1959

A polynomial analysis of digital computer counters

John Anderson

The University of Montana

Follow this and additional works at: http://scholarworks.umt.edu/etd

Recommended Citation

This Thesis is brought to you for free and open access by the Graduate School at ScholarWorks at University of Montana. It has been accepted for inclusion in Theses, Dissertations, Professional Papers by an authorized administrator of ScholarWorks at University of Montana. For more information, please contact scholarworks@mail.lib.umt.edu.
A Polynomial Analysis of Digital Computer Counters

23 pages, by John Anderson

An abstract of a thesis presented
in partial fulfillment of the requirements
for the degree of Master of Science
Montana State University, 1959

Approved

A polynomial representation of a certain type of shift register counter has been effected by F.H. Young and this representation has been shown to be effective in determining properties of this type of counter. In this paper the polynomial representation of shift register counters is further developed. In particular, the cycle length for a shift register counter is defined; the characteristic polynomial of a type of shift register is defined; a complete set of initiating states for cycles relative to a polynomial are defined; a complete set of initiating states for cycles relative to a polynomial are exhibited in terms of the initiating states relative to its relatively prime factors; the number of cycles of each possible length for a shift register counter is determined from the cycle lengths associated with its characteristic polynomial.
A POLYNOMIAL ANALYSIS OF DIGITAL COMPUTER COUNTERS

by

JOHN ANDERSON

B.S. University of Illinois, 1956

Presented in partial fulfillment
of the requirements for the degree of

Master of Science

MONTANA STATE UNIVERSITY

1959

 Approved by:

F. H. Young

Ellis Waldron

AUG 18 1959
PREFACE

The author of this paper is indebted to members of the faculty in the department of mathematics of Montana State University for advice and criticism kindly rendered during the preparation of this paper. The author is especially indebted to Dr. F. H. Young, whose original work led to the present investigation, and who directed the author in preparing this manuscript.
# TABLE OF CONTENTS

I  INTRODUCTION  
   1

II  REPRESENTATIONS  
    6

III SOME THEOREMS CONCERNING COUNTERS  
   12
Abstract

A polynomial representation of a certain type of shift register counter has been effected by F.H. Young (1). This representation has been shown to be effective in determining properties of this type of counter (1)(2). In this paper a polynomial representation of shift register counters is studied. In particular, the cycle length of shift register counters is defined; the characteristic polynomial for a type of shift register counter is defined; some theorems are given which show the relation between the cycle lengths and the factorization of the characteristic polynomial.

Counters

Definition: A state of a register of n elements is an ordered sequence of n symbols, each either 0 or 1.

Theorem 1.1 A register of n elements has $2^n$ states.

Definition: A shift register is a register in which, on each clock pulse, the symbols are shifted one place to the left and discarded on the left end. The input to the first place is unspecified.

Definition: A shift register counter is a shift register in which the input to the first place is a single-valued logical function of the elements of the register, treated as elements of a boolean algebra.

Theorem 1.2 A state of a shift register counter has a unique successor state.
Theorem 1.3  Any sufficiently prolonged sequence of states in a shift register counter must return to a state already in the sequence.

Proof: The number of states is finite.

Definition: A state $S$ which initiates a sequence of states returning to $S$ is a state of a cycle.

Definition: $T$ is said to be in the same cycle as $S$ in case $S$ is a state of a cycle and $S$ initiates a sequence of states leading to $T$.

Definition: The number of distinct states in a cycle is the length of the cycle.

Example: Consider the shift register counter on the elements $A_3A_2A_1$ in which the input to $A_1$ is the function $A_3A_2$ defined by the truth table

<table>
<thead>
<tr>
<th>$A_3$</th>
<th>$A_2$</th>
<th>$A_3A_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

The sequence initiated by the state 101 is

<table>
<thead>
<tr>
<th>$A_3$</th>
<th>$A_2$</th>
<th>$A_3A_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The states 100, 001 and 010 constitute a cycle of length three. The states 101, 011 and 110 are not states of a cycle.

An interesting shift register counter is the one in
which the input function is the symmetric difference of two particular elements, i.e. the function \( N \Delta J = N J + N' J \) where \( N \) and \( J \) are the boolean algebra representations of the \( n^{th} \) and \( j^{th} \) register elements. For this type of counter the state with all elements zero, called the zero state, initiates a cycle of length one, called the zero cycle. It is this type of counter which has been studied previously (1) and to which a major portion of the present paper is devoted.

**Polynomials**

**Definition:** If \( D \) is an integral domain then \( a \) is said to divide \( b \) in \( D \) in case \( a \) and \( b \) are contained in \( D \) and there exists a \( c \) contained in \( D \) such that \( b = ac \) in \( D \).

**Definition:** \( a \) is said to be congruent to \( b \) modulo \( c \), written \( a \equiv b \mod(c) \), relative to an integral domain \( D \), in case \( c \) divides \( a - b \) in \( D \).

