On the ranks of Toeplitz matrices over finite fields

Geoffrey L. Price*, Glenn H. Truitt

Department of Mathematics, 9E, United States Naval Academy, Annapolis, Maryland, 21402 USA
Received 4 May 1998; accepted 17 February 1999
Submitted by R.A. Brualdi

Abstract

Let $T$ be a skew-symmetric Toeplitz matrix with entries in a finite field. For all positive integers $n$ let $T_n$ be the upper $n \times n$ corner of $T$, with nullity $v_n = v(T_n)$. The sequence $\{v_n : n \in \mathbb{N}\}$ satisfies a unimodality property and is eventually periodic if the entries of $T$ satisfy a periodicity condition. We compute the maximum value and the period of the nullity sequence for Toeplitz matrices of finite bandwidth. This sequence satisfies a certain symmetry condition about its maximal values. These results apply to give some information about the ranks of general skew-symmetric Toeplitz matrices with eventually periodic entries. © 1999 Elsevier Science Inc. All rights reserved.

1. Introduction

Following the terminology of [6], an $n \times n$ matrix $T_n$ with entries in a field $F$ is called centroisymmetric if it is symmetric with respect to its main and secondary diagonals. A matrix is called skew centroisymmetric if it is symmetric with respect to its secondary diagonal and skew-symmetric with respect to its main diagonal. In this paper we study some properties of the ranks of matrices of the latter type. We shall refer to these matrices as finite skew-symmetric Toeplitz matrices, since they may be realized as corners of infinite ones.

*Supported in part by grants from the National Science Foundation, the National Security Agency, and by a United States Naval Academy Recognition Grant
*Corresponding author. E-mail: glp@nadn.navy.mil

0024-3795/99/$ – see front matter © 1999 Elsevier Science Inc. All rights reserved.
PII: S 0 0 2 4 - 3 7 9 5 ( 9 9 ) 0 0 0 5 2 - X
particular, if $F$ is a finite field and $\{a_n : n \in \mathbb{Z}^+\}$ is a sequence in $F$, then one may form an infinite skew-symmetric Toeplitz matrix $T =$

\[
\begin{pmatrix}
a_0 & -a_1 & -a_2 & -a_3 & \ldots \\
a_1 & a_0 & -a_1 & -a_2 & \ldots \\
a_2 & a_1 & a_0 & -a_1 & \ldots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{pmatrix}
\]

which is uniquely defined by its first column, and hence by the terms of the sequence $\{a_n\}$. If $F$ has characteristic other than 2, then $a_0 = 0$. In the characteristic 2 case we impose the condition $a_0 \neq 0$. For each $n \in \mathbb{N}$, let $T_n$ be the upper left $n \times n$ corner of $T$.

Previously R.T. Powers and one of the authors observed that if $\{T_n : n \in \mathbb{N}\}$ is the sequence of $n \times n$ corners of a skew-symmetric Toeplitz matrix $T$ over the field $F_2$ of two elements, and if $v_n$ is the nullity of $T_n$, then the sequence $\{v_n : n \in \mathbb{N}\}$ satisfies a certain unimodality property, [8, Theorem 6.6]. This property proved useful in the classification of a family of shift endomorphisms on the hyperfinite $II_1$ factor, [8–10]. In [1, Theorem 2.7], K. Culler and one of the authors proved that skew symmetric Toeplitz matrices over general finite fields satisfy similar unimodality properties. This result led to a combinatorial way to determine the number of $n \times n$ skew-symmetric Toeplitz matrices of any specified rank, for any $n \in \mathbb{N}$. In the next section we consider skew-symmetric Toeplitz matrices of finite bandwidth. If $\{T_n : n \in \mathbb{N}\}$ is the corresponding sequence of matrix corners of $T$ we show that $\{v_n : n \in \mathbb{N}\}$ is a periodic sequence, and we determine its period, Theorem 2.10 (cf. [10, Theorem 6.2]). If $T$ has finitely non-zero initial row $a_0, -a_1, -a_2, \ldots, -a_{k-1}$ is the last non-zero entry of this sequence, then we show in Theorem 2.10 that the maximum nullity of the $T_n$'s is $k - 1$. In addition, we show in Theorem 2.18 that for any $n$ such that $v_n = k - 1$, and for any non-negative integer $r \leq n$, $v_{n+r} = v_{n-r}$. This symmetry result is established by appealing to some well-known properties of linear recurring sequences [2,4,5]. In combination with the unimodality properties of the nullity sequence and knowledge of its period, the symmetry property often suffices in making a complete determination of the values of the nullity sequence (see Section 4).

In the third section of this paper we apply the results obtained on skew-symmetric Toeplitz matrices of finite bandwidth to analyze the nullity sequences associated with skew-symmetric Toeplitz matrices defined by an eventually periodic sequence $\{a_n : n \in \mathbb{N}\}$ of elements of the field. Some of the techniques used in establishing these results are taken from [10].

2. Finite bandwidth Toeplitz matrices

We begin this section by introducing some notation and reviewing some of the results which have already been established for the ranks of sequences of
skew-symmetric Toeplitz matrices, [1,8–10]. We also require some results from
the theory of linear recurring sequences [2,4,5,11].

In this and succeeding sections we shall always use the term kernel of a
matrix $M$ to refer to the right kernel of $M$, i.e., if $M$ is an $m \times n$ matrix then $\ker(M) = \{v \in F^n : Mv = 0\}$.

**Definition 2.1.** Let $T$ be a skew-symmetric Toeplitz matrix over a finite field $F$. The signature of $T$ is the sequence $\{a_n : n \in \mathbb{Z}^+\}$ consisting of the entries in the first column of $T$ in (1.1).

As mentioned above, we shall always assume in the case where $F$ has
characteristic 2 that $a_0 = 0$.

**Proposition 2.2** ([7, Theorem IV.1, Theorem IV.11]). Let $T$ be a skew-symmetric Toeplitz matrix over a finite field $F$ with signature $\{a_n : n \in \mathbb{Z}^+\}$. For each $n \in \mathbb{N}$ let $\rho_n$ be the rank of $T_n$ and let $v_n$ be its nullity. Then $\rho_n$ is even. For each $n \in \mathbb{N}$, either $v_{n+1} = v_n + 1$ or $v_{n+1} = v_n - 1$.

**Proposition 2.3** ([1, Theorem 2.6]). Assume the same hypotheses as above. If $\rho_n < \rho_{n+1}$ and $\rho_{n+1}$ does not have full rank (i.e., if $\rho_{n+1} < n + 1$) then $\rho_{n+1} < \rho_{n+2}$.

As a corollary to the preceding two results we have the following
unimodality property for the nullity sequences of skew-symmetric Toeplitz
matrices.

**Corollary 2.4** (cf. [1, Theorem 2.7], [8, Theorem 5.4]). If $T$ is a skew-symmetric Toeplitz matrix over a finite field then one of the following two conditions must hold:

(i) There is a sequence $\{m_i\}$ of positive integers such that the nullity sequence $v_n = v(T_n), n \in \mathbb{N}$, is a concatenation of the strings $1, 2, \ldots, m_i - 1, m_i, m_i - 1, \ldots, 2, 1, 0$.

(ii) There are finitely many positive integers $m_1, \ldots, m_j$ such that $v_n, n \in \mathbb{N}$ consists of the concatenation of the strings $1, 2, \ldots, m_i - 1, m_i, m_i - 1, \ldots, 2, 1, 0$ for $i = 1, 2, \ldots, j$, followed by the sequence $1, 2, \ldots$

In Proposition 2.9 we show that condition (ii) holds if and only if the signature sequence for $T$ satisfies a certain periodicity condition. The following result gives more precise information about the kernels of the sequence of matrices $T_n, n \in \mathbb{N}$. We shall need the following terminology.
Definition 2.5. The flip $\hat{v}$ of a vector $v = [v_0, v_1, \ldots, v_{n-1}]$ is the vector $[v_{n-1}, v_{n-2}, \ldots, v_0]$. The transpose of a row vector $\mathbf{v}$ will be denoted by $\mathbf{v}'$.

