On the Linear Span of Binary Sequences
Obtained from Finite Geometries

AGNES HUI CHAN, RICHARD A. GAMES

The MITRE Corporation
Bedford, Massachusetts 01730

ABSTRACT

A class of periodic binary sequences that are obtained from the incidence vectors of hyperplanes in finite geometries is defined, and a general method to determine their linear spans (the length of the shortest linear recursion over GF(2) satisfied by the sequence) is described. In particular, we show that the projective and affine hyperplane sequences of odd order both have full linear span. Another application involves the parity sequence of order n, which has period $p^n - 1$ and linear span $vL(s)$ where $v = (p^n - 1)/(p - 1)$ and $L(s)$ is the linear span of a parity sequence of order 1. The determination of the linear span of the parity sequence of order 1 leads to an interesting open problem involving primes.

1. INTRODUCTION.

Binary sequences which satisfy recursions over $GF(2)$ are easy to generate and have many applications in modern communication systems. If the recursions involved are linear, then the sequences can have several desirable properties, e.g., long periods, useful correlation properties, and balanced statistics. Binary sequences of maximum period $2^n - 1$ that are generated by linear recursions over $GF(2)$ of degree n are called binary *m-sequences* of span n [**1**].

These linear recursive sequences suffer from one drawback: only relatively few terms of the sequence are needed to solve for the generating recursion; i.e., their *linear span* (the length of the shortest linear recursion over $GF(2)$ satisfied by the sequence) is short relative to their period. Such easy predictability makes binary m-sequences unsuitable for some applications requiring pseudorandom bits.

This work was supported by the MITRE-Sponsored Research Program. A. H. Chan is also with the College of Computer Science, Northeastern University, Boston MA 02115

A.M. Odlyzko (Ed.): Advances in Cryptology - CRYPTO '86, LNCS 263, pp. 405-417, 1987.

In this paper, we consider a class of periodic binary sequences that are obtained from the incidence vectors of hyperplanes in finite geometries. From another point of view, these sequences can be obtained from q-ary m-sequences of span n through a mapping ρ from $GF(q)$ to $GF(2)$, where q is a power of an odd prime. We show that the linear span of these sequences is comparable to their large periods. In fact, the linear span of such a sequence S of period $q^n - 1$ is given by $vL(s)$ where $v = (q^n - 1)/(q - 1)$ and $L(s)$ denotes the linear span of a sequence s of period $q - 1$. The binary sequence s is obtained by applying the defining mapping ρ of S to a listing of the nonzero elements of $GF(q)$ according to the powers of some primitive element. If q is of moderate size, then the linear span of s is easily computed by the Berlekamp-Massey algorithm [2].

The next section introduces the notions involving the linear span of a sequence. Section 3 describes the construction of the binary sequences obtained from finite geometries. Section 4 establishes the upper bound of the linear span of these sequences, while section 5 shows that this bound is always attained. Finally, section 6 gives four examples of sequences obtained from finite geometries and their associated linear spans. These include the hyperplane sequences for both projective and affine spaces. One of these sequences, called the parity sequence, gives rise to an interesting open problem involving primes.

2. THE LINEAR SPAN OF A SEQUENCE.

This paper considers binary sequences and linear recursions over $GF(2)$. All operations used are those of $GF(2)$ unless otherwise stated. Let E denote the sequence shift operator: Es is the sequence with i^{th} term $(Es)_i = s_{i+1}$. A sequence $s = (s_0, s_1, ..., s_i, ...)$ satisfies a linear recursion of degree m if, for $a_j \in GF(2)$,

$$s_{i+m} + \sum_{j=1}^{m} a_j s_{i+m-j} = 0, \quad i \geq 0.$$

This recursion can be expressed in terms of the shift operator,

$$(E^m + \sum_{j=1}^{m} a_j E^{m-j})s = 0.$$

The polynomial $f(E) = E^m + \sum_{j=1}^{m} a_j E^{m-j}$ is called the *characteristic polynomial* of the recursion. If $m(E)$ denotes the unique monic polynomial of least degree such that $m(E)s = 0$, then the *linear span* of s, denoted by $L(s)$, equals the degree of $m(E)$; $m(E)$ is called the *minimal polynomial* of s. If $f(E)s = 0$, then from the division algorithm, $m(E)|f(E)$. In particular, if s has period N, then $(E^N + 1)s = 0$, so that $m(E)|E^N + 1$, and $L(s) \leq N$.

