Set Intersection Matrices*

H. J. RYSER

California Institute of Technology, Pasadena, California 91125

Received January 23, 1981

DEDICATED TO PROFESSOR MARSHALL HALL, JR., ON

THE OCCASION OF HIS RETIREMENT

Let $A$ be a matrix of size $m$ by $n$ with elements in a field $F$. Let $X = \text{diag}[x_1, \ldots, x_n]$ be a diagonal matrix of order $n$, where $x_1, \ldots, x_n$ are $n$ independent indeterminates over $F$. Throughout the paper we investigate the matrix equation $AXA^T = Y$, where $A^T$ denotes the transpose of the matrix $A$. We call this equation the fundamental matrix equation of set intersections and we call the symmetric matrix $Y$ of order $m$ the set intersection matrix defined by $A$. The terminology arises from the important special case in which $A$ is a $(0, 1)$-matrix. Then $A$ may be regarded as the incidence matrix for $m$ subsets of an $n$-set and in this special case the equation gives us a complete description of the pairwise intersection patterns of the subsets. Moreover, it displays this information in an exceedingly compact form. Our paper is primarily concerned with the derivation of four theorems involving the set intersection matrix $Y$. Two of the theorems reveal the extent to which the polynomial $\det(Y)$ and the characteristic polynomial $f(z)$ of $Y$ characterize the set intersection matrix $Y$. The remaining two theorems determine simple necessary and sufficient conditions for the irreducibility of the polynomial $\det(Y)$ in the polynomial ring $F^* = F[x_1, \ldots, x_n]$ and for the irreducibility of the characteristic polynomial $f(z)$ of $Y$ in the polynomial ring $F^*[z]$. Our results are of interest from both a matrix theoretic and combinatorial point of view.

1. Introduction

Let $A = [a_{ij}]$ be a matrix of $m$ rows and $n$ columns with elements in a field $F$. We say that $A$ is of size $m$ by $n$. Let $X$ be the diagonal matrix of order $n$

$$X = \text{diag}[x_1, \ldots, x_n], \quad (1.1)$$

* This research was supported in part by the National Science Foundation under Grant Number MCS78-21599.
where \( x_1, \ldots, x_n \) are \( n \) independent indeterminates over \( F \). Throughout the paper we investigate the matrix equation

\[ A X A^T = Y, \]

where \( A^T \) denotes the transpose of the matrix \( A \). The elements of all of the matrices in (1.2) may be regarded as belonging to the polynomial ring

\[ F^* = F[x_1, \ldots, x_n]. \]

We call (1.2) the \textit{fundamental matrix equation of set intersections} and we call the symmetric matrix \( Y \) of order \( m \) the \textit{set intersection matrix} defined by \( A \). The elements of the set intersection matrix \( Y \) are linear forms in the indeterminates \( x_1, \ldots, x_n \) and for this reason we sometimes write

\[ Y = Y(x_1, \ldots, x_n). \]

Our paper is primarily concerned with the derivation of four theorems involving the set intersection matrix \( Y \). Two of the theorems reveal the extent to which the polynomial \( \det(Y) \) in \( F^* \) and the characteristic polynomial \( f(z) \) of \( Y \) in \( F^*[z] \) characterize the set intersection matrix \( Y \). The remaining two theorems determine simple necessary and sufficient conditions for the irreducibility of the polynomial \( \det(Y) \) in \( F^* \) and for the irreducibility of the characteristic polynomial \( f(z) \) of \( Y \) in \( F^*[z] \). Our results are of interest from both a matrix theoretic and combinatorial point of view.

Matrix equations of the form (1.2) were studied earlier in [9] and a somewhat more general matrix equation has been studied in [10]. Related literature that has also motivated these investigations includes [2–7, 11–15].

The "set intersection" terminology that we have introduced arises from the important special case of (1.2) in which \( A \) is a \((0, 1)\)-matrix and \( x_1, \ldots, x_n \) are independent indeterminates over the field of rational numbers \( Q \). More precisely, let \( S = \{x_1, \ldots, x_n\} \) be an \( n \)-set (a set of \( n \) elements) and let \( S_1, \ldots, S_m \) be subsets of \( S \). We set \( a_{ij} = 1 \) if \( x_j \) is a member of \( S_i \) and we set \( a_{ij} = 0 \) if \( x_j \) is not a member of \( S_i \). The resulting \((0, 1)\)-matrix

\[ A = [a_{ij}] \]