Proposition 2.6 ([1, Lemma 2.8], [10, Theorem 3.4]). Let $T$ be a skew-symmetric Toeplitz matrix over a finite field $F$. Let $v_n = v(T_n)$ be the nullity of $T_n$, $n \in \mathbb{N}$.

(i) If $v_n = 0$ then $\ker(T_{n+1})$ is spanned by a single vector $\mathbf{r} = [r_0, r_1, \ldots, r_n]'$ satisfying $\mathbf{r} = c\mathbf{v}$ for some $c \in F$, and $r_0 \neq 0$.

(ii) If $v_n = 0$ and if there is a $p$ such that $v_{n+j} = j$ for $j = 1, 2, \ldots, p$, then for $j = 1, 2, \ldots, p$, $\ker(T_{n+j})$ is spanned by the $j$ vectors $[r_0, \ldots, r_n, 0, \ldots, 0]'$, $[0, r_0, \ldots, r_n, 0, \ldots, 0]'$, $\ldots$, $[0, \ldots, 0, r_0, \ldots, r_n]'$.

(iii) Suppose $v_n = 0$ and $p$ is a positive integer such that $v_{n+j} = j$ for $j = 1, 2, \ldots, p$ and $v_{n+p+j} = p - j$ for $j = 1, 2, \ldots, p$. Consider the $p$ vectors spanning $\ker(T_{n+p})$ as in (ii). Then for $j = 1, \ldots, p - 1$, $\ker(T_{n+p+j})$ is spanned by the $p - j$ vectors obtained by deleting the first $j$ vectors in the set of $p$ vectors above, and appending $j$ 0’s to the remaining $p - j$ vectors.

Proof. (i) and (ii) follow directly from [1, Lemma 2.8]. It is not difficult to show that if (ii) holds then the $p - j$ vectors in the statement of condition (iii) lie in $\ker(T_{n+p+j})$ so that (iii) follows by Corollary 2.4 (ii). □

Definition 2.7. For any $n \in \mathbb{N}$, let $\mathbf{c} = [c_0, c_1, \ldots, c_{n-1}]$ be any vector in $F^n$. If $m \geq n$ and $\mathbf{r} = [r_0, \ldots, r_{m-1}] \in F^m$, then $\mathbf{c}$ annihilates $\mathbf{r}$ if $\sum_{i=0}^{n-1} c_i r_{i+j} = 0$ for $j = 0, \ldots, m - n$. Similarly, $\mathbf{c}$ annihilates a sequence $\{r_q : q \in \mathbb{Z}^+\}$ if $\sum_{i=0}^{n-1} c_i r_{i+j} = 0$ for all $j \in \mathbb{Z}$.

We recall [4, Theorem 6.11] that a sequence $\{b_n : n \in \mathbb{Z}^+\}$ in a finite field is periodic if and only if there is a vector (called a key in the literature on linear recurring sequences) $\mathbf{s} = [s_0, \ldots, s_q]$ with $s_0 \neq 0$ such that $b_{n+1} = \sum_{i=0}^{q} s_{q-i}b_{n-i}$ for $n > q$. Setting $s_{q+1} = -1$ it is straightforward to prove the following.

Proposition 2.8 ([4, Theorem 6.11]). A sequence $\{b_n : n \in \mathbb{Z}^+\}$ in a finite field is eventually periodic if and only if there is a non-trivial vector $\mathbf{s} = [s_0, \ldots, s_m]$ which annihilates the sequence. It is periodic if and only if $\mathbf{s}$ can be chosen such that $s_0 \neq 0$.

Proposition 2.9. Let $T$ be a skew-symmetric Toeplitz matrix over a finite field $F$ with signature $\{a_n : n \in \mathbb{Z}^+\}$. For each $n \in \mathbb{N}$ let $v_n$ be the nullity of $T_n$. Consider the doubly-infinite sequence $\{a(n) : n \in \mathbb{Z}\}$ given by $\ldots, a_2, a_1, a_0, -a_1, -a_2, \ldots$. This sequence is periodic if and only if there is an $n \in \mathbb{Z}^+$ such that $v_{n+j} = j$ for all $j \in \mathbb{N}$. If the doubly-infinite sequence is not periodic, there is a sequence of (not
necessarily distinct) positive integers \( \{p_m : m \in \mathbb{N} \} \) such that the sequence \( \{v_n : n \in \mathbb{N} \} \) consists of the concatenation of the strings of the form

\[ 1, 2, \ldots, p_m - 1, p_m, p_m - 1, \ldots, 1, 0, \text{ for } 1 \leq m \leq r. \]

**Proof.** Suppose \( \{a(n) : n \in \mathbb{Z} \} \) is periodic. Let \( p \) be a positive integer such that \( a(m) = a(m + p) \) for all \( m \in \mathbb{Z} \). Let \( q > p \), and suppose \( [k_0, \ldots, k_{q-1}]' \in \ker(\mathcal{A}_q) \). Then clearly \( \mathcal{A}_{q+1}[k_0, \ldots, k_{q-1}, 0]' = [0, \ldots, 0, c]' \), for some \( c \in F \), but using the periodicity of \( \{a(m)\} \) the first \( n \) entries of the last row \( [a_q, a_{q-1}, \ldots, a_1, a_0] = [a(-q), a(-q + 1), \ldots, a(-1), a(0)] \) are the same as \( [a(-q + p), a(-q + p + 1), \ldots, a(-1 + p)] \), which coincides with the \((q - p + 1)\)st row of \( \mathcal{A}_n \). Hence \( c = 0 \), so \( [k_0, \ldots, k_{q-1}, 0]' \in \ker(\mathcal{A}_{q+1}) \), and therefore \( v_{q+1} \geq v_q \). But then \( v_{q+1} = v_q + 1 \) by Proposition 2.2. Then there is an \( n \) such that \( v_{n+j} = j \) for all \( j \in \mathbb{N} \). Conversely suppose \( v_{n+j} = j \) for some \( n \in \mathbb{Z}^+ \) and all \( j \in \mathbb{N} \). Then by [1, Lemma 2.4] there is a vector \( k = [k_0, \ldots, k_n]' \in \ker(\mathcal{A}_{n+1}) \) such that \( k_0 \neq 0 \), such that \( [k_n, \ldots, k_0]' = k = ck \) for some \( c \in F \), and such that \( k_1 \in \ker(\mathcal{A}_{n+j}) \), where \( k_1 \) is the vector \( [k_0, \ldots, k_n, 0, \ldots, 0]' \) obtained by appending \( j - 1 \) 0’s to \( k \). Since \( k_1 \in \ker(\mathcal{A}_{n+j}) \) it follows that \( \sum k_i a_i(-m + i) = 0 \), for \( m = 0, \ldots, n + j \). Since \( k_n \neq 0 \) the sequence, \( \ldots, a(-1), a(0), a(1), \ldots, a(n) \) is periodic by Proposition 2.8. Since \( a(-n) = a(n) \), then also \( a(-n), a(-1), a(0), a(1), a(2), \ldots, \) is periodic. Since the sequence, \( \ldots, a(-1), a(0), a(1), \ldots, a(n) \) is annihilated by \( [k_0, \ldots, k_n], a(-n), \ldots, a(-1), a(0), a(1), a(2), \ldots, \), is annihilated by \( k \). Since \( k = ck \), the sequence \( a(-n), \ldots, a(-1), a(0), a(1), \ldots, \) is annihilated by \( k \). Since the doubly-infinite sequence, \( \ldots, a(-1), a(0), a(1), \ldots, \) is annihilated by \( k \), the sequence is periodic.