The linear span of a sequence is one measure of its predictability. Any "good" pseudorandom sequence must have large linear span relative to its period [3], [4]. If a sequence has linear span L, then its linear recursion can be determined from $2L$ successive elements of the sequence. The remaining elements then can be produced from the recursion. .

3. SEQUENCES FROM FINITE GEOMETRIES.

In this section, we give the construction of a class of periodic binary sequences that are obtained from finite geometries. Let $q = p^r$, where p is an odd prime, and α be a primitive element of $GF(q^n)$. The nonzero elements of $GF(q^n)$ can be ordered using the primitive element $\alpha : \{\alpha^i : i = 0, 1, ..., q^n - 2\} = GF(q^n)^*$. Elements of $GF(q^n)$ can also be considered as points of an n-dimensional affine space, denoted by $EG(n,q)$. We shall first establish the geometric structure of an affine space $EG(n,q)$ defined by a q-ary m-sequence of span n.

Let $Tr : GF(q^n) \to GF(q)$ be the trace function defined by $Tr(x) = x + x^q + ... + x^{q^{n-1}}$. It is well known that the sequence $R = (R_i)$, obtained by $R_i = Tr(\alpha^i)$, is a q-ary m-sequence of span n with period $q^n - 1$. Furthermore, one period of R has the form $R = (T, \beta T, ..., \beta^{q-2}T)$ where T is a q-ary vector of length $v = (q^n - 1)/(q - 1)$, and $\beta = \alpha^v$ is the corresponding primitive element of $GF(q)$[5]. The sequence R partitions the elements of $GF(q^n)^*$ into q subsets $H_a^*, a \in GF(q)$, where $H_a^* = \{\alpha^i : R_i = Tr(\alpha^i) = a\}$. If we consider $H_0 = H_0^* \cup \{0\}$ and $H_a = H_a^*$ for $a \neq 0$, then $\Pi = \{H_a : a \in GF(q)\}$ forms a parallel class of affine hyperplanes in $EG(n,q)$. In general, corresponding to every cyclic shift $E^kR, k = 0, 1, ..., v-1$, of R there is in $EG(n,q)$ a corresponding parallel class of hyperplanes $\Pi^{(k)}$ consisting of $H_a^{(k)} = \{\alpha^{i-k} : \alpha^i \in H_a\}, a \in GF(q)^*$, and $H_0^{(k)} = \{0\} \cup \{\alpha^{i-k} : \alpha^i \in H_0^*\}$. Thus all parallel classes of hyperplanes in $EG(n,q)$ can be obtained from R.

We define periodic binary sequences, which are indexed by the elements of $EG(n,q)\backslash\{0\}$, by considering the incidence vectors of subcollections of $\Pi^* = \{H_a : a \in GF(q)^*\}$. In particular, for $I \subseteq GF(q)^*$ and corresponding subcollection $\Sigma_I = \{H_a : a \in I\}$, the sequence $S(\Sigma_I)$ has period $q^n - 1$ and i^{th} term, corresponding to α^i given by

$$S_i = \begin{cases} 1, & \text{if } \alpha^i \in H_a \in \Sigma_I \\ 0, & \text{otherwise.} \end{cases}$$

Equivalently, if $\rho_I : GF(q) \to GF(2)$ is defined by

$$\rho_I(a) = \begin{cases} 1, & \text{if } \alpha \in I \\ 0, & \text{otherwise,} \end{cases}$$

then $S(\Sigma_I)$ has i^{th} term given by $S_i = \rho_I(R_i)$. Note that points in H_0 are always mapped to 0 in $GF(2)$. For simplicity of notation, we shall use Σ and ρ to denote Σ_I and ρ_I whenever I is understood. The purpose of this paper is to determine the linear span of $S(\Sigma_I)$.

Example 1: For $p = 3, n = 2$ and primitive polynomial $x^2 + x + 2$, the ternary m-sequence R of span 2 is given by

$$\begin{array}{rcccccccc} & \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ R = & (2 & 2 & 0 & 2 & 1 & 1 & 0 & 1) \end{array}$$

The parallel class of hyperplanes corresponding to R consists of

$$\begin{aligned} H_0 &= \{0, \alpha^2, \alpha^6\}, \\ H_1 &= \{\alpha^4, \alpha^5, \alpha^7\}, \\ H_2 &= \{\alpha^0, \alpha^1, \alpha^3\}. \end{aligned}$$

For $I = \{1, 2\}, S(\Sigma_I) = (01110111)$ has linear span 4. For $I = \{1\}, S(\Sigma_I) = (01000011)$ has linear span 8.