of size \( m \) by \( n \) is the familiar \textit{incidence matrix} for the subsets \( S_1, \ldots, S_m \) of \( S \). It is clear that \( A \) characterizes the configuration of subsets. Now let us regard \( x_1, \ldots, x_n \) as independent indeterminates over \( Q \). Then the set intersection matrix \( Y \) has in its \((i, i)\) position the sum of the indeterminates in \( S_i \). More generally, the set intersection matrix \( Y \) has in its \((i, j)\) position the sum of the indeterminates in \( S_i \cap S_j \). Thus in this special case the fundamental matrix equation on set intersections gives us a complete description of the intersection patterns \( S_i \cap S_j \) for the subsets \( S_1, \ldots, S_m \) of \( S \). Moreover, it
H. J. RYSER

displays this information in an exceedingly compact form. We may set

\[ x_1 = \cdots = x_n = 1 \]

and then the matrix equation (1.2) reduces to the classical
equation

\[ A A^T = Y(1, \ldots, 1) \tag{1.6} \]

that reveals the cardinalities of the set intersections \( S_i \cap S_j \).

2. The Structure of \( \det(Y) \)

We return to the general matrix equation (1.2) and the set intersection
matrix \( Y \) and verify that

\[ \text{rank}(Y) = \text{rank}(A). \tag{2.1} \]

In order to prove (2.1) we let \( A \) be of rank \( r \). Then it follows from (1.2) that

\[ \text{rank}(Y) \leq \text{rank}(A) = r. \tag{2.2} \]

There exist permutation matrices \( P \) and \( Q \) of orders \( m \) and \( n \), respectively, such that

\[ PAQ = B = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix}, \tag{2.3} \]

where the submatrix \( B_1 \) of \( B \) is of order and rank \( r \). Let

\[ BXB^T = PAQQ^TA^TP^T = Z. \tag{2.4} \]

Then

\[ \text{rank}(Z) = \text{rank}(Y) \tag{2.5} \]

because \( Z \) is obtained from \( Y \) by simultaneous permutations of rows and
columns and a relabeling of the indeterminates \( x_1, \ldots, x_n \). Let

\[ X_1 = \text{diag}[x_1, \ldots, x_r], \quad X_2 = \text{diag}[x_{r+1}, \ldots, x_n] \tag{2.6} \]

and

\[ B_1 X_1 B_1^T + B_2 X_2 B_2^T = W = W(x_1, \ldots, x_n). \tag{2.7} \]

Then \( W \) is the submatrix of \( Z \) of order \( r \) in the upper left corner of \( Z \) and we
assert that

\[ \det(W) \neq 0. \tag{2.8} \]
This assertion follows because \(\det(W) = 0\) implies

\[
\det(B, X, B^T) = \det(W(x_1, \ldots, x_r, 0, \ldots, 0)) = 0,
\]
and this is a contradiction. Hence

\[
\text{rank}(Z) = \text{rank}(Y) \geq r
\]
and (2.1) is valid.

We now study the structure of the polynomial \(\det(Y)\) in the polynomial ring \(F^*\). We suppose that the matrix \(A\) of size \(m\) by \(n\) with elements in \(F\) is of rank \(m\). Then we know that the set intersection matrix \(Y\) satisfies \(\det(Y) \neq 0\).

We now assert that we may write \(\det(Y)\) in the form

\[
\det(Y) = \sum c_i y_i,
\]
where the \(y_i\) are products of \(m\) distinct elements of \(x_1, \ldots, x_n\) and the \(c_i\) are squares of nonzero elements of \(F\). This assertion follows easily from the multiplicative property of compound matrices [8]. Thus we may take the \(m\)th compound of the matrix equation (1.2) and thereby obtain

\[
\det(Y) = C_m(Y) = C_m(A) C_m(X)(C_m(A))^T.
\]

Then by the structure of (2.12) we see that each \(y_i\) in (2.11) with \(c_i \neq 0\) is associated with a unique set of \(m\) linearly independent columns of \(A\). The coefficient \(c_i\) of \(y_i\) is merely the square of the determinant of these \(m\) linearly independent columns. Furthermore, all sets of \(m\) linearly independent columns of \(A\) are accounted for in (2.11).

We also note that each indeterminate \(x_i\) must actually be present in some term of the polynomial \(\det(Y)\), except in the trivial situation in which column \(i\) of \(A\) is a column of 0's. This is the case because every nonzero column of \(A\) may be extended to a basis of the column space.

\section{3. Congruence over \(F\)}

We return to the set intersection matrix \(Y\) of order \(m\) defined by the matrix \(A\) of size \(m\) by \(n\). We note that any principal submatrix of \(Y\) is again a set intersection matrix defined by the appropriate rows of \(A\). Furthermore, if \(A\) and \(B\) are two matrices of size \(m\) by \(n\) that define the same set intersection matrix \(Y\), then it is elementary to verify that \(B\) is obtainable from \(A\) by multiplication of various columns of \(A\) by \(-1\).
Now let \( Y = Y(x_1, \ldots, x_n) \) be a set intersection matrix of order \( m \) defined by the matrix \( A \) of size \( m \) by \( n \). Suppose that \( P \) is a nonsingular matrix of order \( m \) with elements in \( F \) and let
\[
Z = PYP^T.
\] (3.1)

Then \( Z = Z(x_1, \ldots, x_n) \) is also a set intersection matrix and we say that the two set intersection matrices \( Y \) and \( Z \) are congruent over \( F \). Let the set intersection matrix \( Z \) of order \( m \) be defined by the matrix \( B \) of size \( m \) by \( n \). Then under congruence over \( F \) it follows that \( B \) is obtainable from \( A \) by multiplication of \( A \) on the left by the nonsingular \( P \) and by multiplication of various columns of \( A \) by \(-1\).