**Theorem 1.4** Congruence \( \mod(c) \) is an equivalence relation.

**Theorem 1.5** If \( p \) is a prime integer, then the ring of integers \( I \) with the relation congruence \( \mod(p) \) is a field (denoted \( I/(p) \)).

**Corollary** \( I/(2) \) is a field.

**Theorem 1.6** The ring of polynomials in a transcendental \( x \) over a field \( F \) (denoted \( F[x] \)) is an integral domain.

**Corollary** \( I/(2)[x] \) is an integral domain.

**Theorem 1.7** If \( c(x) \) is contained in \( I/(2)[x] \), then \( c(x) \) is uniquely expressible as a product of irreducible
factors except for the order of the factors and possible repetition of the identity 1.

**Definition:** If \( a(x), b(x) \) and \( c(x) \) are contained in \( \mathbb{F}(2)[x] \), then we write \( a(x) \equiv b(x) \pmod{(2,c(x))} \) in case \( c(x) \) divides \( a(x) - b(x) \) in \( \mathbb{F}(2)[x] \).

**Lemma 1** \( a(x) \equiv 0 \pmod{(2,c(x))} \) if and only if \( c(x) \) divides \( a(x) \) in \( \mathbb{F}(2)[x] \).

**Lemma 2** If \( c(x) \) is irreducible in \( \mathbb{F}(2)[x] \) and if \( a(x)b(x) \equiv 0 \pmod{(2,c(x))} \), then either \( c(x) \) divides \( a(x) \) or \( c(x) \) divides \( b(x) \) in \( \mathbb{F}(2)[x] \).

**Definition:** If \( b(x) \) and \( c(x) \) are contained in \( \mathbb{F}(2)[x] \) and if the degree of \( b(x) \) is less than the degree of \( c(x) \), then \( b(x) \) is said to be a residue \( \pmod{(2,c(x))} \).

**Lemma 3** If \( c(x) \) is contained in \( \mathbb{F}(2)[x] \) and if \( c(x) \) is of degree \( n \), then there are \( 2^n \) distinct residues and \( 2^n - 1 \) distinct non-zero residues \( \pmod{(2,c(x))} \).

**Transformations**

**Definition:** \( S \) is a single-valued transformation in case for every \( a: aS \) is defined implies \( aS \) is unique.

**Lemma 4** A shift register counter is acted on by a single-valued transformation.

**Theorem 1.8** If a single-valued transformation \( S \) has an inverse \( S^{-1} \), then \( S^{-1} \) is a single-valued transformation.

**Definition:** If \( S \) is a single-valued transformation acting on a set \( A \) and if \( a \) is contained in \( A \), then \( a \) is an element of a cycle if \( aS^m = a \) for some \( m \) greater than zero.
**Definition:** If $a$ is an element of a cycle, then the length of the cycle containing $a$ is the smallest integer $m$ for which $aS^m = a$.

**Theorem 1.9** If $S$ is a single-valued transformation acting on a finite set $A$ and $S$ has an inverse, then every element of $A$ is an element of a cycle.

**Proof:** Let $x_0$ be a member of $A$. Then $x_0$ initiates a sequence

$$x_0, x_1, x_2, \ldots, x_k, \ldots$$

Since the number of states is finite we must have $x_i = x_j$ for some $i$ and $j$, with $i$ and $j$ distinct. Let $i$ be less than $j$.

If $i = 0$, then we are done. If $i \neq 0$, then, since $S^{-1}$ is single-valued, $A_i S^{-1} = A_{i-1}$, where $A_{i-1}$ is well defined. Thus, $A_i = A_j$ implies $A_{i-1} = A_{j-1}$ and for every $k$ less than or equal to $i$, $A_{i-k} = A_{j-k}$. Let $k = i$; then $A_0 = A_{j-i}$ for $j-i$ different from $0$.

This shows that the state $x_0$ initiates a sequence returning to $x_0$ so that $x_0$ is a state of a cycle. Since $x_0$ is arbitrary, every state is a state of a cycle. Q.E.D.
II REPRESENTATIONS

Vector Representation

A state of a register of n elements may be represented by a vector \( \{a_i\} = (a_n \ a_{n-1} \ldots \ a_2 \ a_1) \) where each \( a_i \) is either 0 or 1. The accompanying addition tables show that the symmetric difference of the \( n^{th} \) and the \( j^{th} \) elements is \( a_n + a_j \) where the addition is carried out \( \mod(2) \).