4. UPPER BOUND ON THE LINEAR SPAN OF SEQUENCES FROM FINITE GEOMETRIES.

For fixed $n \geq 1, R = (R_0, R_1, ..., R_{q^n-2})$ will denote an m-sequence of span n over $GF(q)$. For any collection Σ of hyperplanes obtained from R, $S(\Sigma) = (S_0, S_1, ..., S_{q^n-2})$ will denote a binary sequence determined by Σ; i.e., $S_i = 1$ if $\alpha^i \in H_a \in \Sigma$ and $S_i = 0$ otherwise. Although the sequence $S(\Sigma)$ depends on the choice of primitive polynomial, the results concerning its linear span will not. This is because any sequence obtained using a different primitive polynomial is related to $S(\Sigma)$ by a decimation by a value relatively prime to the period.

We introduce an array operator A which takes any sequence X of period $q^n - 1$ and arranges it into the $(q-1)$ by v array:

$$A(X) = \begin{pmatrix} X_0 & X_1 & \ldots & X_{v-1} \\ X_v & X_{v+1} & \ldots & X_{2v-1} \\ \vdots & \vdots & \ddots & \vdots \\ X_{(q-2)v} & X_{(q-2)v+1} & \ldots & X_{(q-1)v-1} \end{pmatrix}.$$

When applied to R, this operator produces the array $A(R)$ with column i of the form $(R_i, \beta R_i, ..., \beta^{q-2} R_i) = R_i(1, \beta, ..., \beta^{q-2})$. The sequence $(1, \beta, \beta^2, ..., \beta^{q-2})$ is a q-ary m-sequence of span 1 and will be denoted by $r = (r_0, r_1, ..., r_{q-2})$. A binary sequence $s(\Sigma)$ of period $q - 1$ is obtained by applying ρ to each term of r, where ρ is the mapping from $GF(q)$ to $GF(2)$ determined by Σ. The main result of this paper is that the linear span $L(S(\Sigma))$ of $S(\Sigma)$ is given by $vL(s(\Sigma))$. The value of $L(s(\Sigma))$ is relatively easy to compute.

If $R_i = 0$, then column i of $A(R)$ is the zero sequence 0. Otherwise $R_i = \beta^{e_i}$ for some $e_i \in \{0, 1, ..., q-2\}$ and column i is $E^{e_i} r$. In general, we define the ***shift sequence*** of R to be $e = (e_0, e_1, ..., e_{q^n-2})$ where $e_i = \infty$ if $R_i = 0$ or $R_i = \beta^{e_i}$ if $R_i \neq 0$. Likewise, the finite terms of $(e_0, e_1, ..., e_{q^n-2})$ give the shifts of the sequence $s(\Sigma)$ occurring as columns of the $(q-1)$ by v array $A(S(\Sigma))$. $A(S(\Sigma))$ contains columns of all zeros corresponding to the ∞ positions in $(e_0, e_1, ..., e_{v-1})$. By convention, we write $E^{\infty} s = 0$.

Example 2: For $p = 5$, $n = 3$ and primitive polynomial $x^3 + x^2 + 2$ the p-ary m-sequence R of span 3 is given in its array form as

$$A(R) = \begin{pmatrix} 0014120332224243340432042342201 \\ 0032310441112124420241021421103 \\ 0041430223331312210123013213304 \\ 0023240114443431130314034134402 \end{pmatrix}.$$

If $\Sigma = \{H_a : a \equiv 1 \pmod 2\}$ then

$$A(S(\Sigma)) = \begin{pmatrix} 0010100110000001100010000100001 \\ 0010110001110100000001001001101 \\ 0001010001111110010101011011100 \\ 0001000110001011110110010110000 \end{pmatrix},$$