The second conclusion of the proposition follows from combining the first conclusion with Corollary 2.3. \( \Box \)

A weaker version of the following theorem was proved [10] in the special case in which \( F \) is the field of 2 elements. The theorem was then applied in that paper to obtain some results on the classification of endomorphisms of von Neumann algebras. Here we show that the original result remains valid for all finite fields, and we replace the original proof with a more elementary one.

It will be helpful to sharpen the results of Proposition 2.9. Recall that if \( F \) is a finite field and \( b = [b_0, b_1, \ldots, b_{m-1}] \) and \( s = [s_0, s_1, \ldots, s_{m-1}] \) are vectors with entries in \( F \), then one constructs a linear recurring sequence \( \{s_n : n \in \mathbb{Z}^+ \} \) via the recurrence relation

\[
s_{n+m} = b_{m-1}s_{n+m-1} + b_{m-2}s_{n+m-2} + \cdots + b_0s_n, \quad n \in \mathbb{N}.
\]

By Proposition 2.8 the sequence is ultimately periodic, and if \( b_0 \neq 0 \), the sequence is in fact periodic. In this case the companion matrix
is invertible. Since $B$ has entries in a finite field, $B$ has finite order, i.e., there is an $s \in \mathbb{N}$ such that $B^s = I$, the identity matrix. The order of $B$ is a multiple of the period of any sequence $\{s_n : n \in \mathbb{Z}^+\}$ generated as above, [4, Theorem 6.16, Theorem 6.17].

The sequence $\{s_n : n \in \mathbb{Z}^+\}$ whose $m$ initial values are $0, 0, \ldots, 0, 1$ is called the impulse response sequence. Its period coincides with the order of $B$, [4, Theorem 6.17]. Hence the period of any linear recurring sequence generated as in (2.1) divides the period of the impulse response sequence.

**Theorem 2.10** (cf. [10, Theorem 6.2]). Let $T$ be a non-zero finite band skew-symmetric Toeplitz matrix over a finite field $F$ with signature $d_0, d_1, \ldots$, where $d_0 = 0$. Suppose $k \in \mathbb{N}$ is such that $d_{k-1} \neq 0$, and $d_n = 0$ for $n \geq k$. For each $n \in \mathbb{N}$ let $v_n$ be the nullity of the $n \times n$ corner matrix $T_n$ of $T$. Then the nullity sequence $\{v_n : n \in \mathbb{N}\}$ is periodic. Its period is equal to the order of the invertible matrix $C$ below (where $c_j = d_j/d_{k-1}$ for $j = 0, 1, \ldots, k-1$):

$$
B = \begin{bmatrix}
0 & 1 & 0 & \cdots & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 \\
& & \ddots & & \ddots & \\
0 & 0 & \cdots & 0 & 1 \\
b_0 & b_1 & \cdots & b_{m-2} & b_{m-1}
\end{bmatrix},
$$

For each $n \in \mathbb{N}$, $v_n \leq k - 1$ and $v_n = k - 1$ if and only if $n = js - k + 1$, for some $j \in \mathbb{N}$, where $s$ is the order of the matrix $C$.

The proof will be obtained by combining the results of the following lemmas:

**Lemma 2.11.** Assume the same hypotheses as above. Then $v_n \leq k - 1$ for all $n \in \mathbb{N}$.
Proof. Suppose there is a positive integer \( n \) such that \( v_n \geq k \). By Corollary 2.4 there are two possible cases: either (i) \( v_j = j \) for \( 1 \leq j \leq k \), or (ii) there is a positive integer \( m \) such that \( v_{m+j} = j \) for \( j = 0, \ldots, k \). In the first case each of the \( j \times j \) matrices \( T_j \) has rank 0, for \( j = 1, 2, \ldots, k \). Hence \( d_1 = d_2 = \cdots = d_{k-1} = 0 \), a contradiction. In the second case there is by Proposition 2.6 a vector \([r_0, \ldots, r_m]\) \( \in \ker(T_{m+1}) \) such that \( r_0 \neq 0 \) and such that \([0, \ldots, 0, r_0, \ldots, r_m]\) \( \in \ker(T_{m+k}) \). Multiplying this vector on the left by \( T_{m+1} \) yields a vector with first term \(-d_{k-1}r_0\), a contradiction since \( d_{k-1} \neq 0 \). This contradiction yields the lemma. \( \square \)

Lemma 2.12. The matrix \( C \) in the statement of the theorem is invertible with period \( s \geq 2k - 2 \).

Proof. \( C \) is invertible since \( c_{k-1} = 1 \). Note that for \( 0 \leq r \leq 2k - 3 \) the first non-zero entry of the vector \( C'[0, \ldots, 0, 1]' \) is a 1 in the \( 2k - 2 - r \) position and so all of these vectors are distinct. Hence \( C' \neq I \) for \( l \leq r \leq 2k - 3 \). \( \square \)

Lemma 2.13. If \( n > 2k - 2 \) then \( v_n = k - 1 \) if and only if \( n = js - k + 1 \), for \( j \in \mathbb{N} \).

Proof. Let \( s_0 = [0, \ldots, 0, 1]' \in F^{2k-2} \). If \( m \) is any multiple of \( s \), then \( C^m = I \), so \( s_m = C^m s_0 = s_0 \) and therefore there is an \( a \in F \) such that \( s_{m-1} = [a, 0, \ldots, 0]' \). Since \( s_m = C s_{m-1}, s_{m-1} \neq 0 \), so \( a \neq 0 \). For \( j = 0, \ldots, m-1 \), let \( y_j \) be the last entry of \( s_j \), then by appending these entries to the entries of \( s_0 \) one obtains the first \( m + 2k - 2 \) entries of the impulse response sequence corresponding to the key \([c_{k-1}, \ldots, c_1, c_0, -c_1, \ldots, -c_{k-2}]\), namely, \([0, \ldots, 0, y_0, \ldots, y_{m-1}]\). It follows from the form of \( s_{m-1} \) and \( s_m \) that \( y_{m-2k+2} = a \) and \( y_j = 0 \) for \( m - 2k + 2 < j < m \). Consider the vector \( \hat{y} = [y_0, \ldots, y_{m-2k+2}]' \) of length \( m - 2k + 3 \). We claim that \( \hat{y} = ay \). To see this note that the string of entries \([0, \ldots, 0, y_0, \ldots, y_{m-1}]\) is constructed so that it is annihilated by the vector \( \mathbf{c} = [c_{k-1}, \ldots, c_1, c_0, -c_1, \ldots, -c_{k-2}] \) (recall \( c_{k-1} = 1 \)). In particular, taking \( \mathbf{v} \) to be the first \( 2k - 1 \) elements of the string we see, recalling \( y_0 = 1 \), that \(-c_{k-2}y_0 - c_{k-1}y_1 = 0 = -c_{k-2} - y_1 \), so \( y_1 = -c_{k-2} \). By setting \( \mathbf{v} \) to be the last \( 2k - 1 \) elements of the string we find that \( c_{k-1}y_{m-2k+1} + c_{k-2}y_{m-2k+2} = 0 = y_{m-2k+1} + ac_{k-2} \), so that \( y_{m-2k+1} = -ac_{k-2} = ay_1 \). Comparing next the product of \( \mathbf{c} \) with the pair of vectors \([0, \ldots, 0, y_0, y_1, y_2] \) and \([y_{m-2k+1}, y_{m-2k+1}, y_{m-2k+2}, 0, \ldots, 0] \), and given that each of these products is 0, one sees that \( y_2 = ay_{m-2k} \). Continuing in this fashion establishes the claim.