We now prove that a simple determinantal criterion is available for deciding whether or not two nonsingular set intersection matrices of order \( m \) are congruent over \( F \).

**THEOREM 3.1.** Let \( Y \) and \( Z \) be nonsingular set intersection matrices of order \( m \). Then \( Y \) and \( Z \) are congruent over \( F \) if and only if
\[
\det(Y) = c^2 \det(Z),
\] (3.2)

where \( c \neq 0 \) and \( c \) in \( F \).

Our proof requires a special case of the following lemma. A square submatrix of a matrix \( A \) is called critical provided that the submatrix has exactly two nonzero elements on each of its lines. (A line of a matrix designates either a row or a column of the matrix.)

**LEMMA 3.2.** Let \( A \) be a matrix of size \( m \) by \( n \) with elements in a field \( F \) and let \( B \) be the same matrix as \( A \) apart from the sign of its elements. Now suppose that every critical submatrix of \( A \) has the same determinant as its corresponding critical submatrix in \( B \), except possibly for sign. Then we may multiply certain rows and columns of \( B \) by \(-1\)'s and thereby transform \( B \) into \( A \).

The above lemma is a special case of a more general theorem of Engel and Schneider [11]. This follows at once from a consideration of the symmetric matrices
\[
\begin{bmatrix}
0 & A \\
A^T & 0
\end{bmatrix}
\begin{bmatrix}
0 & B \\
B^T & 0
\end{bmatrix}.
\] (3.3)

I am indebted to R. A. Brualdi for pointing out this fact to me. We remark in passing that it is also possible to prove the lemma directly from first principles by induction on the number of columns in \( A \).
We are now ready to prove Theorem 3.1. Suppose that $Y$ and $Z$ are congruent over $F$. Then there exists a nonsingular matrix $P$ of order $m$ with elements in $F$ such that (3.1) is valid. But then (3.2) follows.

We next prove the reverse implication. Let the set intersection matrix $Y$ of order $m$ be defined by the matrix $A$ and let the set intersection matrix $Z$ of order $m$ be defined by the matrix $B$. Then by the structure of $\det(Y)$ and $\det(Z)$ described in Section 2 we may assume that both of the matrices $A$ and $B$ are of the same size $m$ by $n$. Furthermore, if columns $i_1, \ldots, i_m$ of $A$ are linearly independent then columns $i_1, \ldots, i_m$ of $B$ are also linearly independent. Hence we may without loss of generality assume that columns $1, \ldots, m$ of both $A$ and $B$ are linearly independent. Thus there exist nonsingular matrices $P$ and $Q$ of order $m$ such that

$$PA = [I \ A_1], \quad QB = [I \ B_1],$$

(3.4)

where $I$ is the identity matrix of order $m$. But then by our assumption (3.2) it follows that

$$\det(PAX(PA)^T) = \det(QBX(QB)^T),$$

(3.5)

where in this modified equation we now have $c = 1$ because the coefficient of $x_1 \cdots x_m$ on both sides of (3.5) is equal to 1.

Let $M$ be an arbitrary square submatrix of $A_1$ and let $N$ be the corresponding square submatrix in $B_1$. Then by (3.5) and the structure of the polynomials described in Section 2 it follows that

$$(\det(M))^2 = (\det(N))^2.$$  

(3.6)

Hence it follows that an arbitrary square submatrix of $PA$ has the same determinant as its corresponding square submatrix in $QB$, except possibly for sign. But then by Lemma 3.2 we may multiply certain rows and columns of $QB$ by $-1$'s and thereby transform $QB$ into $PA$. Hence there exist diagonal matrices $D$ and $E$ of orders $m$ and $n$, respectively, with main diagonal elements $\pm 1$ such that

$$PA = DQBE.$$  

(3.7)

But then

$$Y = AXA^T = P^{-1}DQBEX(P^{-1}DQBE)^T$$

$$= P^{-1}DQZ(P^{-1}DQ)^T,$$

(3.8)

whence $Y$ and $Z$ are congruent over $F$. 