Relative to the logical function \( N \Delta J \) let \( S \) be a mapping which sends the vector \( \{a_i\} \) into the vector of the next state. Then

\[
\{a_i\}S = (a_{n-1} \ a_{n-2} \ldots \ a_1 \ a_n + a_j)
\]

The transformation \( S \) can be represented by the \( nxn \) matrix:

\[
\begin{bmatrix}
0 & 0 & 0 & \ldots & 0 & 1 \\
1 & 0 & 0 & \ldots & 0 & 0 \\
0 & 1 & 0 & \ldots & 0 & 0 \\
0 & 0 & \ldots & 0 & 0 & 0 \\
0 & 0 & \ldots & 0 & 0 & 1 \\
0 & 0 & \ldots & 1 & 0 & 0
\end{bmatrix}
\]
The matrix $S$ has 0's everywhere except on the diagonal below the main diagonal and the $n$th and $j$th rows of the $n$th column. The shift is effected by multiplying the vector by the matrix with the matrix on the right and the addition carried out mod(2). The register is characterized by its corresponding matrix. The determinant of the matrix $S$ is 1; therefore, $S$ is nonsingular and $S^{-1}$ exists. Since the transformation represented by $S$ is single-valued, theorem 1.9 applies. Thus, for the register with the logical function $\mathbf{N} \Delta \mathbf{J}$, every state is a state of a cycle.

If $m$ is the length of the cycle containing the vector $a$, then $aS^m = al$ where $I$ is the identity matrix. Thus $m$ is the smallest integer such that $\lambda^m = 1$ where $\lambda$ is a root of the polynomial $|S - \lambda I|$, i.e. a solution of the characteristic equation of the matrix $S$. Expanding the determinant $|S - \lambda I|$ by elements of the last column we obtain

\[
\begin{vmatrix}
1 & \lambda & 0 \\
0 & 1 & \lambda \\
0 & 0 & 1
\end{vmatrix} + \begin{vmatrix}
\lambda & 0 & 1 \\
1 & \lambda & 0 \\
0 & 1 & \lambda
\end{vmatrix} + \lambda \begin{vmatrix}
\lambda & 0 & 1 \\
0 & \lambda & 0 \\
0 & 1 & \lambda
\end{vmatrix}
\]

The first determinant has ones on the main diagonal and zeros everywhere below the main diagonal; therefore it is 1.
The third determinant has $\lambda$'s on the main diagonal and zeros everywhere above; thus it is $\lambda^{n-1}$. The second can be written as the product of two determinants one of which is $\lambda^{n-j}$, the other 1. Thus

$$|S - \lambda I| = 1 + \lambda^{n-j} + \lambda^n,$$

and this is the characteristic polynomial for this register.

**Polynomial Representation**

Consider a polynomial $a(x)$ in $\mathbb{F}_2[x]$. Multiply $a(x)$ by $x$ and reduce modd($2, x^n + x^{n-j} + 1$). If

$$a(x) = a_n x^{n-1} + a_{n-1} x^{n-2} + \cdots + a_2 x + a_1$$

then $xa(x) = a_n x^{n-1} + \cdots + a_{n-j} x^{n-j} + \cdots + a_1 x + a_n$

modd($2, x^n + x^{n-j} + 1$).

rearrange the order of the terms to obtain

$$xa(x) = a_{n-j} x^{n-j-1} + \cdots + a_n + \cdots + (a_{n-j} + a_n) x^{n-j}.$$ 

Associate the coefficients of this last form with the elements of a register. The effect of the operation is to shift the coefficients one place to the left and write the sum modd($2$) of the $n$th and the $n-(n-j) = j$th into the first place. Note that the constant term of the polynomial is associated with the $j$th position of the register.

This shows that multiplication of $a(x)$ by $x$ and reduction modd($2, x^n + x^{n-j} + 1$) corresponds to the operation of the shift register counter with the input function $\text{NAJ}$. Thus, for this register, if $m$ is the smallest integer such that $x^m \equiv 1$ modd($2, x^n + x^{n-j} + 1$), i.e., such that $x^n + x^{n-j} + 1$ divides $x^m + 1$ in $\mathbb{F}_2[x]$, then $m$ is the length of the
cycle containing the state $(0 \cdots 010 \cdots 0)$ and the residues of $x^k \mod (2, x^n + x^n - j + 1)$ for $k = 0, 1, \ldots, m$ correspond to the states of the cycle.

**Example:** Consider the residues of $x^k \mod (2, x^2 + x + 1)$. These are given by

$$
\begin{align*}
1 &\rightarrow 1 \\
2 &\rightarrow x \\
x_3 &\rightarrow x + 1 \\
x &\rightarrow 1
\end{align*}
$$

The trinomial $x^2 + x + 1$ corresponds to the register on two elements with the input function $(2) \Delta (1)$. Writing the coefficients of the polynomials as register states with the constant term in the $j+1$st $2^{nd}$ position we obtain the cycle of length three

$$
\begin{array}{ccc}
1 & - & 1 \\
x_2 & - & 0 \\
x_3 & - & 1 \\
x & - & 1
\end{array}
$$

**Generalization**

Consider the shift register counter in which the input to the first place is given by the function

$$
\Delta_{j=1}^k J_j = J_1 \Delta J_2 \Delta \cdots \Delta J_k.
$$

This function will be called a generalized symmetric difference and is to be evaluated by inserting sufficient parentheses and using the relation $F_1 \Delta F_2 = F_1 F_2' + F_1' F_2$ where $F_1$ and $F_2$ are any two logical functions. For example

$$
\begin{align*}
J_1 \Delta J_2 \Delta J_3 &= (J_1 \Delta J_2) \Delta J_3 = (J_1 J_2' + J_1' J_2) \Delta J_3 \\
&= (J_1 J_2' + J_1' J_2) J_3 + (J_1 J_2' + J_1' J_2)' J_3 \\
&= J_1 J_2' J_3 + J_1' J_2 J_3 + J_1 J_2 J_3 + J_1 J_2 J_3
\end{align*}
$$
By the symmetry of the result any alternative grouping will give the same value. In general the function $\Delta_j^{k-1} J_j$ is well defined since it is the sum of all minterms on $k$ elements which contain an odd or even number of primes as $k$ is even or odd.

