On the Berlekamp/Massey Algorithm and Counting Singular Hankel Matrices over a Finite Field

Matthew T. Comer

Dept. of Mathematics, North Carolina State University
Raleigh, North Carolina, 27695-8205 USA

Erich L. Kaltofen

Dept. of Mathematics, North Carolina State University
Raleigh, North Carolina, 27695-8205 USA

Abstract

We derive an explicit count for the number of singular $n \times n$ Hankel (Toeplitz) matrices whose entries range over a finite field with q elements by observing the execution of the Berlekamp/ Massey algorithm on its elements. Our method yields explicit counts also when some entries above or on the anti-diagonal (diagonal) are fixed. For example, the number of singular $n \times n$ Toeplitz matrices with 0's on the diagonal is $q^{2n-3} + q^{n-1} - q^{n-2}$.

We also derive the count for all $n \times n$ Hankel matrices of rank r with generic rank profile, i.e., whose first r leading principal submatrices are non-singular and the rest are singular, namely $q^r(q-1)^r$ in the case $r < n$ and $q^{r-1}(q-1)^r$ in the case $r = n$. This result generalizes to block-Hankel matrices as well.

Key words: Toeplitz matrix, Hankel matrix, block matrix, finite field, singularity counts, fixed entry, Berlekamp/Massey algorithm.

⋆ This material is based on work supported in part by the National Science Foundation under Grant CCF-0830347.

Email addresses: mcomer@ncsu.edu (Matthew T. Comer), kaltofen@math.ncsu.edu (Erich L. Kaltofen).

URL: http://www.kaltofen.us (Erich L. Kaltofen).

1. Introduction

Throughout the discussion, entries will be taken from the field $\mathbb{F}_q$ of q elements, and we will identify a square Hankel matrix

$$\begin{bmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & \dots & a_{n-1} & a_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-2} & a_{n-1} & \dots & a_{2n-4} & a_{2n-3} \\ a_{n-1} & a_n & \dots & a_{2n-3} & a_{2n-2} \end{bmatrix} = [a_{i+j-2}]_{i,j=1}^{n}$$

with the list $[a_0, a_1, \dots, a_{2n-2}]$. A Toeplitz matrix is the mirror image $[a_{n+i-j-1}]_{i,j=1}^{n}$.

Our investigation was motivated by the question of Ramamohan Paturi who asked in October 2009 how many Toeplitz matrices over $\mathbb{F}_q$ with zeros on the main diagonal were non-singular. Paturi needed the estimate for circuit satisfiability complexity lower bounds (Paturi and Pudlák, 2010).

David E. Daykin (1960) proved theorems regarding the number of Hankel matrices over a finite field with a specified rank or determinant. Kaltofen and Lobo (1996) established some of Daykin's counts using the extended Euclidean algorithm form of the Berlekamp/ Massey algorithm for polynomials (Sugiyama et al., 1975). Additionally, they gave the number of square Toeplitz matrices with *generic rank profile*. Generic rank profile means that for a matrix A of rank r, the first r leading principal submatrices A_1, ..., A_r are non-singular. We prove analogous results here, albeit with a different approach, for the Hankel case. The counts for Toeplitz and Hankel matrices of generic rank profile are not the same.

The determination of singularity of a Hankel matrix has a natural connection with running the Berlekamp/Massey algorithm on the list $[a_0, a_1, \dots, a_{2n-2}]$, and for this reason we count how many Hankel matrices have zeros along the anti-diagonal in order to answer the question regarding Toeplitz matrices. Kaltofen and Lee (2003) have observed that the Berlekamp/Massey algorithm (Massey, 1969, cf. Theorem 1) detects the non-singular leading principal submatrices of a Hankel matrix from those non-zero discrepancies that increase the linear generator degrees, and that the corresponding sequence elements determine the singularity of the corresponding leading principal submatrices.

We will use this property to partition the space of Hankel matrices into unique correspondences of one singular Hankel matrix to $q-1$ non-singular Hankel matrices. This process generalizes when particular entries of the list $[a_0, \dots, a_{2n-2}]$ are fixed to arbitrary values (such as the case of zeros along the anti-diagonal).

We then investigate the properties of block-Hankel matrices. We cannot answer the analogous question for block-Hankel matrices, but we present some brute-force counts that we have computed with Maple. Last, we follow in the theme of (Kaltofen and Lobo, 1996) by counting block-Hankel matrices with *block generic rank profile*. A block matrix A (of square submatrices of dimension m) of rank mr has block generic rank profile if for $k = 1, 2, \dots, r$, we have $\operatorname{rank}(A_k) = mk$, where A_k is the $k \times k$ block leading principal submatrix of A.

The counts for unblocked rank r Hankel matrices are given in (Garcìa-Armas et al., 2011).

2. Connection with the Berlekamp/Massey algorithm

Given a list of n field elements, $[a_0, \ldots, a_{n-1}]$, the Berlekamp/Massey algorithm will produce for each $r \in \{1, 2, \ldots, n\}$ a monic polynomial

$$\Lambda_r = c_0 + c_1 z + \cdots + c_{L_r-1} z^{L_r-1} + z^{L_r}$$

of minimal degree $L_r \leq r-1$ such that

$$-c_0 a_i - c_1 a_{i+1} - \cdots - c_{L_r-1} a_{i+L_r-1} = a_{i+L_r}, \quad i = 0, 1, \ldots, r - L_r - 1 \tag{1}$$

Such a polynomial is called a *(minimal) generating polynomial*, and L_r is called the *minimal length* required to generate the first r elements of the sequence. Theorem 2 in (Massey, 1969) states that if a polynomial (of minimal degree L_n) generates the list $[a_0, \ldots, a_{n-1}]$ but fails to generate a_n (i.e., equation (1) does not hold for $i = n-L_r$), then the minimal generating polynomial of $[a_0, \ldots, a_n]$ will be of degree $L_{n+1} = n - L_n + 1$.