4. THE IRREDUCIBILITY OF \( \det(Y) \)

We say that the set intersection matrix \( Y = AXA^T \) splits under congruence over \( F \) provided that \( Y \) is congruent over \( F \) to a direct sum of two set intersection matrices \( Y_1 \) and \( Y_2 \). We note that the same indeterminate cannot appear in both components of a direct sum set intersection matrix. Hence such a direct sum set intersection matrix must have a defining matrix that upon column permutations is also a direct sum of the form

\[
A_1 \oplus A_2 = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}.
\]  

(4.1)

But note that in the direct sum (4.1) the matrices \( A_1 \) and \( A_2 \) are not necessarily square and the 0's denote zero matrices of appropriate sizes. The preceding concepts turn out to be useful in deciding upon the irreducibility of the polynomial \( \det(Y) \) in the polynomial ring \( F^* = F[x_1, \ldots, x_n] \).

**Theorem 4.1.** Let \( Y \) be a set intersection matrix of order \( m > 1 \). Then the polynomial \( \det(Y) \) is irreducible in \( F^* \) if and only if the set intersection matrix \( Y \) does not split under congruence over \( F \).

**Proof.** Suppose that \( \text{rank}(Y) < m \). Then \( \text{rank}(A) < m \) and \( Y = AXA^T \) is congruent over \( F \) to a direct sum, one component of which is the zero matrix. Thus the theorem is valid in this case and we henceforth take \( \text{rank}(Y) = m \).

Suppose that \( \det(Y) \) is irreducible in \( F^* \). Then it follows at once that \( Y \) cannot be congruent over \( F \) to a direct sum of two set intersection matrices because this would yield a proper factorization of \( \det(Y) \) in \( F^* \).

It remains to prove that if \( Y \) of rank \( m \) does not split under congruence over \( F \) then \( \det(Y) \) is irreducible in \( F^* \). We now write

\[
f = \det(Y)
\]

(4.2)

and suppose to the contrary that there is some proper factorization of

\[
f = gh
\]

(4.3)

in \( F^* \). We assert that the polynomials \( g \) and \( h \) can have no indeterminates in common. Suppose that an indeterminate \( x_i \) appears in both \( g \) and \( h \). Let \( R \) denote the same polynomial ring as \( F^* \) but with the indeterminate \( x_i \) deleted. Then \( g \) is a polynomial in \( x_i \) with coefficients in \( R \) of degree at least 1 in \( x_i \). The same holds for \( h \). But then \( f \) is a polynomial in \( x_i \) with coefficients in \( R \) of degree at least 2 in \( x_i \), and this is a contradiction. Furthermore, it follows that the polynomials \( g \) and \( h \) are homogeneous of certain degrees, say \( r \) and
Let us say that the polynomial \( g \) contains \( e \) indeterminates and that the polynomial \( h \) contains the remaining \( n - e \) indeterminates, where \( 1 < e < n \). Thus apart from column permutations \( A \) is of the form

\[
\begin{bmatrix}
A_1 & A_2
\end{bmatrix},
\]  

(4.4)

where \( A_1 \) contains the \( e \) columns corresponding to the indeterminates in \( g \) and \( A_2 \) contains the remaining \( n - e \) columns corresponding to the indeterminates in \( h \). (Possible zero columns of \( A \) are unimportant and may be placed in either \( A_1 \) or \( A_2 \).) Now by the structure of \( f \) described earlier in connection with (2.11) and by (4.3) we know that all possible sets of \( m \) linearly independent columns of \( A \) must be formed from \( r \) columns of \( A_1 \) and from \( m - r \) columns of \( A_2 \). We assert that this observation implies that \( A_1 \) is of rank \( r \). It is clear that \( A_1 \) must have at least \( r \) linearly independent columns because \( f \neq 0 \). But \( A_1 \) cannot have more than \( r \) linearly independent columns because these could be extended to a basis of the column space and this would contradict our previous observation. A similar argument shows that \( A_2 \) is of rank \( m - r \).

We now consider the matrix (4.4), where \( A_1 \) is of rank \( r \) and \( A_2 \) is of rank \( m - r \). Then by elementary row operations we may reduce the matrix to the form

\[
\begin{bmatrix}
B_1 & B_2 \\
0 & B_3
\end{bmatrix},
\]  

(4.5)

where \( B_1 \) is of size \( r \) by \( e \) and of rank \( r \) and \( 0 \) is a zero matrix. The entire matrix is still of rank \( m \) and hence \( B_1 \) is of rank \( m - r \). But the last \( n - e \) columns of the matrix are also of rank \( m - r \). This means that the rows of \( B_2 \) are dependent on the rows of \( B_3 \). Hence we may apply further elementary row operations to the matrix and replace \( B_2 \) by a zero matrix. But then \( Y \) splits under congruence over \( F \) and this is a contradiction. Hence \( \det(Y) \) is irreducible in \( F^* \).