This generalized symmetric difference is 1 or 0 as the sum $a_{i_1} + a_{i_2} + \cdots + a_{i_k}$ is 1 or 0 mod(2) where $J_j$ is the boolean algebra representation of the vector element $a_{i_j}$. For this register the zero state gives rise to a cycle of length one.

The shift of this register can be represented by a matrix $S_1$ where

$$
S_1 = \begin{bmatrix}
0 & 0 & 0 & c_n \\
1 & 0 & \cdots & 0 & c_{n-1} \\
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & \cdots \\
\end{bmatrix}
$$

and $c_1 = 1$ if $a_1$ is included in the sum and 0 otherwise. The determinant of $S_1$ is $c_n$ thus $S_1$ is non-singular if and only if $c_n \neq 0$; i.e. $c_n = 1$.

The characteristic polynomial of $S_1$ is

$$
c(x) = x^n + c_1 x^{n-1} + \cdots + c_{n-1} x + c_n.
$$

Consider multiplying a polynomial $a(x)$ by $x$ and reducing modd$(2,c(x))$. The result is

$$(a_{n-1} + c_1 a_n)x^{n-1} + (a_{n-2} + c_2 a_n)x^{n-2} + \cdots + (a_1 + c_{n-1} a_n)x + c_n a_n.$$
This operation corresponds to the shift whose matrix is $S_2$ where

$$S_2 = \begin{bmatrix} c_1 & c_2 & \cdots & c_n - 1 & c_n \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The characteristic polynomial of $S_2$ is also $c(x)$.

This shows that we can be aided in studying the shift register counter whose input function is a generalized symmetric difference by looking at finite polynomial rings modd($2, c(x)$). Since the transformation represented by $S_2$ is single-valued, theorem 1.9 applies. Thus, if $c_n = 1$ so that $S^{-1}$ exists, then every polynomial is an element of a cycle; i.e., if $p(x)$ is a residue modd($2, c(x)$) and $c_n = 1$, then there exists an $m$ such that $x^m p(x) \equiv p(x) \text{ modd}(2, c(x))$.

**Definition:** If $S$ is a logic acting in a shift register counter and $S$ can be represented by a matrix, then the characteristic polynomial of the matrix is called the characteristic polynomial of the shift register counter.

**Example:** Consider the four element counter in which the symmetric difference of all four elements is the input to the first place. The characteristic polynomial is $x^4 + x^3 + x^2 + x + 1$ which divides $x^m + 1$ for $m = 5$ and for no smaller integer. Thus the cycle lengths for this register divide 5. In particular the cycle containing the polynomial 1 is of length 5.
III SOME THEOREMS CONCERNING COUNTERS

Determination of the cycle lengths in terms of the factors of the characteristic polynomial

Theorem 3.1 If \( c(x) \) is irreducible in \( \mathbb{Z}/(2)[x] \) and the constant term of \( c(x) \) is 1, then all non-zero cycles have the same length \( m \) and \( m \) divides \( 2^n - 1 \).

Proof: Suppose \( c(x) \) is irreducible in \( \mathbb{Z}/(2)[x] \) and \( m \) is the smallest integer such that \( c(x) \) divides \( x^m + 1 \).

Construct the set of residues
\[
P_1 = \{ x^k \mod (2, c(x)) \mid k = 0, 1, \ldots, m - 1 \}
\]
These constitute \( m \) distinct residues for if not, then
\[
x^k \equiv x^s \mod (2, c(x))
\]
for \( k \) different from \( s \) and both \( k \) and \( s \) less than \( m \). We may assume \( k \) less than \( s \). Then
\[
x^k(x^s - k + 1) \equiv 0 \mod (2, c(x))
\]
for \( 0 < s - k = q < m \). Thus by lemma 2, \( c(x) \) divides \( x^q + 1 \) for \( q \) less than \( m \), contrary to assumption.

If \( P_1 \) does not contain all \( 2^n - 1 \) non-zero residues then choose a non-zero residue \( p(x) \) not contained in \( P_1 \).