We visualize the generating polynomials in the following way: for each $r = 1, 2, \ldots, n$, define

$$H_r = \begin{bmatrix} a_0 & a_1 & \ldots & a_{L_r-2} & a_{L_r-1} \\ a_1 & a_2 & \ldots & a_{L_r-1} & a_{L_r} \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ a_{r-L_r-1} & a_{r-L_r} & \ldots & a_{r-1} & a_{r-2} \\ a_{r-L_r} & a_{r-L_r+1} & \ldots & a_{r-2} & a_{r-1} \end{bmatrix}, \quad \lambda_r = \begin{bmatrix} -c_0 \\ -c_1 \\ \vdots \\ -c_{L_r-2} \\ -c_{L_r-1} \end{bmatrix}, \quad h_r = \begin{bmatrix} a_{L_r} \\ a_{L_r+1} \\ \vdots \\ a_{r-1} \\ a_r \end{bmatrix},$$

so that by definition of Λ_r above, we have $H_r \lambda_r = h_r$ (for $r = 1, 2, \ldots, n-1$) except possibly in the last entry (which corresponds to equation (1) for $i = r - L_r$). The last entry of $H_r \lambda_r$ will not be a_r if and only if Λ_r generates $[a_0, \ldots, a_{r-1}]$ but not a_r.

Suppose that $\Lambda_{n'}$ of degree $L_{n'} \leq n'$ generates $[a_0, \ldots, a_{n-1}]$ but not a_n. Then the vector

$$\vec{\Lambda}_{n'} = [-\lambda_{n'} \ 1]^T = [c_{L_{n'}} \ c_{L_{n'}-1} \ \ldots \ c_1 \ 1]^T$$

is a null-space vector of the leading $(n-L_{n'}) \times (L_{n'}+1)$ submatrix of the matrix depicted in Figure 1; the first $L_{n'}$ columns of this submatrix form the first $n - L_{n'}$ rows of H_{n-1}.

As noted above, Theorem 2 in (Massey, 1969) implies that the minimal length required to generate $[a_0, \ldots, a_n]$ is $L_{n+1} = n - L_{n'} + 1$. Thus, H_{n+1} will have $n - L_{n'} + 1$ columns, and in fact, the entire $(n-L_{n'}+1) \times (n-L_{n'}+1)$ leading principal submatrix in Figure 1 will be non-singular. For completeness, we now give those details in the proof of Lemma 2 in (Kaltofen and Yuhasz, 2009), that justify that claim.

If we post-multiply the $(n - L_{n'} + 1) \times (n - L_{n'} + 1)$ leading principal submatrix

$$\begin{bmatrix} a_0 & \ldots & a_{L_{n'}-1} & \ldots & a_{n-L_{n'}} \\ \vdots & \iddots & \vdots & \iddots & \vdots \\ a_{L_{n'}-1} & \ldots & a_{2(L_{n'}-1)} & \ldots & a_{n-1} \\ \vdots & \iddots & \vdots & \iddots & \vdots \\ a_{n-L_{n'}} & \ldots & a_{n-1} & \ldots & a_{2(n-L_{n'})} \end{bmatrix}$$

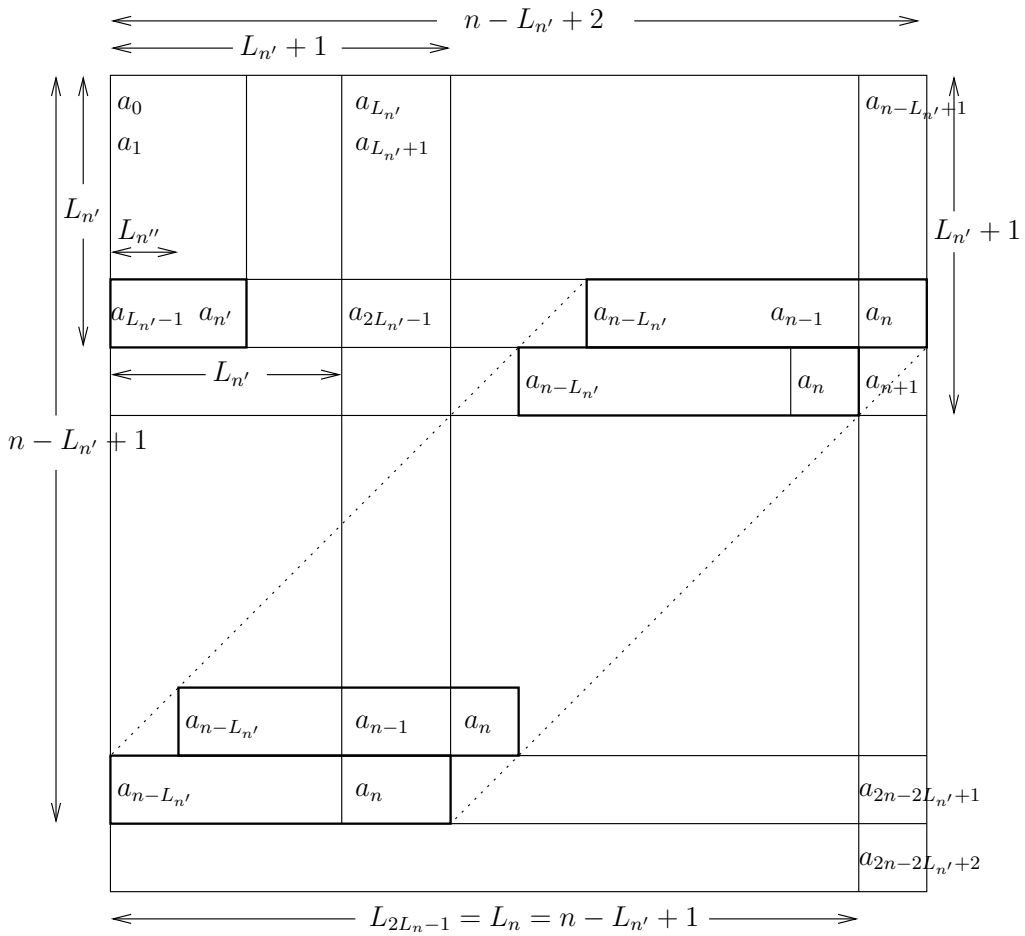

Fig. 1. Berlekamp/Massey algorithm, as seen in (Kaltofen and Lee, 2003)