**Corollary 4.2.** Let \( A \) be a matrix of size \( m \) by \( n \) with elements in a field \( F \). Let \( A \) be of rank \( r \) and let \( A \) contain no columns of 0's. Let the \( n \) columns of \( A \) be partitioned into \( t \) components \( A_1, \ldots, A_t \), where component \( A_i \) of \( A \) contains exactly \( r_i \) linearly independent column vectors \( (i = 1, \ldots, t) \). Suppose that

\[
r = \sum_{i=1}^{t} r_i
\]  

(4.6)
and that the integer \( t \) that appears in \( (4.6) \) is maximal. Then it follows that the components \( A_i \) of \( A \) are uniquely determined apart from their order.

**Proof.** We suppose for the moment that the matrix \( A \) is of rank \( m \). We now apply elementary row operations to the matrix \( A \). This leaves fixed the number of linearly independent column vectors in each of the components. Furthermore, we may apply elementary row operations and column permutations to the matrix \( A \) and thereby replace \( A \) by a matrix of the form

\[
B = B_1 \oplus \cdots \oplus B_t.
\]

In (4.7) each \( B_i \) of \( B \) is of size \( r_i \) by \( n_i \) and of rank \( r_i \). Moreover, the columns of \( B \) that pass through \( B_i \) are precisely the columns in the original component \( A_i \) of \( A \) transformed by elementary row operations. This assertion follows by the same argument used in the last part of the proof of Theorem 4.1.

Let \( Z_i \) be the set intersection matrix defined by \( B_i \). Then \( \det(Z_i) \) is a homogeneous polynomial of degree \( r_i \) in \( n_i \) indeterminates. We assert that \( \det(Z_i) \) is irreducible in \( F^* \). This is the case because if \( \det(Z_i) \) factors in \( F^* \) then it follows from Theorem 4.1 that \( Z_i \) splits under congruence over \( F \). This means that the matrix \( B_i \) may be transformed into a direct sum by elementary row operations and column permutations. But then the partition of the columns of \( A \) may be extended to \( t+1 \) components and this contradicts our assumption that \( t \) is maximal.

It now follows that the set intersection matrix \( Y \) defined by \( A \) satisfies

\[
\det(Y) = \det(AXA^T) = f_1 \cdots f_t.
\]

In (4.8) the polynomial \( f_i \) is homogeneous of degree \( r_i \) in \( n_i \) indeterminates. Furthermore, the polynomial \( f_i \) contains precisely those indeterminates that correspond to the various columns of the components \( A_i \) of \( A \). We also know that the polynomial \( f_i \) is irreducible in \( F^* \). Now a second partition of the columns of \( A \) into \( t \) components would induce a second factorization of \( \det(Y) \) into irreducible polynomials in \( F^* \). But \( F^* \) is a unique factorization domain and hence it follows that the components \( A_i \) of \( A \) are uniquely determined apart from their order.

We may deal with the more general situation in which \( A \) is of rank \( r \) by merely applying the preceding argument to any \( r \) linearly independent rows of \( A \).

5. **The Characteristic Polynomial of \( Y \)**

Let \( Y \) be the set intersection matrix of order \( m \) defined by the matrix \( A \) of size \( m \) by \( n \). Let \( f(z) \) denote the characteristic polynomial of \( Y \). Thus \( f(z) \) is
a polynomial of degree \( m \) in the polynomial ring \( F^*[z] \). We study the structure of \( f(z) \).

It follows at once from well known results in matrix theory that the characteristic roots of \( Y = AXA^T \) are the same as the characteristic roots of the matrix

\[
A^TAX, \tag{5.1}
\]

apart from certain zero characteristic roots. The matrix (5.1) is of order \( n \) and hence we may write

\[
f(z) = \det(zI - Y) = z^{m-n} \det(zI - A^TAX). \tag{5.2}
\]

We next investigate the situation in which two set intersection matrices \( Y \) and \( Z \) of order \( m \) have the same characteristic polynomial \( f(z) \).

**Theorem 5.1.** Let \( Y \) and \( Z \) be set intersection matrices of order \( m \) defined by the matrices \( A \) and \( B \), respectively, of size \( m \) by \( n \). Then

\[
f(z) = \det(zI - Y) = \det(zI - Z) \tag{5.3}
\]

if and only if there exists a diagonal matrix \( D \) of order \( n \) with main diagonal elements equal to \( \pm 1 \) such that

\[
A^T A = DB^TBD. \tag{5.4}
\]

Our proof requires a special case of the following lemma. A principal submatrix of a symmetric matrix \( S \) is called *diagonal critical* provided that the submatrix has exactly two nonzero off diagonal elements on each of its lines. Notice that in this definition the main diagonal elements of the submatrix are excluded from consideration.