Construct the set of residues \( P_2 \) where
\[
P_2 = \{ x^kp(x) \mod (2, c(x)) \mid k = 0, 1, \ldots, m - 1 \}
\]
\( P_2 \) consists of \( m \) distinct residues since if
\[
x^kp(x) \equiv x^sp(x) \mod (2, c(x))
\]
we may suppose \( k \) is less than \( s \). Then
\[
x^k(x^s - k + 1)p(x) \equiv 0 \mod (2, c(x))
\]
By lemma 2 \( c(x) \) divides either \( x^k \) or \( x^s - k + 1 \) or \( p(x) \).
But \(c(x)\) does not divide \(x^k\); nor \(x^{s-k} + 1\) since \(s-k\) is less than \(m\); nor \(p(x)\) since \(p(x)\) is a non-zero residue \(\text{modd}(2, c(x))\). This contradiction shows that the \(m\) residues contained in \(P_2\) are all distinct. Since \((x^m + 1)p(x) = 0\) implies \(x^mp(x) \equiv p(x) \text{modd}(2, c(x))\), \(m\) is the smallest integer such that \(x^mp(x) \equiv p(x) \text{modd}(2, c(x))\).

Continuing until all non-zero states are exhausted we obtain a collection of sets \(P_1, P_2, \ldots, P_s\) with each \(P_i\) containing \(m\) elements. Thus \(m_5 = 2^n - 1\). Q.E.D.

**Example:** The polynomial \(x^6 + x^3 + 1\) is irreducible in \(\mathbb{Z}/(2)[x]\) and divides \(x^m + 1\) for \(m = 9\) and for no smaller integer. Since \(2^6 - 1 = 7 \times 9\) the corresponding register has 7 cycles of length 9.

Similarly, the shift register on four elements with the symmetric difference of all four elements written into the first place has the irreducible characteristic polynomial \(x^4 + x^3 + x^2 + x + 1\) which divides \(x^5 + 1\). Since \(2^4 - 1 = 15 = 3 \times 5\) this register has three cycles of length 5.

If \(f(x)\) is a polynomial, sets can be constructed with \(f(x)\) as a modulus in a manner similar to that used in the proof of theorem 3.1.

Let \(f(x)\) be a polynomial of degree \(n\) with constant term 1. Then there are \(2^n - 1\) non-zero residues \(\text{modd}(2, f(x))\). Construct the set of distinct residues

\[R_0 = \{x^k \text{modd}(2, f(x)) \mid k = 0, 1, \ldots, m_0 - 1\}\]

where \(m_0\) is chosen as the smallest integer such that \(x^{m_0} \equiv 1\).
If $m_0$ does not equal $2^n-1$, then choose a residue $p_1(x)$ not contained in $R_0$ and construct the set of distinct residues

$$R_1 = \{x^kp_1(x) \modd(2,f(x)) \mid k = 0, 1, \ldots, m_1 - 1\}$$

where $m_1$ is the smallest integer such that $x^{m_1}p_1(x) \equiv p_1(x) \modd(2,f(x))$.

If $m_0 + m_1$ does not equal $2^n-1$ then choose a residue $p_2(x)$ not contained in $R_0$ or $R_1$ and construct a set $R_2$. Continue in this fashion to obtain a collection of polynomials $P = \{p_i(x)\}$ for $i = 0, 1, \ldots, s$ with $p_0(x) = 1$ and $x^kp_1(x)$ not congruent to $p_j(x)$ for any $k$ unless $i = j$, along with a collection of integers $m_i$ for which

$$m_0 + m_1 + \cdots + m_s = 2^n - 1$$

and

$$x^{m_i}p_i(x) \equiv p_i(x) \modd(2,f(x))$$

but

$$x^kp_1(x) \not\equiv p_1(x) \modd(2,f(x))$$

for $k$ less than $m_1$.

**Definition:** If $P$ is constructed as above then $P$ is called a complete set of initiating states for cycles $\modd(2,f(x))$.

**Definition:** If $p_1(x)$ is contained in $P$ and $m_1$ is defined as above then $m_1$ is called the cycle length associated with $p_1(x) \modd(2,f(x))$.

**Theorem 3.2** Let $F(x) = f_1(x)f_2(x)$, where $f_1(x)$ and $f_2(x)$ are relatively prime, each have constant term 1 and are of degree $n_1$ and $n_2$ respectively. Let $P_1 = \{p_{1i}(x)\}$
and $p_2 = \{ p_{2j}(x) \}$ be complete sets of initiating states for cycles of length $m_{1i} \mod (2, f_1(x))$ and $m_{2j} \mod (2, f_2(x))$ respectively. Then the polynomials $p_{1i}(x)f_2(x)$ and $p_{2j}(x)f_1(x)$ are initiating states for distinct cycles of length $m_{1i}$ and $m_{2j}$ respectively $\mod (2, f(x))$.