The remarks about products in the previous paragraph show that the \( k - 1 \) vectors \([y_0, \ldots, y_{m-2k+2}, 0, \ldots, 0], \quad [0, \ldots, y_{m-2k+2}, 0, \ldots, 0], \quad [0, \ldots, 0, y_0, \ldots, y_{m-2k+2}] \) all lie in the right kernel of \( T_{2p+k-1} \). Thus \( v_{2p+k-1} \geq k - 1 \), so by Lemma 2.11, \( v_{m-k+1} = k - 1 \). Hence \( v_q = k - 1 \) for \( q \) of the form \( m - k + 1 = js - k + 1 \), for any \( j \in \mathbb{N} \).
We show next that \( v_q = k - 1 \) only if \( q = js - k + 1 \) for some positive integer \( j \). Suppose \( v_q = k - 1 \). Since \( v_q \) is the maximum value of the nullity sequence, Corollary 2.4 implies that \( v_{q-k+2}, \ldots, v_q \) are \( 1, 2, \ldots, k-1 \), respectively. By Proposition 2.6 there is a vector of the form \([z_0, \ldots, z_{q-k+1}, 0, \ldots, 0]'\) in \( \ker(T_q) \), with \( z_0 \neq 0 \). It follows that the vector \([0, \ldots, 0, z_0, \ldots, z_{q-k+1}, 0, \ldots, 0]'\), obtained by adding \( k - 2 \) 0’s to the beginning of the preceding vector, is annihilated by \( c \). Using the proposition we may assume, without loss of generality, that \( z_0 = 1 \), and therefore it is clear from the previous discussion that \( 0, \ldots, 0, z_0, z_1, \ldots, \), is the initial part of the impulse response sequence. It then follows, as in the previous paragraph, that \( q = js - k + 1 \) for some \( j \in \mathbb{N} \). □

**Lemma 2.14.** The nullity sequence \( \{v_n : n \in \mathbb{N}\} \) is eventually periodic with period \( s \) and preperiod \( p_0 \leq 2k - 2 \).

**Proof.** For \( n > 2k - 2 \) let \( B_n \) be the matrix consisting of the first \( k - 1 \) rows of \( T_n \), let \( D_n \) be the matrix consisting of the last \( k - 1 \) rows of \( T_n \), and let \( E_n \) be the matrix consisting of the remaining rows of \( T_n \). Let \( y_0, \ldots, y_{2k-3} \) be arbitrary elements of \( F \). Set \( y = [y_0, \ldots, y_{2k-3}]' \). Define \( y_{2k-2}, \ldots, y_{s+n-1} \) recursively by setting

\[
[y_r, y_{r+1}, \ldots, y_{r+2k-3}]' = C' [y_0, \ldots, y_{2k-3}]'
\]

for \( 0 \leq r \leq s + n - 2k + 2 \). Set \( \tilde{y} = [y_0, \ldots, y_{n-1}]' \) and \( \tilde{\tilde{y}} = [y_0, \ldots, y_{s+n-1}]' \). Since \( y \) and \( \tilde{y} \) share the same first \( 2k - 2 \) elements it follows that \( y \in \ker(B_n) \) if and only if \( \tilde{y} \in \ker(B_{s+n}) \). By (2.2) \( y \in \ker(E_n) \) and \( \tilde{y} \in \ker(E_{s+n}) \). Since \( C'S = I \), the last \( 2k - 2 \) entries of \( y \) and of \( \tilde{y} \) are the same, so it follows that \( y \in \ker(D_n) \) if and only if \( \tilde{y} \in \ker(D_{s+n}) \). Hence \( y \in \ker(T_n) \) if and only if \( \tilde{y} \in \ker(T_{s+n}) \), so \( v_n = v_{s+n} \) for \( n > 2k - 2 \). On the other hand, the preceding lemma shows that the period of the eventually periodic part of the nullity sequence cannot be less than \( s \).

**Lemma 2.15.** If \( v_n = 0 \) for some \( n \in \{1, 2, \ldots, 2k - 3\} \), then \( v_{s+n} = 0 \).

**Proof.** If \( n \leq k \) then

\[
T_n = \begin{bmatrix}
  d_0 & -d_1 & -d_2 & \cdots & -d_{n-1} \\
  d_1 & d_0 & -d_1 & \cdots & -d_{n-2} \\
  \vdots & \ddots & \ddots & \ddots & \ddots \\
  d_{n-1} & d_{n-2} & d_{n-3} & \cdots & d_0
\end{bmatrix}
\]

and if \( n > k \) then
In either case, the lower right \( n \times n \) corner of \( T_{s+n} \) coincides with \( T_n \). Suppose \( v_n = 0 \) but \( v_{s+n} = \text{null} \left( T_{s+n} \right) > 0 \) with non-trivial vector \( \left[ y_0, \ldots, y_{s+n-1} \right]' \) \( \in \ker \left( T_{s+n} \right) \). Adding \( k-1 \) 0's to this vector yields the vector \( y = [0, \ldots, 0, y_0, \ldots, y_{s+n-1}]' \) which is annihilated by \( d = [d_{k-1}, \ldots, d_1, d_0, -d_1, \ldots, -d_{k-1}] \), and therefore also by \( c \). Then if \( \bar{y} = [0, \ldots, 0, y_0, \ldots, y_{k-2}]' \) is the vector consisting of the first \( 2k-2 \) entries of \( y \) it follows that \( y_{k-2} = 0 \) is the last entry of the vector \( C' \bar{y} \). Since \( C \) has period \( s \), \( C' \bar{y} = \bar{y} \), so the terms of \( y \) comprise the beginning of a bitstream which is periodic and whose period divides \( s \). It follows, since \( y \) begins with \( k - 1 \) 0's, that \( y_{s-k+1} = y_{s-k+2} = \cdots = y_{s-1} = 0 \). Since \( [y_0, \ldots, y_{s+n-1}]' \) \( \in \ker \left( T_{s+n} \right) \), this vector is of course in the kernel of the matrix consisting of the last \( n \) rows of \( T_{s+n} \). But since \( 0 = y_{s-k+1} = \cdots = y_{s-1} \), it follows that \( [y_0, \ldots, y_{s+n-1}]' \) lies in the kernel of the lower right \( n \times n \) matrix of \( T_{s+n} \), i.e., \( [y_0, \ldots, y_{s+n-1}]' \) \( \in \ker \left( T_n \right) \). Since \( T_n \) has trivial kernel, \( y_s = \cdots = y_{s+n-1} = 0 \). Then \( y_{s-k+1} = y_{s-k+2} = \cdots = y_s = y_{s+1} = \cdots = y_{s+n-1} = 0 \). Hence the last \( n + k - 1 \) entries of any vector in \( \ker \left( T_{s+n} \right) \) are all 0. By Corollary 2.4 and Proposition 2.6, \( v_{s+n} < v_{s+n-1} < \cdots < v_s < \cdots < v_{s-k+1} \). Since \( v_{s+n} > 0 \) by assumption, \( v_{s-k+1} \geq k \), contradicting Lemma 2.11. By contradiction, \( v_{s+n} = 0 \). □

**Lemma 2.16.** If \( v_m > 0 \) then \( \ker(T_m) \) contains a non-trivial vector \( v \) such that \( \bar{v} = zv \), for some \( z \in F \).

**Proof.** \([1]\)\( \in \ker(T_1) \), so we may suppose \( m > 1 \). By Proposition 2.2, \( v_m = v_{m-1} \pm 1 \). First suppose \( v_{m-1} < v_m \). If \( v_{m-1} = 0 \) then \( v_m = 1 \) and \( \ker(T_m) \) is spanned by a vector \( v \) satisfying the conclusion of the lemma, by Proposition 2.6. If \( 0 < v_{m-1} < v_m \) there is a positive integer \( n < m \), and a non-trivial vector \( k = [k_0, \ldots, k_{n-1}]' \in F^n \), such that (i) \( k_0 \neq 0 \), (ii) \( \bar{k} = bk \) for some \( b \in F \), and (iii) both \( [k_0, \ldots, k_{n-1}, 0, \ldots, 0]' \) and \( [0, \ldots, 0, k_0, \ldots, k_{n-1}]' \) lie in the kernel of \( T_m \). Hence \( [0, \ldots, 0, k_{n-1}, \ldots, k_0] \) is in \( \ker(T_m) \), so the sum \( v \) of this vector with \( [k_0, \ldots, k_{n-1}, 0, \ldots, 0] \) satisfies the conclusion of the lemma.
Next suppose $v_{m-1} > v_m$. If $v_m = 1$, then by Proposition 2.6 a single vector of the desired form spans $\ker(T_m)$. If $v_{m-1} > v_m > 1$ then again by the proposition there is an $n$, a vector $k$ as above, and $q, r \in \mathbb{N}$ such that $q < n + r$, $q + r + n = m$, and $[q, k_0, \ldots, k_{n-1}, 0]$, and its flip lie in $\ker(T_m)$, where $0_i$ denotes a vector consisting of $r$ 0’s. The sum of the two vectors is a non-trivial flip-symmetric vector in $\ker(T_m)$. □

Lemma 2.17. Suppose $0 \leq n \leq 2k - 3$. If $v_n > 0$ then $v_{n+k} > 0$.