**Lemma 5.2.** Let \( S \) be a symmetric matrix of order \( n \) with elements in a field \( F \) and let \( T \) be the same matrix as \( S \) apart from the sign of its elements. We further assume that \( T \) is also symmetric and that the main diagonal elements of \( T \) are identical to the corresponding main diagonal elements of \( S \). Now suppose that every diagonal critical principal submatrix of \( S \) has the same determinant as its corresponding diagonal critical principal submatrix in \( T \). Then we may simultaneously multiply certain rows and columns of \( T \) by \(-1\)'s and thereby transform \( T \) into \( S \).

The above lemma is once again a special case of the more general theorem of Engel and Schneider [1].
We are now ready to prove Theorem 5.1. Suppose that (5.4) is valid. Then
\[ \det(zI - A^TAX) = \det(D(zI - DB^TBDX)D) \]
\[ = \det(zI - B^TBX), \]
whence by (5.2) we have that (5.3) is valid.

We next prove the reverse implication. Let
\[ A^TA = S, \quad B^TB = T. \]
(5.6)
Then (5.2) and (5.3) imply
\[ \det(zI - SX) = \det(zI - TX). \]
(5.7)
We now recall the familiar structure of the coefficients of the characteristic polynomial of a matrix in terms of sums of determinants of its principal submatrices. But then by the structure of the matrices SX and TX it follows from (5.7) that every principal submatrix of S has the same determinant as its corresponding principal submatrix in T. Furthermore, it then follows that the matrix T is the same matrix as S apart from the sign of its elements. But then by Lemma 5.2 we may simultaneously multiply certain rows and columns of T by -1's and thereby transform T into S. Thus (5.4) is valid.

6. THE IRREDUCIBILITY OF m(z)

Let \( Y = AXA^T \) be the set intersection matrix of order \( m \) defined by the matrix \( A \) of size \( m \) by \( n \). Let \( f(z) \) denote the characteristic polynomial of \( Y \) of degree \( m \) in the polynomial ring \( F^*[z] \). Throughout the discussion we write
\[ f(z) = z^tm(z), \]
(6.1)
where the integer \( t \) in (6.1) is the maximal power of \( z \) that divides \( f(z) \). We note that we have \( t = 0 \) if and only if \( \det(Y) \neq 0 \) or, equivalently, if and only if \( \text{rank}(A) = m \). We henceforth study the irreducibility of \( m(z) \) in \( F^*[z] \).

We write the characteristic polynomial \( f(z) \) of \( Y \) in the form
\[ f(z) = z^m + a_{m-1}z^{m-1} + \cdots + a_1z + a_0. \]
(6.2)
Each coefficient \( a_i \) (\( i = 0, 1, \ldots, m - 1 \)) of \( f(z) \) is apart from sign the sum of the determinants of all principal submatrices of \( Y \) of order \( m - i \). But these principal submatrices of \( Y \) of order \( m - i \) are themselves set intersection matrices. Thus it follows that each coefficient \( a_i \) (\( i = 0, 1, \ldots, m - 1 \)) such that
$a_i \neq 0$ is a homogeneous form of degree $m - i$ in the $n$ indeterminates $x_1, \ldots, x_n$. Moreover, each term of the homogeneous form $a_i \neq 0$ consists of a nonzero coefficient in $F$ and a product of $m - i$ distinct elements of $x_1, \ldots, x_n$.

We say that the characteristic polynomial $f(z)$ of the set intersection matrix $Y$ covers the matrix $X = \text{diag}[x_1, \ldots, x_n]$ provided that each of the indeterminates $x_1, \ldots, x_n$ is actually present in at least one of the coefficients $a_i$ ($i = 0, 1, \ldots, m - 1$).

The following remark describes the structure of $A$ in case $f(z)$ does not cover $X$.

**Remark 6.1.** Suppose that the indeterminate $x_i$ does not appear in any of the coefficients of the characteristic polynomial $f(z)$ of $Y$. Then column $i$ of $A$ is orthogonal to itself and to each of the other $n - 1$ columns of $A$.

**Proof.** Let the indeterminate $x_i$ not appear in any of the coefficients of $f(z)$ and let $x_j$ be any other indeterminate of $x_1, \ldots, x_n$. Then the principal submatrix of order 2 of $A^TAX$ formed by the intersection of rows $i$ and $j$ and columns $i$ and $j$ is

\[
\begin{bmatrix}
(a_{ii}^2 + \cdots + a_{mi}^2)x_i & (a_{1i}a_{1j} + \cdots + a_{mi}a_{mj})x_j \\
(a_{1i}a_{1j} + \cdots + a_{mi}a_{mj})x_i & (a_{jj}^2 + \cdots + a_{mj}^2)x_j
\end{bmatrix}.
\] (6.3)

But then by (5.2) we must have $a_{ii}^2 + \cdots + a_{mi}^2 = 0$ because otherwise $x_i$ appears in the coefficient $z^{m-1}$ of $f(z)$. Similarly, $a_{i1}a_{ij} + \cdots + a_{mi}a_{mj} = 0$ because otherwise $x_ix_j$ appears in the coefficient $z^{m-2}$ of $f(z)$. Hence column $i$ of $A$ is orthogonal to itself and to every other column of $A$.