**Proof:** First, the cycles are distinct; for if
\[
x^kp_{1i}(x)f_2(x) \equiv x^sp_{2j}(x)f_1(x) \mod (2, f(x))
\]
then multiply by $f_2(x)$ and transpose to obtain
\[
0 \equiv x^kp_{1i}(x)(f_2(x))^2 + x^sp_{2j}(x)f_1(x)f_2(x)
\]
\[
\quad \equiv x^kp_{1i}(x)(f_2(x))^2 \mod (2, f(x)).
\]
Then, for some $\zeta(x)$
\[
x^kp_{1i}(x)(f_2(x))^2 = \zeta(x)f_1(x)f_2(x) \text{ in } I/(2)[x].
\]
Thus
\[
x^kp_{1i}(x)f_2(x) = \zeta(x)f_1(x) \text{ in } I/(2)[x].
\]
But $x^kp_{1i}(x)$ is a non-zero residue $\mod (2, f_1(x))$ so that $f_1(x)$ does not divide $x^kp_{1i}(x)$; therefore, this last requires that $f_1(x)$ and $f_2(x)$ are not relatively prime, contrary to assumption. This contradiction shows that these two polynomials cannot be congruent $\mod (2, f(x))$ for any choice of $i$ and $j$.

Now, if
\[
x^kp_{1i}(x)f_2(x) \equiv x^sp_{2j}(x)f_2(x) \mod (2, f(x))
\]
then transpose to obtain
\[
(x^kp_{1i}(x) + x^sp_{2j}(x))f_2(x) \equiv 0 \mod (2, f(x)).
\]
This requires that
\[
x^kp_{1i}(x) + x^sp_{2j}(x) \equiv 0 \mod (2, f_1(x)).
\]
Suppose \( s \) is greater than \( k \); then

\[
p_{11}(x) \equiv x^{s-k} \cdot p_{1j}(x) \mod (2, f_1(x)).
\]

From the way in which the \( p_{11}(x) \) were chosen, this requires that \( i = j \) and that \( s - k \) is a multiple of \( m_{1i} \). The smallest value of \( s - k \) for which the congruence can hold is \( m_{1i} \); thus \( m_{1i} \) is the smallest value of \( m \) for which

\[
p_{11}(x)f_2(x) \equiv x^m p_{11}(x)f_2(x) \mod (2, F(x)).
\]

This shows that the polynomial \( p_{11}(x)f_2(x) \) initiates a cycle of length \( m_{1i} \mod (2, F(x)) \) distinct from cycles initiated by the polynomials \( p_{1j}(x)f_2(x) \) for \( j \) different from \( i \) and from the cycles initiated by the polynomials \( p_{2j}(x)f_1(x) \mod (2, F(x)) \). In the same manner, one can show that the polynomial \( p_{2j}(x)f_1(x) \) initiates a cycle of length \( m_{2j} \mod (2, F(x)) \) distinct from the cycles initiated by the polynomial \( p_{2i}(x)f_1(x) \) for \( i \) different from \( j \). \( \text{Q.E.D.} \)

**Example:** Consider the polynomial

\[
x^9 + x^3 + 1 = (x^3 + x^2 + 1)(x^6 + x^5 + x^4 + x^2 + 1)
\]

\( x^3 + x^2 + 1 \) is irreducible in \( \mathbb{F}_2[x] \) and divides \( x^m + 1 \) for \( m = 7 \) and for no smaller integer. \( x^6 + x^5 + x^4 + x^2 + 1 \) is irreducible in \( \mathbb{F}_2[x] \) and divides \( x^m + 1 \) for \( m = 21 \) and for no smaller integer. By theorem 3.1 there are three cycles of length 21 associated with the 6\(^{th} \) degree polynomial. If \( p_i(x) \) for \( i = 1, 2, 3 \) is a complete set of initiating states for cycles \( \mod (2, x^6 + x^5 + x^4 + x^2 + 1) \) then \( p_i(x)(x^3 + x^2 + 1) \) for \( i = 1, 2, 3 \) is a set of initiating states for three cycles of length 21 \( \mod (2, x^9 + x^3 + 1) \) and these are distinct from
each other and from the cycle of length 7 initiated by the polynomial \(x^6 + x^5 + x^4 + x^2 + 1\).

**Theorem 3.3** Let \(f_1(x)f_2(x) = i(x)\); let \([p_{1i}(x)]\) and \([p_{2j}(x)]\) be complete sets of initiating states for cycles of length \(m_{1i}\) and \(m_{2j}\) modd \((2,f_1(x))\) and modd \((2,f_2(x))\) respectively; let \([m_{1i}, m_{2j}]\) be the least common multiple of \(m_{1i}\) and \(m_{2j}\) and let \((m_{1i}, m_{2j})\) be their greatest common divisor, so that \(m_{1i}m_{2j} = [m_{1i}, m_{2j}] (m_{1i}, m_{2j})\); then, for each \(i\) and \(j\), and for
\[
r = 0, 1, \ldots, (m_{1i}, m_{2j}) - 1
\]
the residues of the form
\[
x^r p_{1i}(x)f_2(x) + p_{2j}(x)f_1(x) \modd (2,F(x))
\]
are initiating states for distinct cycles of length \([m_{1i}, m_{2j}]\).