Proof. Suppose $n \in \{0, \ldots, 2k - 3\}$ and $v_n > 0$. By the preceding lemma there is a non-trivial vector $[y_0, \ldots, y_{n-1}]^t$ in the kernel of $T_n$ such that $[y_{n-1}, \ldots, y_0] = a[y_0, \ldots, y_{n-1}]^t$, some $a \in F$. Let $y = [y_0, \ldots, y_{n-1}, 0, \ldots, 0]^t = [y_0, \ldots, y_{n-1}, y_n, \ldots, y_{n+k-2}]$ be the vector obtained by appending $k - 1$ 0’s to $[y_0, \ldots, y_{n-1}]^t$. Since $[y_0, \ldots, y_{n-1}]^t \in \ker(T_n)$, $y$ lies in the right kernel of the matrix consisting of the first $n$ rows of $T_{n+k-1}$, namely,

\[
\begin{bmatrix}
  d_0 & -d_1 & -d_2 & \cdots & -d_{k-1} & 0 & 0 & 0 & \cdots & 0 \\
  d_1 & d_0 & -d_1 & \cdots & -d_{k-2} & -d_{k-1} & 0 & 0 & \cdots & 0 \\
  d_2 & d_1 & d_0 & \cdots & -d_{k-3} & -d_{k-2} & -d_{k-1} & 0 & \cdots & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  d_{n-2} & d_{n-3} & \cdots & d_0 & -d_1 & -d_2 & \cdots & \cdots & -d_{k-1} & 0 \\
  d_{n-1} & d_{n-2} & d_{n-3} & \cdots & d_1 & d_0 & -d_1 & \cdots & \cdots & -d_{k-1}
\end{bmatrix}
\]

(taking $d_m = 0$ if $m \geq k$). One can recursively obtain entries $y_{n+k-1}, \ldots, y_{n+k-1}$ so that $[y_0, \ldots, y_{n+k-1}]^t$ lies in the kernel of the matrix consisting of all but the last $k - 1$ rows of $T_{n+s}$, namely,

\[
\begin{bmatrix}
  d_0 & -d_1 & \cdots & -d_{k-1} & 0 & \cdots & 0 \\
  d_1 & d_0 & \cdots & -d_{k-2} & -d_{k-1} & 0 & \cdots & 0 \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  d_{s-1} & d_{s-2} & \cdots & d_0 & \cdots & -d_{k-1} & 0 & \cdots & 0 \\
  d_s & d_{s-1} & \cdots & d_{s-1} & d_0 & \cdots & \cdots & \cdots & 0 \\
  0 & d_{s-1} & \cdots & d_{s-2} & d_{s-1} & d_s & \cdots & \cdots & 0 \\
  0 & \cdots & 0 & d_{s-1} & d_{s-2} & d_{s-1} & \cdots & \cdots & \cdots & 0
\end{bmatrix}
\]

This is done by choosing $y_{n+k-1}$ so that $[y_0, \ldots, y_{n+k-1}]^t$ has scalar product 0 with $[d_n, d_{n-1}, d_{n-2}, \ldots, -d_1, \ldots, -d_{k-1}]$, then choosing $y_{n+k}$ so that the vector $[y_0, \ldots, y_{n+k}]^t$ has product 0 with $[d_{n+1}, \ldots, d_1, d_0, -d_1, \ldots, -d_{k-1}]$, and so on. It follows, as in the proof of Lemma 2.13, that $0, \ldots, 0, y_0, \ldots, y_{n+k-1}$ is the beginning of a periodic sequence whose period is a divisor of $s$. In particular the last $n - k - 1$ elements of this string agree with the first $n - k - 1$ elements, namely $0, \ldots, 0, y_0, \ldots, y_{n-1}$, which is the same as $0, \ldots, 0, 0, \ldots, y_{n-1}$,
\[ x^{-1}y_{n-2}, \ldots, x^{-1}y_{0}. \] It follows that since \([y_{0}, \ldots, y_{n-1}]'\) lies in the kernel of \(T_n\), \([y_{0}, \ldots, y_{s+n-1}]'\) lies in the kernel of the matrix consisting of the last \(n\) rows of \(T_{s+n}\). Hence \([y_{0}, \ldots, y_{s+n-1}]'\) \(\in\ker(T_{s+n})\). Since \([y_{0}, \ldots, y_{n-1}]'\) is non-trivial, so of course is \([y_{0}, \ldots, y_{s+n-1}]'\), and therefore \(v_{s+n} > 0. \quad \square \)

**Proof of theorem.** It follows from the two preceding lemmas that if \(0 \leq n \leq 2k - 3\) that \(v_n = v_{s+n}\). Combining this with Lemma 2.14 gives the result. \(\square\)

**Theorem 2.18.** Assume the same hypotheses as above. If \(q = js - k + 1\) for some positive integer \(j\), then for any non-negative integer \(r \leq q\), \(v_{q+r} = v_{q-r}\).

**Proof.** For any \(n \geq 2k - 1\) let \(Z_n\) be the matrix obtained from \(T_n\) by deleting its last \(k - 1\) rows. Since \(d_{k-1} \neq 0\), \(Z_n\) has maximal rank and therefore has nullity \(k - 1\). Following the proof of Lemma 2.13 it is not difficult to show that if \(0, 0, \ldots, 0, y_0, \ldots\) is the impulse response sequence corresponding to \([c_{k-1}, \ldots, c_1, c_0, -c_1, \ldots, -c_{k-2}]\) (so that \(y_0 = 1\) and is preceded by \(2k - 3\) 0’s), the kernel of \(Z_n\) is spanned by the \(k - 1\) vectors \(y_0(n) = [y_0, \ldots, y_{n-1}]', y_1(n) = [0, y_0, \ldots, y_{n-2}]', y_2(n) = [0, 0, y_0, \ldots, y_{n-3}]', \ldots, y_{k-2}(n) = [0, \ldots, 0, y_0, \ldots, y_{n-k+1}]'. \) Fix \(q = 2s - k + 1\) then by Theorem 2.10, \(v_q = k - 1\) and therefore \(\ker(T_q) = \ker(Z_q)\), so that \(y_0(q), \ldots, y_{k-2}(q)\) span the kernel of \(T_q\). Let \(v_0(q), \ldots, v_{k-2}(q)\) be the vectors of length \(2k - 2\) obtained by taking last \(2k - 2\) entries of \(y_0(q), \ldots, y_{k-2}(q)\), respectively. Observe from the form of the last \(k - 1\) rows of \(T_q\) that \(v_0(q), \ldots, v_{k-1}(q)\) span the kernel of the matrix

\[
D = \begin{bmatrix}
d_{k-1} & \ldots & d_1 & d_0 & -d_1 & \ldots & -d_{k-2} \\
0 & d_{k-1} & d_2 & d_1 & d_0 & \ldots & -d_{k-3} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & \ldots & 0 & d_{k-1} & d_{k-2} & d_{k-3} & \ldots & d_0
\end{bmatrix}.
\]