We note that if no indeterminate appears in $f(z)$ then $f(z) = z^m$. Thus in this situation it follows that $A^TA = 0$.

We repeat a classical definition. A matrix $A$ of order $n > 1$ with elements in a field $F$ is irreducible over $F$ provided that there does not exist a permutation matrix $P$ of order $n$ such that

\[
PAP^T = \begin{bmatrix}
A_1 & 0 \\
\ast & A_2
\end{bmatrix}.
\] (6.4)

In (6.4) the matrices $A_1$ and $A_2$ are square of orders $r$ and $n - r$, respectively, for some integer $r$ in the interval $1 \leq r \leq n - 1$ and the matrix 0 is the zero matrix of size $r$ by $n - r$. The matrix $A$ of order $n = 1$ is irreducible provided that $A$ is not the zero matrix of order 1. A matrix that is not irreducible is called reducible.

Theorem 6.1 which follows concerns the irreducibility of $m(z)$ in $F^*[z]$. This theorem is actually a special case of a very recent and interesting theorem of de Sá [13]. We include a self-contained proof of Theorem 6.1 for completeness.
THEOREM 6.1. Let \( f(z) = z^m m(z) \) be the characteristic polynomial of the set intersection matrix \( Y = AXA^T \) and suppose that \( f(z) \) covers \( X \). Then \( m(z) \) is irreducible in \( F^*[z] \) if and only if the symmetric matrix \( A^TA \) of order \( n \) is irreducible over \( F \).

We begin with the derivation of two elementary remarks concerning the factors of the characteristic polynomial \( f(z) \) of the set intersection matrix \( Y \). Our arguments parallel the discussion in [12]. We consider a proper factorization of \( f(z) \) in \( F^*[z] \) of the form

\[
f(z) = z'g(z) h(z).
\]  

We assume that

\[
\deg(g(z)) = r, \quad \deg(h(z)) = s = m - r - t,
\]  

where \( r \) and \( s \) are positive integers and we write

\[
g(z) = z^r + b_{r-1}z^{r-1} + \cdots + b_1z + b_0, \quad h(z) = z^s + c_{s-1}z^{s-1} + \cdots + c_1z + c_0.
\]

Remark 6.2. The coefficients \( b_i \) of \( g(z) \) and \( c_j \) of \( h(z) \) do not have any indeterminates in common.

Proof. Suppose that an element \( x_i \) appears in the coefficients of both \( g(z) \) and \( h(z) \). Let \( R \) denote the same polynomial ring as \( F^*[z] \) but with the indeterminate \( x_i \) deleted. Then \( g(z) \) is a polynomial in \( x_i \) with coefficients in \( R \) of degree at least 1 in \( x_i \). The same holds for \( h(z) \). But then \( f(z) \) is a polynomial in \( x_i \) with coefficients in \( R \) of degree at least 2 in \( x_i \). This contradicts the structure of \( f(z) \).

Remark 6.3. Each coefficient \( b_i \) of \( g(z) \) is a sum of terms that appear in the coefficient \( a_{i+s+t} \) of \( f(z) \) (\( i = 0, 1, \ldots, r - 1 \)). A corresponding statement holds for the coefficients \( c_j \) of \( h(z) \).

Proof. We first prove that no coefficient \( b_i \) of \( g(z) \) or \( c_j \) of \( h(z) \) contains a term that is a nonzero element of \( F \). Suppose the contrary. Then we set all \( x_i = 0 \) and (6.5) yields a contradictory factorization of \( z^m \). We next set only those \( x_i = 0 \) that appear in the coefficients of \( h(z) \). Then by Remark 6.2 and the preceding observation it follows that this substitution leaves \( g(z) \) unchanged and replaces \( h(z) \) by \( z^t \). The conclusion now follows from (6.5).

We are now ready to begin the proof of Theorem 6.1. We first deal with the cases \( m = 1 \) and \( n = 1 \). In case \( m = 1 \) then \( A \) is a row vector without zero components. We then have \( f(z) = m(z) \) and both \( m(z) \) and \( A^TA \) are irreducible. In case \( n = 1 \) then \( A \) is a column vector and we let \( A^TA = [a] \).
We then have $m(z) = z - ax_1$, where $a \neq 0$. Thus both $m(z)$ and $A^TA$ are irreducible. We henceforth always take $m > 1$ and $n > 1$.