**Proof:** Suppose
\[
(1) \ x^r p_{1i}(x)f_2(x) + x^s p_{2j}(x)f_1(x) \equiv x^t p_{1k}(x)f_2(x) + x^u p_{2h}(x)f_1(x) \modd (2,F(x)).
\]
Then, transposing,
\[
(2) \ (x^r p_{1i}(x) + x^t p_{1k}(x))f_2(x) \equiv (x^s p_{2j}(x) + x^u p_{2h}(x))f_1(x).
\]
Multiply both sides of (2) by \(f_2(x)\). Then
\[
(x^r p_{1i}(x) + x^t p_{1k}(x))(f_2(x))^2 \equiv 0 \modd (2,F(x)).
\]
Since \(f_1(x)\) and \(f_2(x)\) are relatively prime
\[
x^r p_{1i}(x) + x^t p_{1k}(x) \equiv 0 \modd (2,f_1(x)).
\]
Suppose \(r\) is greater than \(t\). Then
\[
x^r - t p_{1i}(x) \equiv p_{1k}(x) \modd (2,f_1(x)).
\]
From the way in which the \(p_{1i}(x)\) were chosen, this requires that \(p_{1i}(x) = p_{1k}(x)\), i.e. that \(i = k\); and that \(r - t\) is a
multiple of \( m_{1i} \), the cycle length associated with \( p_{1i}(x) \modd (2, f_1(x)) \).

Multiplying (2) by \( f_1(x) \) instead of \( f_2(x) \) we obtain that (1) requires \( p_{2j}(x) = p_{2n}(x) \) and assuming that \( s \) is greater than \( u \), \( s - u \) is a multiple of \( m_{2j} \). Thus for fixed \( i \) and \( j \) the residues of the polynomials

\[ x^{r} p_{1i}(x)f_2(x) + x^{s} p_{2j}(x)f_1(x) \]

for \( r = 0, 1, \cdots, m_{1i} - 1 \)

and \( s = 0, 1, \cdots, m_{2j} - 1 \)

are \( m_{1i} m_{2j} \) distinct residues \( \modd (2, F(x)) \); and these are distinct from all similar forms for each different pair of \( i \) and \( j \).

To determine the cycle length associated with the polynomial \( x^{r} p_{1i}(x)f_2(x) + p_{2j}(x)f_1(x) \) suppose

(3) \[ x^{s} (x^{r} p_{1i}(x)f_2(x) + p_{2j}(x)f_1(x)) \equiv x^{r} p_{1i}(x)f_2(x) + p_{2j}(x)f_1(x) \modd (2, F(x)). \]

Then transposing,

\[ x^{r} (x^{s} p_{1i}(x) + p_{1i}(x)) f_2(x) \equiv (x^{s} p_{2j}(x) + p_{2j}(x)) f_1(x). \]

Proceeding as above, we obtain that

\[ x^{s} p_{1i}(x) \equiv p_{1i}(x) \modd (2, f_1(x)) \]

so that \( s \) is a multiple of \( m_{1i} \), and

\[ x^{s} p_{2j}(x) \equiv p_{2j}(x) \modd (2, f_2(x)) \]

so that \( s \) is a multiple of \( m_{2j} \). Thus the smallest \( s \) for which the two sides of (3) are congruent is \( \lcm(m_{1i}, m_{2j}) \).

**Theorem 3.4** The cycles guaranteed by theorem 3.3 are distinct from those guaranteed by theorem 3.2.
\textbf{Proof:} If 
\[ x^{r_{p_{11}(x)f_2(x)} + x^{t_{p_{2j}(x)f_1(x)}} = x^{s_{p_{1k}(x)f_2(x)}} \mod (2, F(x)) \]
then 
\[ (x^{r_{p_{11}(x)}} + x^{s_{p_{1k}(x)}}) f_2(x) = x^{t_{p_{2j}(x)}} f_1(x) \mod (2, F(x)). \]
thus 
\[ 0 = x^{t_{p_{2j}(x)}} (f_1(x))^2 \mod (2, F(x)) \]
so that 
\[ x^{t_{p_{2j}(x)}} f_1(x) = q(x) f_2(x) \]
in \( I/(2)[x] \).

But this is a contradiction and since a similar result holds for the polynomial \( x^{s_{p_{2k}(x)}} f_1(x) \) this verifies the statement.

\textbf{Theorem 3.5} Theorems 3.2, 3.3 and 3.4 give a complete accounting for the cycles of a polynomial with constant term 1 in terms of the cycles associated with its relatively prime factors; i.e., the initiating states exhibited in theorems 3.2 and 3.3 are a complete set of initiating states for a polynomial with relatively prime factors and constant term 1.