Note that for any \(n \geq 2k - 1\) a vector \(\sum \alpha_i y_i(n)\) lies in the kernel of \(T_n\) if and only if \(\sum \alpha_i y_i(n) \in \ker(D)\). Note also that for \(i = 0, 1, \ldots, k - 2\) and for any \(r \in \{0, 1, 2, \ldots, s - 1\}\), \(v_i(q + r) = C^r v_i(q)\) (respectively, \(v_i(q - r) = C^{-r} v_i(q)\)). Hence \(\sum \alpha_i y_i(q + r) \in \ker(T_{q+r})\) if and only if there are \(\beta_i \in F, \ i = 0, \ldots, k - 2, \) such that \(\sum \alpha_i C^r v_i(q) = \sum \beta_i v_i(q)\). Taking \(C^{-r}\) of this equation shows that \(\sum \alpha_i y_i(q + r) \in \ker(T_{q+r})\) if and only if there are \(\beta_i\) such that \(\sum \beta_i C^{-r} y_i(q) = \sum \beta_i y_i(q - r) = \sum \alpha_i y_i(q) \in \ker(D)\), or equivalently, such that \(\sum \beta_i y_i(q - r) \in \ker(T_{q-r})\). Hence \(\dim(\ker(T_{q+r})) = \dim(\ker(T_{q-r}))\), i.e., \(v_{q+r} = v_{q-r}\) for \(q = 2s - k + 1\) and \(r = 0, 1, \ldots, s - 1\). One can then use the periodicity of the nullity sequence, Theorem 2.10, to conclude that \(v_{q+r} = v_{q-r}\) for all \(q = js - k + 1, j \in \mathbb{N}, \) and all \(r = 0, \ldots, q\). \(\square\)
3. Toeplitz matrices with eventually periodic signatures

We apply the results of the preceding section on the nullity sequences of Toeplitz matrices of finite bandwidth to obtain analogous results on the nullity sequences of certain skew-symmetric Toeplitz matrices over finite fields. More precisely, let $\mathcal{A}$ be a skew-symmetric Toeplitz matrix over a finite field whose signature sequence (see Definition 2.1) $(a) = a_0, a_1, \ldots$, is eventually periodic. We show in Theorem 3.7 that the nullity sequence $f(a_n^T) : n \in \mathbb{N}$, where $a_n$ is the nullity of the $n \times n$ corner matrix of $\mathcal{A}$, is eventually periodic. This is done by associating with $\mathcal{A}$ a certain skew-symmetric Toeplitz matrix $T$ over $F$ of finite bandwidth. We prove in Theorem 3.7 that the period of the eventually periodic part of the nullity sequence for $\mathcal{A}$ divides the period of the nullity sequence for $T$.

**Definition 3.1.** For a fixed positive integer $n$, for $i, j \in \{1, \ldots, n\}$, $i \neq j$, and for fixed $\mu \in F$, $E_{ij}^\mu$ is the elementary matrix with $\mu$ in the $(i, j)$ position, 1’s along the main diagonal, and 0’s elsewhere.

We shall omit the superscript for $E_{ij}^\mu$ since the size of the matrices will be clear from the context in which they are used. By trivial calculations it follows that if $M$ is an $n \times n$ matrix, $E_{ij}^\mu M$ is obtained from $M$ by adding $\mu$ times row $j$ to row $i$, and $ME_{ij}^\mu$ by adding $\mu$ times column $i$ to column $j$. The inverse of $E_{ij}^\mu$ is $E_{ij}^{-\mu}$, and its transpose is $E_{ji}^\mu$. Hence if $S$ is a skew-symmetric $n \times n$ matrix then so is $E_{ij}^\mu SE_{ij}^\mu$. In particular, the latter matrix has 0 diagonal.

**Definition 3.2** ([7, Chapter IV]). A pair $B, C$ of $n \times n$ matrices with entries in a finite field $F$ are said to be congruent if $B^U = C$ for some invertible matrix $U$ (where $U^T$ is the transpose of $U$).

**Remark 3.3.** It is clear that congruence is an equivalence relation. It is also obvious that congruent matrices have the same rank. It is difficult in general to determine when two matrices of the same rank are congruent [7].

In what follows we shall fix $\{a_n : n \in \mathbb{Z}^+\}$, an eventually periodic sequence in $F$, and we denote by $\{a(n) : n \in \mathbb{Z}\}$ the doubly-infinite sequence $\{\ldots, a_1, a_0, -a_1, \ldots\}$ cited in Proposition 2.9. The following result is an easy consequence of that proposition.

**Lemma 3.4.** Suppose $\{a_n : n \in \mathbb{Z}^+\}$ is a sequence in $F$ such that $\{a(n) : n \in \mathbb{Z}\}$ is periodic. Let $\mathcal{A}$ be the skew-symmetric Toeplitz matrix having $\{a_n : n \in \mathbb{Z}^+\}$ as its signature sequence. Then there is a positive integer $m$ such that for $n \geq m$, $\mathcal{A}_n$ is congruent to the $n \times n$ matrix with corner $\mathcal{A}_{m-1}$ and with 0’s everywhere else.
Proof. By Proposition 2.8 there is a non-trivial vector which annihilates \(\{a(n) : n \in \mathbb{Z}\}\). It will be convenient to write the annihilating vector as the flip \(\tilde{x} = [x_{m-1} \ldots, x_0]\) of a vector \(x = [x_0, \ldots, x_{m-1}]\). We may assume that \(x_0 = 1\) and that \(x_{m-1}\) is non-zero. For each \(n \geq m\), let \(E_n = E_{n-m+1,n}(x_{m-1}) \cdots E_{n-1,n}(x_1)\). Then \(E_n^t E_n\) is an \(n \times n\) matrix with \(\mathcal{A}_{n-1}\) in the upper left corner and with last row and column all 0. Continuing one sees that \(E_n^t E_n \cdots E_1^t E_1\) is the \(n \times n\) matrix with \(\mathcal{A}_{m-1}\) in the upper left corner and 0’s elsewhere.

Lemma 3.5. Suppose \(\{a_n : n \in \mathbb{Z}^+\}\) is eventually periodic but \(\{a(n) : n \in \mathbb{Z}\}\) is not periodic. Then there is an \(m \in \mathbb{N}\), a vector \(x = [x_0, \ldots, x_{m-1}] \in F^m\), with \(x_0 = 1\) and \(x_{m-1} \neq 0\), and an integer \(k > 1\) such that the flip \(\tilde{x}\) of \(x\) annihilates the sequence \(\{a(k - m + 1), a(k - m + 2), a(k - m + 3), \ldots\}\) but not \(\{a(k - m), a(k - m + 1), \ldots\}\).