We now prove that $m(z)$ irreducible in $F^*[z]$ implies that $A^TA$ is irreducible over $F$. Suppose that $A^TA$ is reducible over $F$. Then there exists a permutation matrix $P$ of order $n$ such that

$$P(A^TA)P^T = A_1 \oplus A_2,$$  \hspace{1cm} (6.8)

where $A_1$ is of order $r$ and $A_2$ is of order $n - r$, $1 \leq r \leq n - 1$. It then follows that $P(A^TA)P^T$ also splits into a direct sum, where one component is of order $r$ and the other component is of order $n - r$. But the above congruence transformation applied to $A^TAx$ is also a similarity transformation. Hence by (5.2) we have

$$f(z) = \det(zI - Y) = z^{m-n} \det(zI - P(A^TAx)P^T).$$  \hspace{1cm} (6.9)

But in this equation we know that

$$\det(zI - P(A^TAx)P^T)$$  \hspace{1cm} (6.10)

factors into two polynomials in $F^*[z]$. Since $f(z)$ covers $X$ the coefficients of the one factor must contain $r$ indeterminates and the coefficients of the other factor must contain the remaining $n - r$ indeterminates. This in turn contradicts the hypothesis that $m(z)$ is irreducible in $F^*[z]$.

We next prove that $A^TA$ irreducible over $F$ implies that $m(z)$ is irreducible in $F^*[z]$. Suppose that $m(z)$ factors in $F^*[z]$. We then have

$$f(z) = z^rg(z)h(z),$$  \hspace{1cm} (6.11)

where $g(z)$ and $h(z)$ are of positive degrees $r$ and $s = m - r - t$, respectively. By Remark 6.2 we know that the coefficients $b_i$ of $g(z)$ and $c_j$ of $h(z)$ do not have any indeterminates in common. Let $x_i$ be an indeterminate of $g(z)$ and let $x_j$ be an indeterminate of $h(z)$. We now take into account the special form of the factors $g(z)$ and $h(z)$ described in Remark 6.3 and we set all of the indeterminates $x_1, \ldots, x_n$ equal to 0 except $x_i$ and $x_j$. Upon completion of this substitution the polynomial $f(z)$ simplifies to the following form

$$z^{m-2}(z - a_ix_i)(z - a_jx_j).$$  \hspace{1cm} (6.12)

where $a_i$ and $a_j$ are elements of $F$.

On the other hand suppose that we set all of the indeterminates $x_1, \ldots, x_n$ equal to 0 except $x_i$ and $x_j$ in the expression

$$z^{m-n} \det(zI - A^TAx).$$  \hspace{1cm} (6.13)
Then by (5.2) we must again obtain (6.12). But this substitution into (6.13) yields
\[
z^{m-n}z^{n-2}\left\{ [z - (a_{1i}^2 + \cdots + a_{mi}^2)]z - (a_{1j}^2 + \cdots + a_{mj}^2) \right\} - (a_{1i}a_{1j} + \cdots + a_{mi}a_{mj})^2 \cdot x_i x_j. \tag{6.14}
\]

Hence we must have
\[
(z - a_i x_i)(z - a_j x_j) = [z - (a_{1i}^2 + \cdots + a_{mi}^2)]z - (a_{1j}^2 + \cdots + a_{mj}^2) \cdot x_i \cdot x_j - (a_{1i}a_{1j} + \cdots + a_{mi}a_{mj})^2 \cdot x_i x_j. \tag{6.15}
\]

But then
\[
a_i = a_{1i}^2 + \cdots + a_{mi}^2, \quad a_j = a_{1j}^2 + \cdots + a_{mj}^2, \tag{6.16}
\]
whence
\[
a_{1i}a_{1j} + \cdots + a_{mi}a_{mj} = 0. \tag{6.17}
\]

Thus columns \(i\) and \(j\) of \(A\) are orthogonal.

Let us say that \(g(z)\) contains \(e\) of the indeterminates \(x_1, \ldots, x_n\). Then since \(f(z)\) covers \(X\) it follows that \(h(z)\) contains the remaining \(n - e\) indeterminates. But this implies that there exists a permutation matrix \(Q\) of order \(n\) such that
\[
Q^T A^T A Q = A_1 \oplus A_2, \tag{6.18}
\]

where \(A_1\) is of order \(e\) and \(A_2\) is of order \(n - e\). But this means that \(A^T A\) is reducible over \(F\). Hence it follows that \(m(z)\) is irreducible in \(F^*[z]\).

The following corollary is an immediate consequence of Theorem 6.1.

**Corollary 6.2.** Let \(f(z)\) be the characteristic polynomial of the nonsingular set intersection matrix \(Y = AXA^T\) and suppose that \(A\) contains no column of 0's. Then \(f(z)\) is irreducible in \(F^*[z]\) if and only if the symmetric matrix \(A^T A\) of order \(n\) is irreducible over \(F\).

**References**