioners whose entries are chosen uniformly at random from the field $\mathbb{F}_q$.

In (Kaltofen and Saunders, 1991) the preconditioning is done for Wiedemann's (1986) original coordinate recurrence algorithm with a pair of random, triangular, unimodular Toeplitz matrices whose entries come from an extension field of $\mathbb{F}_q$ of degree $O(\log n)$ over $\mathbb{F}_q$. We are seeking to avoid computing in an extension field.

Theorem (5) indicates that the probability that a randomly selected $n \times n$ Toeplitz matrix has full generic rank is almost $(1-1/q)\cdot e^{(1-n)/q}$. That probability approaches zero as n tends to infinity and leads us to think that the desired rank profile might be unattainable with just a single pair of Toeplitz preconditioners with entries from $\mathbb{F}_q$.

Cascaded Toeplitz preconditioners in the fashion $\mathcal{A} = T_n^{(s)} \cdots T_n^{(1)} \cdot A \cdot \tilde{T}_n^{(1)} \cdots \tilde{T}_n^{(s)}$ where $s > 1$ might be more effective. The pairs $(T_n^{(j)}, \tilde{T}_n^{(j)})$ would perhaps raise the generic rank of A by stages until $\mathcal{A}$ has the desired generic rank profile. Particular attention must be paid to the rank of the preconditioners, for the actual rank of A might be lowered if a random preconditioner is singular. Our results are a resource for further research in this direction.

[2] This result is the restriction to square matrices of a result due to Landesberg (1893) that for $m \times n$ matrices over $\mathbb{F}_q$, the number of matrices of rank r is

$$g(m,n,r) = q^{r(r-1)/2} \prod_{i=1}^{r} \frac{(q^{m-i+1}-1)(q^{n-i+1}-1)}{(q^i-1)}.$$

Literature Cited

Borodin, A., von zur Gathen, J., and Hopcroft, J. E., "Fast parallel matrix and GCD computations," *Inf. Control* **52**, pp. 241–256 (1982).

Brent, R. P., Gustavson, F. G., and Yun, D. Y. Y., "Fast solution of Toeplitz systems of equations and computation of Padé approximants," *J. Algorithms* **1**, pp. 259–295 (1980).

Brown, W. S. and Traub, J. F., "On Euclid's algorithm and the theory of subresultants," *J. ACM* **18**, pp. 505–514 (1971).

Coppersmith, D., "Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm," *Math. Comput.* **62**/205, pp. 333–350 (1994).

Daykin, D. E., "Distribution of bordered persymmetric matrices in a finite field," *J. reine u. angew. Math.* **203**, pp. 47-54 (1960).

Gohberg, I., Kailath, T., and Koltracht, I., "Efficient solution of linear systems of equations with recursive structure," *Linear Algebra Applic.* **80**, pp. 81–113 (1986).

Gantmacher, F., *The Theory of Matrices, Vol. 1*; Chelsea Publ. Co., New York, N.Y., 1990.

Gragg, W. B., "The Padé table and its relation to certain algorithms of numerical analysis," *SIAM Review* **14**/1, pp. 1–62 (1972).

Kaltofen, E., "Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems," *Math. Comput.* **64**/210, pp. 777-806 (1995).

Kaltofen, E. and Saunders, B. D., "On Wiedemann's method of solving sparse linear systems," in *Proc. AAECC-9*, Springer Lect. Notes Comput. Sci. **539**; pp. 29–38, 1991.

Landsberg, G., Über eine Anzahlbestimmung und eine damit zusammenhängende Reihe *J. reine u. angew. Math.* **111**, pp. 87–88 (1893).

Lobo, A., "Matrix-Free Linear System Solving and Applications to Symbolic Computation," in *Ph.D. Thesis*, Dept. Comput. Sci., Rensselaer Polytech. Instit., Troy, New York; (1995).

Ma K., and von zur Gathen, J., "Analysis of Euclidean Algorithms for Polynomials over Finite Fields," *J. Symbolic Computation* **9**, pp. 429–455 (1990).

Wiedemann, D., "Solving sparse linear equations over finite fields," *IEEE Trans. Inf. Theory* IT-**32**, pp. 54–62 (1986).

Erich Kaltofen received both his M.S. degree in Computer Science in 1979 and his Ph.D. degree in Computer Science in 1982 from Rensselaer Polytechnic Institute. He was an Assistant Professor of Computer Science at the University of Toronto and an Assistant, Associate, and full Professor at Rensselaer Polytechnic Institute. Since 1996 he is a Professor of Mathematics at North Carolina State University. His current interests are in computational algebra and number theory, design and analysis of sequential and parallel algorithms, and symbolic manipulation systems and languages. Kaltofen was the Chair of ACM's Special Interest Group on Symbolic & Algebraic Manipulation 1993 - 95. He serves as associate editor on several journals on symbolic computation. From 1985 - 87 he held an IBM Faculty Development Award. From 1990 - 91 he was an ACM National Lecturer. He has contributed 20 papers to ISSAC and its predecessor conferences.

Austin Lobo (B.Tech. EE '81, M.S. ECSE '83, M.S. CSci '93, Ph.D. CSci '95) received his Doctorate from Rensselaer Polytechnic Institute. He has worked for several years as an electrical engineer. He is presently an NSF postdoctoral fellow in Computer Science at the University of Delaware, Newark. His interests are computational linear algebra and applications; the design and implementation of algorithms; and distributed and parallel aspects of symbolic computation.