by

$$\left[\begin{array}{c|ccccc} & c_{L_{n'}} & 0 & \cdots & 0 & 0 \\ & c_{L_{n'}-1} & c_{L_{n'}} & \ddots & \vdots & \vdots \\ I_{L_{n'}} & \vdots & c_{L_{n'}-1} & \ddots & 0 & \vdots \\ & c_1 & \vdots & \ddots & c_{L_{n'}} & 0 \\ \hline & 1 & c_1 & \ddots & c_{L_{n'}-1} & c_{L_{n'}} \\ & 0 & 1 & \ddots & \vdots & c_{L_{n'}-1} \\ 0^{m_1 \times m_2} & \vdots & 0 & \ddots & c_1 & \vdots \\ & \vdots & \vdots & \ddots & 1 & c_1 \\ & 0 & 0 & \cdots & 0 & 1 \end{array}\right], \quad \begin{array}{l} m_1 = n - 2L_{n'} + 1 \\ m_2 = L_{n'} \end{array}, \quad (2)$$

the result is

$$\left[\begin{array}{c|cccccc} \bar{H} & \multicolumn{5}{c}{0^{m_1\times m_2}} \\ \hline & 0 & \cdots & \cdots & 0 & \alpha \\ & \vdots & \iddots & \iddots & \alpha & * \\ \divideontimes & \vdots & 0 & \iddots & * & \vdots \\ & 0 & \alpha & \iddots & \vdots & * \\ & \alpha & * & \cdots & * & * \end{array}\right], \quad \begin{array}{l} m_1 = L_{n'} \\ m_2 = n - 2L_{n'} + 1, \end{array} \quad \alpha \neq 0, \tag{3}$$

where $\bar{H}$ is the $L_{n'} \times L_{n'}$ leading principal submatrix of H and $\alpha \neq 0$ is the last entry of $H_n\lambda_n$. The $(n - L_{n'} + 1) \times (n - L_{n'} + 1)$ leading principal submatrix of H will be non-singular if the above matrix is non-singular, which will happen if $\bar{H}$ is non-singular. This can be shown as a consequence of Lemmas 1 and 2 below.

Lemma 1. *Given a list* $[0, 0, \ldots, 0, \alpha]$ *with* $\alpha \neq 0$ *as the* $(k + 1)$*-st entry, the first* H_r *with* $L_r > 0$ *will be* $H_{k+1} = [0\ 0\ \cdots\ 0\ \alpha]$.

Proof. The Berlekamp/Massey algorithm initializes $\Lambda_0 = 1$, which generates the zero sequence of any length. Thus we have $\Lambda_1 = \cdots = \Lambda_k = 1$ and $L_0 = \cdots = L_k = 0$, where Λ_k generates $a_0, a_1, \ldots, a_{k-1}$ (the zero sequence) but not $a_k = \alpha$. We then have

$$L_{k+1} = \max\{L_k, k - L_k + 1\} = \max\{0, k - 0 + 1\} = k + 1,$$

and $\Lambda_{k+1} = z^{k+1}$.

So for $r \leq k$, H_r is of size $(r - L_r + 1) \times L_r = (r + 1) \times 0$ (i.e., a matrix of $r + 1$ empty rows), and H_{k+1} is of size

$$(k + 1 - L_{k+1} + 1) \times L_{k+1} = (k + 1 - (k + 1) + 1) \times (k + 1) = 1 \times (k + 1),$$

and thus H_{k+1} has the proposed form. □

With H_{k+1} as in Lemma 1, the H_r matrices will keep adding rows until a length change (in the minimal generator) occurs. We can show that a length change will not occur until the H_r matrices "fill-up" the rest of the rows of the $L_{k+1} \times L_{k+1}$ leading principal submatrix of H.

Lemma 2. *Suppose* H_p *is a leading submatrix of rows of the* $L_p \times L_p$ *leading principal submatrix of* H*, and suppose* $L_p = L_{p+1} = \cdots = L_{p+q} < L_{p+q+1}$*. Then* H_{p+q} *will have at least* $L_p + 1$ *rows, and* H_{p+q+1} *will have exactly* $L_p + 1$ *rows.*

Proof. We see that $H_p, H_{p+1}, \ldots, H_{p+q}$ all have the same number of columns, so by the definition of H_r for arbitrary r, these matrices will be formed by augmenting by one row at a time. Also by definition of H_r, we have

$$H_{p+q} = \begin{bmatrix} a_0 & \ldots & a_{L_{p+q}-1} \\ \vdots & \iddots & \vdots \\ a_{p+q-L_{p+q}} & \ldots & a_{p+q-1} \end{bmatrix} = \begin{bmatrix} a_0 & \ldots & a_{L_p-1} \\ \vdots & \iddots & \vdots \\ a_{p+q-L_p} & \ldots & a_{p+q-1} \end{bmatrix}.$$

Because of the length change between L_{p+q} and L_{p+q+1}, we will have

$$\begin{aligned} L_{p+q+1} &= \max\{L_{p+q}, (p+q) - L_{p+q} + 1\} \\ &= (p+q) - L_{p+q} + 1 \\ &= p + q - L_p + 1 \\ &> L_{p+q} = L_p, \end{aligned}$$

so that H_{p+q} will have more than L_p rows. Also, we will have

$$H_{p+q+1} = \begin{bmatrix} a_0 & \dots & a_{L_{p+q+1}-1} \\ \vdots & \iddots & \vdots \\ a_{p+q+1-L_{p+q+1}} & \dots & a_{p+q} \end{bmatrix} = \begin{bmatrix} a_0 & \dots & a_{p+q-L_p} \\ \vdots & \iddots & \vdots \\ a_{L_p} & \dots & a_{p+q} \end{bmatrix},$$

so that H_{p+q+1} will have $L_p + 1$ rows. □

Corollary 3. *If $L_{r+1} > L_r$, then H_{r+1} is a leading submatrix of rows of the $L_{r+1} \times L_{r+1}$ leading principal submatrix of H.*

From Lemma 1, it is clear that the first $L_p \times L_p$ leading principal submatrix of H is non-singular (for $L_p > 0$). From Lemma 2, we see that when the next length change occurs, say $L_{p+q+1} > L_p$, H_{p+q} will have at least $L_p + 1$ rows, which corresponds to Λ_p generating $[a_0, \dots, a_{p+q-1}]$ but not a_{p+q}. We can post-multiply the $L_{p+q} \times L_{p+q}$ leading principal submatrix by an appropriate matrix like (2) to obtain a matrix product whose result is analogous to (3). Because $\bar{H}$ here is the $L_p \times L_p$ non-singular leading principal submatrix of H, we have that the $L_{p+q} \times L_{p+q}$ leading principal submatrix of H is non-singular.