\textbf{Proof:} Suppose \( F(x) = f_1(x) f_2(x) \) where \( f_1(x) \) and \( f_2(x) \) are relatively prime, have constant term 1 and are of degree \( n_1 \) and \( n_2 \) respectively. Let \( \{m_{1i}\} \) and \( \{m_{2j}\} \) be a complete set of cycle lengths for non-zero cycles relative to \( f_1(x) \) and \( f_2(x) \) respectively. Then
\[ \sum_{1}^{m_{1i}} = 2^{n_1-1} \quad \text{and} \quad \sum_{j}^{m_{2j}} = 2^{n_2-1} \]
and
\[ 2^{n_1+n_2-1} = (2^{n_1-1})(2^{n_2-1}) + (2^{n_1-1}) + (2^{n_2-1}) \]
\[ = (\sum_{i}^{m_{1i}})(\sum_{j}^{m_{2j}}) + (\sum_{i}^{m_{1i}}) + (\sum_{j}^{m_{2j}}) \]
Theorem 3.2 exhibits initiating states for cycles which account for \( \sum_i m_{1i} \) and \( \sum_j m_{2j} \) states. Theorem 3.3 exhibits initiating states which give for each \( i \) and \( j \), \( (m_{1i},m_{2j}) \) cycles of length \( [m_{1i},m_{2j}] \) which accounts for all products \( m_{1i}m_{2j} \). Theorem 3.3 also shows that all of these cycles are distinct. Theorem 3.4 shows that these latter cycles are distinct from the former.

If \( f_1(x) \) and \( f_2(x) \) are further reducible the theorems may be applied to \( f_1(x) \) and \( f_2(x) \). Q.E.D.

Example: Consider the polynomial
\[ x^9 + x^3 + 1 = (x^3 + x^2 + 1)(x^6 + x^5 + x^4 + x^2 + 1) \]
with cycles of length seven and twenty-one. The least common multiple of 7 and 21 is 21 and their greatest common divisor is 7. \( \{ p_{11} \} = \{ 1 \} \) is a complete set of initiating states for the cycle of length seven modd \((2,x^3 + x^2 + 1)\). Let \( \{ p_{21}, p_{22}, p_{23} \} \) be a complete set of initiating states for the cycles of length twenty-one modd \((2,x^6 + x^5 + x^4 + x^2 + 1)\). Then the residue \( x^6 + x^5 + x^4 + x^2 + 1 \) is an initiating state for a cycle of length seven modd \((2,x^9 + x^3 + 1)\). The residues \( p_{21}(x^3 + x^2 + 1) \) for \( i = 1,2,3 \) are initiating states for cycles of length 21. The residues \( x^k(x^6 + x^5 + x^4 + x^2 + 1) + p_{21}(x^3 + x^2 + 1) \) for \( i = 1,2,3 \) and \( k = 0,1,\cdots,6 \) are initiating states for \( 3 \cdot 7 = 21 \) distinct cycles of length 21 and these are distinct from the previous three. Since
\[ 2^9 - 1 = (2^6 - 1)(2^3 - 1) + (2^6 - 1) + (2^3 - 1) = 21 \cdot 3 \cdot 7 + 3 \cdot 21 + 7 \]
this accounts for all cycles for this register.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Conclusion

The study of shift register counters was originally undertaken with a practical motive, the design of digital computer counters. It was found in the course of the study that the shift register counter is particularly amenable to mathematical analysis. Concomitant to this discovery was a shift of the emphasis of the study to the fundamental mathematical questions which arose in regard to the analysis. In particular, we have been led to the study of the order of a certain cyclic operation in a finite polynomial ring.

In this paper, it is shown that certain shift register counters can be associated with a "characteristic polynomial" and that the cycle lengths for the register are the same as the order of the cyclic operation, multiplication of a polynomial by $x$ and reduction with respect to the characteristic polynomial as a modulus. It is further shown that the set of cycle lengths for a register can be composed from the cycle lengths associated with the relatively prime factors of the characteristic polynomial. This leaves unanswered questions related to the cycle lengths when the characteristic polynomial has repeated factors.

Other mathematical questions, as yet unanswered, given rise to by the study of shift register counters, are: (1) the explicit determination of the cycle lengths associated with an irreducible polynomial; (2) a practicable irreducibility criterion for polynomials contained in $\mathbb{F}_2[x]$; (3) determi-
nation of all counters for which a polynomial analysis is useful; i.e., if we multiply a polynomial \( a(x) \) by a polynomial \( b(x) \) and reduce \( \text{mod}(2,c(x)) \), the coefficients of the resulting polynomial are linear combinations of the coefficients of the original polynomial \( a(x) \). The transformation can be represented by a matrix and therefore, the logic for a corresponding register can be written. Given a register representable by a matrix, the modulus \( c(x) \) which goes with \( b(x) = x \) can be determined; but, a suitable criterion for ascertaining all pairs, \( b(x) \) and \( c(x) \) which have corresponding cyclic properties, is yet to be discovered.

These comments show that extensive work remains to be done in applying polynomial analysis to digital computer counters. Because of the essentially mathematical nature of the questions which have arisen in studying counters it is believed that further development, along the lines indicated in this paper, should be undertaken.
Bibliography

(1) Young, F.H., "Analysis of Shift Register Counters", Journal of the Association for Computing Machinery, October 1958; vol. 5, no. 4.