Proof. Since \(\{a_n : n \in \mathbb{Z}^+\}\) is eventually periodic but \(\{a(n) : n \in \mathbb{Z}\}\) (the sequence, \(\ldots, a_2, a_1, a_0, -a_1, -a_2, \ldots\)) is not periodic there is an \(r \in \mathbb{Z}\) such that the sequence \(a(r+1), a(r+2), \ldots\) is periodic but \(a(r), a(r+1), \ldots\) is not. Let \(x = [x_0, \ldots, x_{m-1}]\) be a vector whose flip \(\tilde{x} = [x_{m-1}, \ldots, x_0]\) annihilates the former sequence. By Proposition 2.8 we may assume the leading entry \(x_{m-1} \neq 0\). We may also assume that \(\tilde{x}\) has been chosen to have minimal length among all non-trivial vectors annihilating the sequence, so that, in particular \(x_0 \neq 0\). We may assume \(x_0 = 1\). We shall show that \(r > -m + 2\). For otherwise the sequence \(\mathcal{G} = \{a(-m+2), a(-m+3), \ldots\}\) would be periodic. Then consider the infinite matrix

\[
B = \begin{bmatrix}
-a_1 & a_0 & a_1 & \cdots & a_{m-2} \\
-a_2 & a_1 & a_0 & \cdots & a_{m-3} \\
-a_3 & a_2 & a_1 & \cdots & a_{m-4} \\
\vdots & & & \ddots & \ddots
\end{bmatrix}
\]

Since \(\tilde{x}\) annihilates \(\mathcal{G}\), its flip \(x\) lies in the kernel of \(B\). Suppose \(y = [y_0, \ldots, y_{m-1}] \neq x\) is another non-trivial vector in \(\ker(B)\). Replacing \(y\) with a linear combination of \(x\) and \(y\), if necessary, we may assume that \(y_0 = 0\). Since \(y \in \ker(B)\) it follows that there is a \(p \geq -m + 2\) such that \(\tilde{y}\) annihilates \(a(p), a(p+1), \ldots\). Since \(y_0 = 0\) there is a non-trivial vector \(z\) of shorter length than \(\tilde{x}\) which annihilates \(a(p), a(p+1), \ldots\). Since \(z\) annihilates \(a(p), a(p+1), \ldots\), it also annihilates \(a(-m+2), a(-m+3), \ldots\), contradicting the minimality of the length of \(x\). Hence \(x\) spans the kernel of \(B\). Hence \(B\) has nullity 1. If \(K\) is the matrix obtained from \(B\) by removing its first column, then by the minimality of \(m\), \(K\) must have full rank. Let \(\mathcal{A}\) be the skew-symmetric Toeplitz matrix with signature \(\{a_n : n \in \mathbb{Z}^+\}\). Note that \(\mathcal{A}_{m-1}\) is the matrix consisting of the first \(m-1\) rows of \(K\). We claim that \(\mathcal{A}_{m-1}\) has full rank. To see this, note that by the symmetry of \(B\) it follows that since \(x \in \ker(B)\), the vector \([x_{m-1}, \ldots, x_0]\) lies in the left kernel of \(B\). Since that is the case, and since
both \( x_{m-1} \) and \( x_0 \) are non-zero, it follows that row \( m \) is a linear combination of rows 1 through \( m - 1 \) of \( B \), that row \( m + 1 \) is a linear combination of rows 2 through \( m + 1 \) of \( B \), and so on, so that rows \( m, m + 1, \ldots \), of \( B \) are linear combinations of rows 1 through \( m - 1 \) of \( B \). Hence rows \( m, m + 1, \ldots, \) of \( K \) are linear combinations of rows 1 through \( m - 1 \) of \( K \). Hence \( m - 1 = \text{rank}(K) = \text{rank}(\mathcal{A}'_{m-1}) = \text{rank}(\mathcal{A}_{m-1}) \). Hence \( \mathcal{A}_{m-1} \) has nullity \( \nu(\mathcal{A}_{m-1}) = 0 \). Hence \( \nu(\mathcal{A}'_n) = 1 \), by Proposition 2.2. Since \( x \in \ker(B), x \) lies in the kernel of the matrix consisting of all but the first row of \( \mathcal{A}'_m \). Since \( \nu(\mathcal{A}'_n) = \nu(\mathcal{A}'_m) = 1, x \in \ker(\mathcal{A}'_m) \). By the symmetry of \( \mathcal{A}'_m \), then since \( x \in \ker(\mathcal{A}'_m), \bar{x} \in \ker(\mathcal{A}'_m) \). Since \( \nu(\mathcal{A}'_m) = 1, x \) and its flip \( \bar{x} \) are scalar multiples of each other. Therefore, \( \bar{x} \) annihilates \( a(-m + 2), a(-m + 3), \ldots, \), it must actually annihilate \( \{a(n) : n \in \mathbb{Z}\} \) (see the proof of Proposition 2.9). Hence the latter sequence is periodic, by an obvious generalization of Proposition 2.8 to doubly-infinite sequences. But this sequence is not periodic, by hypothesis. By this contradiction we conclude that \( r > -m + 2 \). Hence there is a non-negative integer \( k \) which satisfies the last statement of the proposition. \( \square \)

**Lemma 3.6.** Suppose \( \{a_n : n \in \mathbb{Z}^+\} \) is an eventually periodic sequence with \( a_0 = 0 \). Suppose \( \{a(n) : n \in \mathbb{Z}\} \) is not periodic. Let \( \mathcal{A} \) be the skew-symmetric Toeplitz matrix whose signature is \( \{a_n : n \in \mathbb{Z}^+\} \). Then there are positive integers \( m, k, \) and elements \( e_1, \ldots, e_{k-1}, d_1, \ldots, d_{k-1} \) of \( F \), with \( d_{k-1} \neq 0 \), such that, for any \( n > m + 2k, \mathcal{A}_n \) is congruent to the \( n \times n \) matrix \( B_n \) below.

\[
\begin{bmatrix}
\mathcal{A}_{m-1} & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & -d_1 & -d_2 & \cdots & -d_{k-1} & 0 & \cdots & 0 \\
0 & 0 & d_1 & -d_1 - d_2 & \cdots & -d_{k-2} & -d_{k-1} & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 0 & d_{k-1} & \cdots & d_1 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & -d_1 & \cdots & -d_{k-1} & 0 \end{bmatrix}
\]

**Proof.** Let \( k, m, x \) be as in preceding lemma. Fix \( n > m \). Let \( e_0, \ldots, e_{k-1} \in F \) satisfy 

\[
[a(-m + 1), \ldots, a(-1), a(0)], \bar{x} = -e_0, [a(-m + 2), \ldots, a(-1), a(0)];
\]

\[
a(1)] \cdot \bar{x} = -e_1, \ldots, [a(-m + k), \ldots, a(k - 1)] \cdot \bar{x} = -e_{k-1}.
\]

By the preceding lemma \( e_{k-1} \neq 0 \), but for \( j > k, -e_j = [a(-m + j), \ldots, a(j - 1)] \cdot x = 0 \). Since \( x_0 = 1 \) it follows from these equations that if \( E_n = E_{n-m+1,n}(x_{m-1}) \)

\[
\cdots E_{n-1,n}(x_1), \mathcal{A}_n E_n \text{ has last column}
\]


\[0, \ldots, 0, -e_{k-1}, \ldots, -e_1, -e_0, \ldots\]

and therefore
\[
E_n^t A_n E_n = \begin{bmatrix} A_{n-1} & 0 \\ \vdots & \vdots \\ 0 & -e_1 \end{bmatrix}.
\]

For \(i \in \mathbb{N}\) let \(d_i = \sum_{j=0}^{m-1} x_i e_i + j\). Since \(e_q = 0\) for \(q \geq k\), \(d_q = 0\) for \(q \geq k\). Also \(d_{k-1} = x_0 e_{k-1} = e_{k-1} \neq 0\). If \(E_{n-1} = E_{n-m,n-1}(x_{m-1}) \cdots E_{n-2,n-1}(x_1)\), then
\[
E_n^t E_n^t A_n E_n E_{n-1} = \begin{bmatrix} A_{n-2} & 0 \\ \vdots & \vdots \\ 0 & -e_1 \end{bmatrix}.
\]

Continuing in this fashion, one sees that if \(E_m^t \cdots E_n^t A_n E_n \cdots E_1\) has the form of the matrix in the statement of the theorem, where \(E_q = E_{q-m+1,q}(x_{m-1}) \cdots E_{q-1,q}(x_1)\), for \(q = m, m + 1, \ldots, n\). \(\square\)