Using induction on Lemma 2, we conclude that for all n, the $L_n \times L_n$ leading principal submatrix is non-singular (when $L_n > 0$).

Lemma 4. *Given an $n \times n$ Hankel matrix H, let r be maximal such that $r - L_r + 1 \leq n$ and $L_r \leq n$ (i.e., H_r is a submatrix of H but H_{r+1} is not). Then H_{r+1} will have $n + 1$ rows and at most n columns.*

Proof. We make the convention that if $L_s = 0$ for some s, then H_s has $s - L_s + 1 = s + 1$ empty rows, and is (trivially) a submatrix of H.

If $L_{r+1} = L_r \leq n$, then we will have

$$H_{r+1} = \left[\begin{array}{ccc} a_0 & a_1 \ \ldots & a_{L_{r+1}-1} \\ a_1 & a_2 \ \ldots & a_{L_{r+1}} \\ \vdots & \iddots \ \iddots & \vdots \\ a_{r-L_{r+1}} & \ldots \ \ldots & a_{r-1} \\ \hline a_{r+1-L_{r+1}} & \ldots \ \ldots & a_r \end{array}\right] = \left[\begin{array}{ccc} a_0 & a_1 \ \ldots & a_{L_r-1} \\ a_1 & a_2 \ \ldots & a_{L_r} \\ \vdots & \iddots \ \iddots & \vdots \\ a_{r-L_r} & \ldots \ \ldots & a_{r-1} \\ \hline a_{r+1-L_r} & \ldots \ \ldots & a_r \end{array}\right]$$

$$= \left[\begin{array}{c} H_r \\ \hline a_{r+1-L_r} \ a_{r+1-(L_r-1)} \ \ldots \ a_r \end{array}\right],$$

so that H_{r+1} has $L_{r+1} = L_r \leq n$ columns. By the maximality of r, we must have

$$n < (r+1) - L_{r+1} + 1 = (r - L_r + 1) + 1 \leq n + 1,$$

so H_{r+1} has $n+1$ rows.

If $L_{r+1} > L_r$, then by Theorem 2 in (Massey, 1969) we have $L_{r+1} = r - L_r + 1 \leq n$, so H_{r+1} has at most n columns. Again by the maximality of r, we must have

$$n < (r+1) - L_{r+1} + 1 = (r+1) - (r - L_r + 1) + 1 = L_r + 1 \leq n + 1,$$

so again H_{r+1} has $n+1$ rows. □

Lemma 4 implies the following for any $n \times n$ Hankel matrix H: if we run the Berlekamp/Massey algorithm on the entries of H, then there will be an $r \in \{1, \ldots, 2n-2\}$ such that H_r is a leading submatrix of entire columns of H, and H_{r+1} is obtained by augmenting an appropriate row of entries to H_r, but H_{r+1} is not a submatrix of H.

Definition 5. We will say that the Berlekamp/Massey algorithm *exits* an $n \times n$ Hankel matrix H at r if H_r is a submatrix of H but H_{r+1} is not. We make the convention that if $L_1 = \cdots = L_n = 0$ (so that H_{n-1} is $n \times 0$ and H_n is $(n+1) \times 0$), then we say that the algorithm exits at $n-1$. Also, we use the terminology *exits at* $2n-1$ even though a_{2n-1} is not defined in H.

Lemma 6. *Let H be a square Hankel matrix. If A is a non-singular leading principal submatrix of H, then $H_r = A$ for some $r \geq 1$, when running the Berlekamp/Massey algorithm on the entries of H.*

Proof. Let

$$A = \left[\begin{array}{ccc} a_0 & \ldots & a_{k-1} \\ \vdots & \iddots & \vdots \\ a_{k-1} & \ldots & a_{2k-2} \end{array}\right].$$

Then because A is a square Hankel matrix, Lemma 4 implies that the Berlekamp/Massey algorithm will exit A at one of $k-1, k, \ldots, 2k-1$. Let $m-1$ be that index and suppose

$m-1 \leq 2k-2$. Then we may write

$$H_m = \begin{bmatrix} \tilde{A} \\ y^T \end{bmatrix}_{(m-L_m+1)\times L_m}, \quad h_m = \begin{bmatrix} \tilde{a} \\ \alpha \end{bmatrix}_{(m-L_m+1)\times 1},$$

where $\tilde{A}$ is an appropriate leading submatrix of columns of A, and $\tilde{a}$ is an appropriate column of A. Then we have

$$A = \begin{bmatrix} \tilde{A} & \tilde{a} & B \end{bmatrix},$$

so that

$$\begin{bmatrix} \tilde{A} & \tilde{a} & B \end{bmatrix} \cdot \begin{bmatrix} \lambda_m \\ -1 \\ 0 \end{bmatrix} = 0,$$

hence A is singular, a contradiction.

Thus, we must have that the Berlekamp/Massey algorithm exits A at $2k-1$, so that

$$H_{2k} = \begin{bmatrix} H_{2k-1} \\ y^T \end{bmatrix} = \begin{bmatrix} A \\ y^T \end{bmatrix},$$

hence $H_{2k-1} = A$. □

Corollary 7. *The Berlekamp/Massey algorithm will exit an $n \times n$ Hankel matrix H at one of $n-1, n, \ldots, 2n-2$ if and only if the matrix is singular; the algorithm will exit at $2n-1$ if and only if the matrix is non-singular.*

Proof. By the proof of Lemma 6, the algorithm will exit at $2n-1$ if H is non-singular.

Now suppose that the algorithm exits at $2n-1$. Then H_{2n} will be formed by adding a row to H_{2n-1}, which will be H itself, and we have

$$H_{2n} = \begin{bmatrix} H_{2n-1} \\ y^T \end{bmatrix} = \begin{bmatrix} H \\ y^T \end{bmatrix},$$

so that

$$H = H_{2n-1} = \begin{bmatrix} a_0 & \cdots & a_{L_{2n-1}-1} \\ \vdots & \iddots & \vdots \\ a_{2n-1-L_{2n-1}} & \cdots & a_{2n-2} \end{bmatrix}.$$

We see then that $L_{2n-1} = n$, hence H is $L_{2n-1} \times L_{2n-1}$, and thus non-singular by the proof of Lemma 2 in (Kaltofen and Yuhasz, 2009). □

3. Counting Singular Hankel Matrices

Let $\mathcal{H}^{n\times n}$ denote the set of all $n \times n$ Hankel matrices. We define maps

$$\begin{aligned} \varphi : \mathcal{H}^{n\times n}_{\text{non-singular}} &\to \mathcal{H}^{n\times n}_{\text{singular}} \\ [a_0, \ldots, a_k, \ldots, a_{2n-2}] &\mapsto [a_0, \ldots, a_{k-1}, a'_k, a_{k+1}, \ldots, a_{2n-2}] \end{aligned}$$

and

$$\begin{aligned}\psi : \mathcal{H}^{n\times n}_{\text{singular}} &\to \mathcal{P}(\mathcal{H}^{n\times n}_{\text{non-singular}})\\ [a_0,\ldots,a_k,\ldots,a_{2n-2}] &\mapsto \left\{[a_0,\ldots,a_{k-1},a'_k,a_{k+1},\ldots,a_{2n-2}] \;\middle|\; a'_k \in \mathbb{F}_q \setminus \{a_k\}\right\}\end{aligned}$$

in the following way: we run the Berlekamp/Massey algorithm on the list of entries associated with a Hankel matrix H, and we let k be maximal such that $L_k < n$ and $k - L_k + 1 = n$ (i.e., H_k is a *proper* submatrix of columns of H). Because $L_k < n$, H_{k+1} will exit H if and only if H is singular; H_{k+1} will have $L_{k+1} > L_k$ columns (and remain a submatrix of H) if and only if H is non-singular.

We may factor H as

$$\begin{aligned}\left[H_k \;\; h_k \;\; B\right] &= \left[\begin{array}{cccc|c} a_0 & \cdots & a_{L_{k-1}} & a_{L_k} & \\ \vdots & \iddots & \vdots & \vdots & \\ a_{k-L_k} & \cdots & a_{k-1} & a_k & \end{array}\right. \left. B \right]\\ &= \left[\begin{array}{cc|c} y_0^T & a_{L_k} & \\ \vdots & \vdots & \\ y_{k-L_k}^T & a_k & \end{array}\right. \left. B \right]\end{aligned}$$

where B may be empty, and $H_k\lambda_k - h_k = (0,0,\ldots,0,y_{k-L_k}^T\lambda_k - a_k)^T$.

We will have H non-singular if and only if $y_{k-L_k}^T\lambda_k \neq a_k$ (again by the proof of Theorem 2 in (Kaltofen and Yuhasz, 2009)), so we define

$$\varphi(H) = [a_0,\ldots,a_{k-1},y_{k-L_k}^T\lambda_k,a_{k+1},\ldots,a_{2n-2}].$$

Similarly, if H is singular (so that $y_{k-L_k}^T\lambda_k = a_k$), then changing a_k to any other value will result in a non-singular matrix, so we define

$$\psi(H) = \left\{[a_0,\ldots,a_{k-1},a'_k,a_{k+1},\ldots,a_{2n-2}] \;\middle|\; a'_k \neq a_k\right\}.$$

Lemma 8. *Given $H \in \mathcal{H}^{n\times n}_{\text{singular}}$, $\varphi\big(\psi(H)\big) = H$.*

Proof. Given $H \in \mathcal{H}^{n\times n}_{\text{singular}}$, say $H = [a_0,\ldots,a_{2n-2}]$, we run the Berlekamp/Massey algorithm on the list of entries of H to get

$$\psi(H) = \left\{[a_0,\ldots,a_{k-1},a'_k,a_{k+1},\ldots,a_{2n-2}] \;\middle|\; a'_k \neq a_k\right\}.$$

If we run the Berlekamp/Massey algorithm on $\psi(H)$, then the H_i, h_i and λ_i will agree for $i = 1,2,\ldots,k$, and we will have $y_{k-L_k}^T\lambda_k = a_k \neq a'_k$. By the discussion of φ above, we will have

$$\begin{aligned}\varphi\big(\psi(H)\big) &= [a_0,\ldots,a_{k-1},y_{k-L_k}^T\lambda_k,a_{k+1},\ldots,a_{2n-2}]\\ &= [a_0,\ldots,a_{k-1},a_k,a_{k+1},\ldots,a_{2n-2}]\\ &= H\end{aligned}$$

as proposed. □

Lemma 8 immediately implies that if $H \neq \bar{H}$ in $\mathcal{H}^{n\times n}_{\text{singular}}$, then $\psi(H) \cap \psi(\bar{H}) = \{\emptyset\}$: if a matrix $\bar{\bar{H}}$ were in the intersection, then we would have $H = \varphi(\bar{\bar{H}}) = \bar{H}$, a contradiction.

We now use these maps to count singular $n \times n$ Hankel matrices, allowing a collection of entries to be fixed to prescribed values.

Definition 9. Given an $n \times n$ Hankel matrix $[a_0, \ldots, a_{2n-2}]$, we define

$$L = (L_{\text{ind}}, L_{\text{val}}) = ([i_1, \ldots, i_k], [\alpha_1, \ldots, \alpha_k])$$

(where $k \leq 2n-1$) to represent fixed entries in H, where a_{i_j} is fixed to α_j. When counting singular Hankel matrices over $\mathbb{F}_q$, we let a_i vary over $\mathbb{F}_q$ if $i \notin L_{\text{ind}}$. We will let $\mathcal{H}_L^{n\times n}$ denote the set of Hankel matrices with entries fixed according to L. Note that $\text{card}(\mathcal{H}_L^{n\times n}) = q^{2n-1-k}$.