**Theorem 3.7.** Assume the hypotheses and notation of the preceding lemma. Let \(T\) be the skew-symmetric Toeplitz matrix with signature sequence \([d_0, d_1, \ldots, d_{k-1}, 0, \ldots]\). Then the nullity sequence \(\{v_n(\mathcal{A}) : n \in \mathbb{N}\}\) of \(\mathcal{A}\) is eventually periodic. Its period is a divisor of the period of \(\{v_n(T) : n \in \mathbb{Z}^+\}\).
Proof. By Theorem 2.10 \( \{v_n(T) : n \in \mathbb{Z}^+ \} \) is periodic. Let \( s \) be its period. We shall show that \( v_n(\mathcal{A}) = v_{n+s}(\mathcal{A}) \) for \( n > m + 2k - 1 \). For such \( n \), let \( D_n \) be the matrix consisting of all but the first \( m + k - 2 \) rows of the matrix \( B_n \) in the preceding lemma. Since \( d_{n-1} \neq 0 \), \( D_n \) has nullity \( m + k - 1 \). Following the proof of Lemma 2.13, it is not difficult to show that if we write a vector \( y \) in the kernel of \( D_n \) as \( [y_n, \ldots, y_0] \), then the vector \( x = [y_{n-m+1}, \ldots, y_0, 0, 0, \ldots, 0] \) (with \( k - 1 \) \( 0 \)'s appended to the end of \( y \), and \( m - 1 \) entries deleted from the beginning of \( y \)), is annihilated by \( [d_{k-1}, \ldots, d_1, d_0, -d_1, \ldots, d_{k-1}] \). Also from the proof of the lemma it follows that there is a linear one to one correspondence between vectors \( y \in \ker(D_n) \) as above and vectors \( \hat{y} \in D_{n+s} \) where the last \( n + 1 \) elements of \( \hat{y} \) are the same as \( y \) and if \( \hat{x} \) is to obtained by appending \( k - 1 \) \( 0 \)'s to the end of \( \hat{y} \), then \( \hat{x} \) is annihilated by \( [d_{k-1}, \ldots, d_1, d_0, -d_1, \ldots, d_{k-1}] \). It follows from the periodicity results in Lemma 2.14 that the first \( m + 2k - 1 \) elements of \( y \) coincide with the first \( m + 2k - 1 \) elements of \( \hat{y} \). Since \( \hat{y} \in \ker(\mathcal{A}_n) \) (respectively, \( \hat{y} \in \ker(\mathcal{A}_{n+s}) \) if and only if the first \( m + 2k - 1 \) elements of \( \hat{y} \) (respectively, \( y \)) form a vector which are annihilated by the matrix consisting of the first \( m + 2k - 1 \) rows of \( B_n \) (respectively, \( B_{n+s} \)) in the statement of the preceding lemma, it follows that \( y \) lies in the kernel of \( B_n \) if and only if \( \hat{y} \) lies in the kernel of \( B_{n+s} \). Hence \( B_n \) and \( B_{n+s} \) have the same nullity. Since congruence preserves nullity, \( \mathcal{A}_n \) and \( \mathcal{A}_{n+s} \) have the same nullity, i.e., \( v_n(\mathcal{A}) = v_{n+s}(\mathcal{A}) \).

4. Examples

We illustrate the results on nullity sequences in the two preceding sections by applying those results to the following examples.

Example 4.1. Let \( F \) be any finite field. Fix \( k \in \mathbb{N} \) and let \( \{d_n : n \in \mathbb{Z}^+ \} \) be the sequence in \( F \) where \( d_{k-1} = 1 \) and \( d_j = 0 \) for \( j \neq k - 1 \). Then the \((2k - 2) \times (2k - 2)\) matrix \( C \) in Theorem 2.10 is the permutation matrix

\[
\begin{bmatrix}
0 & 1 & 0 & 0 & \cdots & 0 & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 & 0 \\
\vdots \\
0 & 0 & 0 & 0 & \cdots & 1 \\
1 & 0 & 0 & 0 & \cdots & 0 & 0 \\
\end{bmatrix},
\]

which has order \( 2k - 2 \). Let \( T \) be the skew-symmetric Toeplitz matrix having \( \{d_n\} \) as its signature, as in Definition 2.1. By Theorem 2.10 the nullity sequence \( \{v_n(T)\} \) is periodic with period \( 2k - 2 \). By the same theorem \( v_n(T) \leq k - 1 \) for all \( n \in \mathbb{N} \), and \( v_n(T) = k - 1 \) for infinitely many \( n \). Hence by Corollary 2.4 the string \( 1, 2, \ldots, k - 2, k - 1, k - 2, \ldots, 2, 1, 0 \) appears infinitely often in the nullity sequence for \( T \). But this string is of length \( 2k - 2 \), and since the period of the
sequence is $2k - 2$, the nullity sequence simply consists of infinitely many copies of this string.

**Example 4.2.** Suppose $F = F_2$ and $\{d_n : n \in \mathbb{Z}^+\}$ is the sequence 0, 1, 0, 1, 0, 0, 0, ... Then $k = 4$ and $C$ is the $6 \times 6$ matrix
\[
\begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0
\end{bmatrix},
\]
which has order 8. According to Theorem 2.10, $v_n \leq 3$ and $v_n = 3$ for $n$ of the form $8j - 3$, $j \in \mathbb{N}$. It then follows from the periodicity of the nullity sequence and the unimodality property of Corollary 2.4 that the sequence just consists of infinitely many copies of the string 10123210.

**Example 4.3.** Consider the periodic bitstream $\{a_n : n \in \mathbb{Z}^+\}$ in $F = F_2$, of period 31, consisting of infinitely many copies of the pattern 0100100001010111011000111110011. Let $A$ be the skew-symmetric Toeplitz matrix having this bitstream as its signature (Definition 2.1). A straightforward calculation shows that $\{a_n : n \in \mathbb{Z}^+\}$ is annihilated (see Definitions 2.5 and 2.7) by the vector $v = [1, 0, 0, 1, 0, 1] \in F^6$. (No non-trivial vector in $F^5$ annihilates the sequence, however, since a sequence annihilated by any non-trivial vector $w \in F^n$ has period of length at most $2^n - 1$ [4, Theorem 6.7].) Using $v$ as in Lemma 3.6 to obtain matrices congruent to $A_n$, for sufficiently large $n$, and applying Theorem 3.7, one observes that the period of the eventually periodic part of $\{v_n(A)\}$, divides the period of $\{v_n(T)\}$, where $T$ is the skew-symmetric Toeplitz matrix with signature 0001000000. . . . From Example 4.1, $\{v_n(T)\}$ has period 6 and consists of infinitely many copies of the pattern 123210. Then by Theorem 3.7 $\{v_n(A)\}$ is eventually periodic with period length dividing 6. By the first paragraph of the proof of that theorem, in fact, one sees that $\{v_n(A)\}$ must be periodic for $n > 12$ (since $v \in F^6 = F^m$ and since $k = 4$, using the notation of that proof). Therefore by computing $v_n(A)$ for $n = 1, 2, \ldots, 18$, one concludes that nullity sequence of $A$ is 10101210101210101210. . . ., with the pattern 101210 continued forever. Hence this sequence is eventually periodic with preperiod 2 and period length 6. Note that although the nullity sequences for $A$ and for $T$ have the same period, the patterns of their nullity sequences differ.

**Example 4.4.** Consider the bitstream $\{a_n : n \in \mathbb{Z}^+\}$ in $F_2$ of period 7 consisting of the pattern 0100111 repeated forever, and let $A$ be the corresponding skew-symmetric Toeplitz matrix. Note that the bitstream is annihilated by $[1, 0, 0, 1, 1, 1] \in F^6$. 

Following the proof of Lemma 3.6 one associates with $A$ the skew-symmetric Toeplitz matrix $T$ with signature $01010000,\ldots$. By Example 4.2 the nullity sequence for $T$ has period 8. Hence the nullity sequence for $A$ must have periodic part with period length dividing 8, by Theorem 3.7. In fact one can apply the proof of Lemma 3.6 and Theorem 3.7 as in the previous example to conclude that the nullity sequence for $A$ consists of the pattern $10$ repeated forever.

Acknowledgements

The authors are grateful to Professor Alexis Alevras for alerting us to an error in the original manuscript.

References