Theorem 10 (General Count)**.** *The number of singular $n \times n$ Hankel matrices with entries fixed according to L (as in Definition 9), where either $L_{\text{ind}} \subseteq \{0, \ldots, n-1\}$ or $L_{\text{ind}} \subseteq \{n-1, \ldots, 2n-2\}$, is equal to*

$$\sigma(n,q,L) = \begin{cases} q^{2n-2-k}, & \text{if } n-1 \notin L_{\text{ind}} \\ & \text{or if } n-1 \in L_{\text{ind}} \text{ with some} \\ & \quad \text{other } j \in L_{\text{ind}} \text{ and } \alpha_j \neq 0 \\ q^{2n-2-k} - q^{n-2}, & \text{if } n-1 \in L_{\text{ind}},\ \alpha_{n-1} \neq 0, \\ & \quad \text{and all other } \alpha_j = 0 \\ q^{2n-2-k} - q^{n-2} + q^{n-1}, & \text{if } n-1 \in L_{\text{ind}},\ \alpha_{n-1} = 0, \\ & \quad \text{and all other } \alpha_j = 0 \end{cases}.$$

Proof. We first prove the counts for $L_{\text{ind}} \subseteq \{0, \ldots, n-1\}$.

Suppose that $n-1 \notin L_{\text{ind}}$. Given a singular Hankel matrix $H \in \mathcal{H}_L^{n\times n}$, we run the Berlekamp/Massey algorithm on the entries of H; the algorithm will exit at one of the entries on the bottom row because H is singular. Note that $n-1 \notin L_{\text{ind}}$ implies that $\varphi^{-1}(H)$ will yield a unique set of $q-1$ non-singular Hankel matrices for every singular $H \in \mathcal{H}_L^{n\times n}$ (because there is no restriction on any entry of the bottom row). It follows that a fraction of $1/q$ of the q^{2n-1-k} matrices in $\mathcal{H}_L^{n\times n}$ will be singular.

Next, suppose that $n-1 \in L_{\text{ind}}$ and $\alpha_j \neq 0$ for some other $j \in L_{\text{ind}}$. We again run the Berlekamp/Massey algorithm on the entries of a singular $H \in \mathcal{H}_L^{n\times n}$, but now we have a restriction on an element of the bottom row (i.e., a_{n-1}), which poses a problem if the algorithm exits at a_{n-1}. However, the condition $\alpha_j \neq 0$ for some $j \in \{0, \ldots, n-2\}$ guarantees that the largest proper non-singular leading principal submatrix will have size at least 1×1, so the algorithm *cannot* exit at a_{n-1}. Thus, the map φ is defined for each non-singular $H \in \mathcal{H}_L^{n\times n}$ and is surjective, so the count follows as in the case of $n-1 \notin L_{\text{ind}}$.

Now suppose that $n-1 \in L_{\text{ind}}$, $\alpha_{n-1} \neq 0$, and all other $\alpha_j \in L_{\text{val}}$ are zero. Consider the subset N of $\mathcal{H}_L^{n\times n}$ where $a_0 = \cdots = a_{n-2} = 0$; there are q^{n-1} such matrices, which are all non-singular because $\alpha_{n-1} \neq 0$. The map φ is not defined on this set because the Berlekamp/Massey algorithm would exit at a_{n-1}, and thus φ would attempt to change a_{n-1} to zero, which cannot be done. The matrices in N do not contribute to the count, so we restrict the domain of φ to $(\mathcal{H}_L^{n\times n} \cap \mathcal{H}_{\text{non-singular}}^{n\times n}) \setminus N$. As above, the condition $\alpha_j \neq 0$ for some $j \in \{0, \ldots, n-2\}$ guarantees that the map φ is defined for each non-singular matrix in $\mathcal{H}_L^{n\times n} \setminus N$, and again is surjective. It follows that a fraction of $1/q$ of the $q^{2n-1-k} - q^{n-1}$ matrices in $\mathcal{H}_L^{n\times n} \setminus N$ are singular.

Last, suppose that $n-1 \in L_{\text{ind}}$, $\alpha_{n-1} = 0$, and all other $\alpha_j \in L_{\text{val}}$ are zero. We consider the set N from above, but now all matrices in N are singular because $\alpha_{n-1} = 0$. Restricting φ to $(\mathcal{H}_L^{n\times n} \cap \mathcal{H}_{\text{non-singular}}^{n\times n}) \setminus N$ yields the same result, so we simply add the q^{n-1} singular matrices in N to the previous count.

To prove the result for $L_{\text{ind}} \subseteq \{n-1, \ldots, 2n-2\}$, let

$$J_n = \begin{bmatrix} 0 & \ldots & 0 & 1 \\ 0 & & 1 & 0 \\ & \iddots & & \vdots \\ 1 & & 0 & 0 \end{bmatrix} \in \mathbb{F}_q^{n\times n}$$

be the "anti-identity" matrix. Consider the linear transformation

$$T_J : \mathcal{H}_L^{n\times n} \to \mathcal{H}_{L'}^{n\times n} \quad \text{via} \quad H \mapsto J_n H J_n^{-1},$$

which is a bijection onto its image, where L' is the set obtained by mapping each $j \in L_{\text{ind}}$ to $2n-2-j$.

Note that in $\mathcal{H}_{L'}^{n\times n}$, all fixed entries are along or above the antidiagonal, as they were in the case of $L_{\text{ind}} \subseteq \{0, \ldots, n-1\}$. We can therefore use the methods above to conclude the same counts in $\mathcal{H}_{L'}^{n\times n}$. Because T_J is a bijection onto its image (and preserves singularity/non-singularity), we conclude the same counts for $\mathcal{H}_L^{n\times n}$. $\square$

4. Counting Block-Hankel Matrices with Block Generic Rank Profile

Definition 11. We say that a block matrix A (of square submatrices of dimension m) of rank mr has *block generic rank profile* if $\operatorname{rank}(A_k) = mk$ for $k = 1, 2, \ldots, r$, where A_k is the $k \times k$ block leading principal submatrix of A.

Lemma 12. *The number of block-Hankel matrices ($m \times m$ submatrices arranged in $r \times r$ block-Hankel form) of rank mr with block generic rank profile, denoted by $\mathcal{H}_{\text{bgrp}}^{mr\times mr}(r)$, is equal to $q^{m^2(r-1)}\big(\prod_{i=0}^{m-1}(q^m - q^i)\big)^r$.*

Proof. The proof follows by induction. For the case $r = 1$, $\mathcal{H}_{\text{blps}}^{m\times m}$ is simply the number of non-singular $m \times m$ matrices over $\mathbb{F}_q$, which is $\prod_{i=0}^{m-1}(q^m - q^i)$.

Now let $r > 1$ and suppose that the $(r-1)\times(r-1)$ block leading principal submatrix A_{r-1} is non-singular:

$$H = \left[\begin{array}{cccc|c} M_0 & M_1 & \ldots & M_{r-2} & M_{r-1} \\ M_1 & M_2 & \ldots & M_{r-1} & M_r \\ \vdots & \iddots & \iddots & \vdots & \vdots \\ M_{r-2} & M_{r-1} & \ldots & M_{2r-4} & M_{2r-3} \\ \hline M_{r-1} & M_r & \ldots & M_{2r-3} & M_{2r-2} \end{array}\right] = \begin{bmatrix} A_{r-1} & B_{r-1} \\ C_{r-1} & M_{2r-2} \end{bmatrix}.$$

We derive conditions on M_{2r-3} and M_{2r-2} that make H non-singular. It is clear that for any choice of M_{2r-3}, the system $A_{r-1}X = M_{2r-3}$ has a unique solution. We now determine conditions on the columns of M_{2r-2}.

Let the columns of B_{r-1} be denoted $b_0, b_1, \ldots, b_{m-1}$, and the columns of M_{2r-2} denoted $v_0, v_1, \ldots, v_{m-1}$, and consider the matrix

$$\begin{bmatrix} A_{r-1} & b_0 \\ C_{r-1} & v_0 \end{bmatrix}.$$

The system $A_{r-1}x = b_0$ will have a unique solution x regardless of b_0, and correspondingly the block 2×2 matrix above will have full column rank if and only if $C_{r-1}x \neq v_0$. Thus, there are $(q^m - 1)$-many choices for v_0.

Next, suppose that we have chosen $v_0, \ldots, v_{t-1}$ so that the matrix

$$\begin{bmatrix} A_{r-1} & b_0 & \ldots & b_{t-1} \\ C_{r-1} & v_0 & \ldots & v_{t-1} \end{bmatrix}$$

has full column rank. Then the matrix

$$\begin{bmatrix} A_{r-1} & b_0 & \ldots & b_{t-1} & b_t \\ C_{r-1} & v_0 & \ldots & v_{t-1} & v_t \end{bmatrix}$$

will have full column rank if and only if the vector $(b_t, v_t)^T$ is not in the span of the previous columns. We see that if the system

$$\begin{bmatrix} A_{r-1} \\ C_{r-1} \end{bmatrix} x = \begin{bmatrix} b_t + \sum_{i=0}^{t-1} \alpha_i b_i \\ v_t + \sum_{i=0}^{t-1} \alpha_i v_i \end{bmatrix}$$

has a solution, then it will be unique by the non-singularity of A_{r-1}. Thus, for each choice of $(\alpha_0, \ldots, \alpha_{t-1}) \in \mathbb{F}_q^t$, there is one vector that v_t must avoid, and so there are $(q^m - q^t)$-many choices for v_t. It follows that the number of suitable matrices M_{2r-2} is $\prod_{i=0}^{m-1}(q^m - q^i)$.

Combining this with the fact that M_{2r-3} may be arbitrary, we see that the number of block-Hankel matrices (with A_{r-1} as the $mr \times mr$ block leading principal submatrix) that have every block leading principal submatrix non-singular is $q^{m^2}\big(\prod_{i=0}^{m-1}(q^m - q^i)\big)$.

Overall, it follows that there are $q^{m^2(r-1)}\big(\prod_{i=0}^{m-1}(q^m - q^i)\big)^r$ block-Hankel matrices of rank mr with block generic rank profile. $\square$

Theorem 13. *The number of block-Hankel matrices ($m \times m$ submatrices arranged in $n \times n$ block-Hankel form) of rank mr with block generic rank profile, denoted by $\mathcal{H}_{\text{bgrp}}^{mn \times mn}(r)$, is equal to*

$$\mathcal{H}_{\text{bgrp}}^{mn \times mn}(r) = \begin{cases} q^{m^2 r}\Big(\prod_{i=0}^{m-1}(q^m - q^i)\Big)^r, & r < n \\ q^{m^2(r-1)}\Big(\prod_{i=0}^{m-1}(q^m - q^i)\Big)^r, & r = n \end{cases}$$

Proof. The case $r = n$ is proved in Lemma 12, so we assume $r < n$. Let H be such a

matrix. Then we can write

$$H = \left[\begin{array}{ccc|c|ccc} M_0 & \dots & M_{r-1} & M_r & M_{r+1} & \dots & M_{n-1} \\ \vdots & \iddots & \vdots & \vdots & \vdots & \iddots & \vdots \\ M_{r-1} & \dots & M_{2r-2} & M_{2r-1} & M_{2r} & \dots & M_{n+r-2} \\ \hline M_r & \dots & M_{2r-1} & M_{2r} & M_{2r+1} & \dots & M_{n+r-1} \\ \vdots & \iddots & \vdots & \vdots & \vdots & \iddots & \vdots \\ M_{n-1} & \dots & M_{n+r-2} & M_{n+r-1} & M_{n+r} & \dots & M_{2n-2} \end{array}\right]$$

$$= \left[\begin{array}{cc|c} A_r & B_r & \\ \hline C_{r+1} & M_{2r} & \\ \vdots & \vdots & D \\ C_n & M_{n+r-1} & \end{array}\right],$$

where A_r is non-singular. It is clear that for any choice of M_{2r-1}, the system $A_r X = B_r$ has a unique solution.

Let the columns of B_r be denoted $b_0, b_1, \dots, b_{m-1}$, and similarly let the columns of $[M_{2r}^T \ \dots \ M_{n+r-1}^T]^T$ be denoted $v_0, v_1, \dots, v_{m-1}$. As in the proof of Lemma 12, consider the matrix

$$\begin{bmatrix} A_r & b_0 \\ C_{r+1} & v_0 \end{bmatrix}.$$

The system $A_r x = b_0$ will have a unique solution x regardless of b_0, and correspondingly the block 2×2 matrix above will have (full column) rank $m(r+1)$ if and only if $C_{r+1}x = v_0$. The matrix H must have rank mr, so we see that v_0 is predetermined.

Next, suppose that

$$\begin{bmatrix} A_r & b_0 & \dots & b_{t-1} \\ C_{r+1} & v_0 & \dots & v_{t-1} \end{bmatrix}$$

has rank mr. Then the matrix

$$\begin{bmatrix} A_r & b_0 & \dots & b_{t-1} & b_t \\ C_{r+1} & v_0 & \dots & v_{t-1} & v_t \end{bmatrix}$$

will have rank mr if and only if the vector $(b_t, v_t)^T$ is in the span of the previous columns. We see that if the system

$$\begin{bmatrix} A_r \\ C_{r+1} \end{bmatrix} x = \begin{bmatrix} b_t + \sum_{i=0}^{t-1} \alpha_i b_i \\ v_t + \sum_{i=0}^{t-1} \alpha_i v_i \end{bmatrix}$$

has a solution, then it will be unique by the non-singularity of A_r. Thus, v_t is predetermined as well. It follows that $M_{2r}, \dots, M_{n+r-1}$ are predetermined.

Moreover, $M_{n+r}, \ldots, M_{2n-2}$ are predetermined, a fact that was corrected by an anonymous referee. To see why, note that the first mr columns of H form a basis for the column space of H. If we denote the columns of D by $d_0, d_1, \ldots, d_{n-r-1}$, then the matrix

$$\left[\begin{array}{c|c|c} A_r & B_r & \\ \hline C_{r+1} & M_{2r} & \\ \vdots & \vdots & d_0 \\ C_n & M_{n+r-1} & \end{array}\right]$$

will have rank mr if and only if d_0 is in the span of the first $m(r+1)$ columns of H, which equals the span of the first mr columns of H. By the non-singularity of A_r, the resulting column relation would be unique, so the last m entries of d_0 (i.e., the first column of M_{n+r}) are predetermined. The same argument follows inductively for every column of D, so that each of $M_{n+r}, \ldots, M_{2n-2}$ is predetermined.

Because only M_{2r-1} may be arbitrary, it follows that H is one of

$$q^{m^2(r-1)}\left(\prod_{i=0}^{m-1}(q^m - q^i)\right)^r \cdot q^{m^2} = q^{m^2 r}\left(\prod_{i=0}^{m-1}(q^m - q^i)\right)^r$$

many matrices. □

For the case $m = 1$, Theorem 13 implies that the number of $n \times n$ Hankel matrices (with entries from $\mathbb{F}_q$) of rank r with generic rank profile is

$$\mathcal{H}^{n\times n}_{\text{bgrp}}(r) = \begin{cases} q^r(q-1)^r, & r < n \\ q^{r-1}(q-1)^r, & r = n \end{cases}.$$

We can compare this to the result in (Kaltofen and Lobo, 1996), which states that the number of $n \times n$ Toeplitz matrices (with entries from $\mathbb{F}_q$) with generic rank r is

$$N_r = \begin{cases} q^{2n-2}\left(1-\frac{1}{q}\right)^2\left(1-\frac{q-1}{q^2}\right)^{r-1}, & 0 < r < n \\ q^{2n-1}\left(1-\frac{1}{q}\right)\left(1-\frac{q-1}{q^2}\right)^{n-1}, & r = n \end{cases}.$$

We have investigated the analogous question for block-Hankel matrices, but we do not know explicit formulas for the counts. Presented below are some brute-force counts for the number of singular block-Hankel matrices ($m \times m$ submatrices arranged in $n \times n$ block-form, with entries from $\mathbb{F}_q$).

m	n	q	Singular/Total
2	2	2	$\frac{2704}{4096}=\frac{2^4\cdot 13^2}{2^{12}}$
2	2	3	$\frac{226881}{531441}=\frac{3^4\cdot 2801}{3^{12}}$
2	3	2	$\frac{701440}{1048576}=\frac{2^{10}\cdot 5\cdot 137}{2^{20}}$
3	2	2	$\frac{93790208}{134217728}=\frac{2^{13}\cdot 107^2}{2^{27}}$
2	2	5	$\frac{58080625}{244140625}=\frac{5^4\cdot 19\cdot 67\cdot 73}{5^{12}}$
2	4	2	$\frac{180158464}{268435456}=\frac{2^{16}\cdot 2749}{2^{28}}$

Acknowledgements

The authors would like to thank the referees for their comments, which improved the presentation of the paper.

References

Daykin, D. E., 1960. Distribution of bordered persymmetric matrices in a finite field. J. reine u. angew. Math. 203, 47–54.

Garcìa-Armas, M., Ghorpade, S. R., Ram, S., 2011. Relatively prime polynomials and nonsingular hankel matrices over finite fields. J. Combin. Theory Ser. A 118, 819–828.

Kaltofen, E., Lee, W., 2003. Early termination in sparse interpolation algorithms. J. Symbolic Comput. 36 (3–4), 365–400, special issue Internat. Symp. Symbolic Algebraic Comput. (ISSAC 2002). Guest editors: M. Giusti & L. M. Pardo. URL: EKbib/03/KL03.pdf.

Kaltofen, E., Lobo, A., 1996. On rank properties of Toeplitz matrices over finite fields. In: Lakshman Y. N. (Ed.), Proc. 1996 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'96). ACM Press, New York, N. Y., pp. 241–249, URL: EKbib/96/KaLo96_issac.pdf.

Kaltofen, E., Yuhasz, G., Feb. 2009. A fraction free matrix Berlekamp/Massey algorithm. Manuscript, 17 pages.

Massey, J. L., 1969. Shift-register synthesis and BCH decoding. IEEE Trans. Inf. Theory IT-15, 122–127.

Paturi, R., Pudlák, P., 2010. On the complexity of circuit satisfiability. In: Schulman, L. J. (Ed.), STOC. ACM, pp. 241–250.

Sugiyama, Y., Kasahara, M., Hirasawa, S., Namekawa, T., 1975. A method for solving key equation for decoding Goppa codes. Information & Control 27, 87–99.