$r = (1, 3, 4, 2), s(\Sigma) = (1, 1, 0, 0)$, and the first $v = 31$ terms of the shift sequence e are:

$$(\infty\infty0203\infty11333232112\infty213\infty231233\infty0).$$

Throughout, let $M(E)$ and $m(E)$ denote the minimal polynomials of $S(\Sigma)$ and $s(\Sigma)$, respectively. We shall use the notation S and s to denote the sequences $S(\Sigma)$ and $s(\Sigma)$ respectively whenever the collection Σ of hyperplanes is assumed. We begin to investigate the properties of $M(E)$ and $m(E)$, obtaining upper bounds on the linear spans of S and s. The *weight* $wt(X)$ of a binary sequence $X = (X_0, X_1, ..., X_{N-1})$ is the sum of any N consecutive terms of X. Thus, $((E^N + 1)/(E + 1))X = (E^{N-1} + E^{N-2} + ... + 1)X = (wt(X) \pmod 2)$.

LEMMA 1. *If Σ contains an odd number of hyperplanes, then $wt(S(\Sigma)) \equiv 1 \pmod 2$. If Σ contains an even number of hyperplanes, then $wt(S(\Sigma)) \equiv 0 \pmod 2$.*

PROOF.

$$wt(S) = |\Sigma|(\text{ number of elements in a hyperplane}).$$

Since each hyperplane in an affine space $EG(n, q)$ contains q^{n-1} elements and q is odd, $wt(S) \equiv |\Sigma| \pmod 2$, and the result follows. ∎

THEOREM 2. *If Σ contains an odd number of hyperplanes in $EG(n,q)$, then the highest power of $(E+1)$ that divides $(E^{q^n-1}+1)$ divides $M(E)$.*

PROOF. Since S has period q^n-1, $M(E)$ divides $(E^{q^n-1}+1)$. But,

$$((E^{q^n-1}+1)/(E+1))S = (wt(S) \pmod 2) = (1)$$

and so $M(E)$ does not divide $(E^{q^n-1}+1)/(E+1)$. The result follows. ▮

COROLLARY 3. *If Σ contains an odd number of hyperplanes, then*

$$(E+1)^2 | m(E).$$

PROOF. Apply the theorem to the case $n=1$, and note that since q is odd, $(E+1)^2|(E^{q-1}+1)$. ▮

Our next theorem establishes an upper bound on the linear span of the sequence S.

THEOREM 4. *$M(E)|m(E^v)$ so that $L(S(\Sigma)) \leq vL(s(\Sigma))$.*

PROOF. We show that if $m(E) = E^{j_1}+E^{j_2}+...+E^{j_k}$,where $j_1 = 0$, is the minimal polynomial of s, then $m(E^v)S = 0$. For $i \in \{0,1,...,q^n-2\}$,

$$\begin{aligned}(m(E^v)S)_i &= S_i + S_{i+j_2v} + ... + S_{i+j_kv}\\ &= (m(E)(S_i, S_{i+v}, ..., S_{i+(q-2)v}))_0.\end{aligned}$$

If $R_i = \beta^{e_i}$, then $(S_i, S_{i+v}, ..., S_{i+(q-2)v}) = E^{e_i}s$, and

$$(m(E^v)S)_i = (m(E)(E^{e_i}s))_0 = (E^{e_i}m(E)s)_0 = (E^{e_i}0)_0 = 0.$$

If $e_i = \infty$, then $(S_i, S_{i+v}, ..., S_{i+(q-2)v}) = 0$, and certainly $(m(E^v)S)_i = 0$. Thus, $m(E^v)S = 0$, so $M(E)|m(E^v)$ and $L(s) \leq$ degree $m(E^v) = v($degree $m(E)) = vL(s)$. ▮

Two questions naturally arise when determining the linear span of S:

(1) Is the bound in theorem 4 attained, that is, does $L(S) = vL(s)$?

(2) What is $L(s)$?

In the next section, we show that the answer to question 1 is always yes. Section 6 describes four particular choices of Σ and the respective values of $L(s)$.

5. LINEAR SPAN OF BINARY SEQUENCES OF FINITE GEOMETRIES.

In the previous section we established the upper bound $((q^n - 1)/(q - 1))L(s(\Sigma))$ on the linear span of the binary sequence $s(\Sigma)$ obtained from affine space $EG(n,q)$. Here, we show that this upper bound is always attained. In fact, we show that the minimal polynomial of $S(\Sigma)$ is $M(E) = m(E^v)$ where $m(E)$ is the minimal polynomial of $s(\Sigma)$.

First, we group the terms of $M(E)$ which have exponents congruent to the same value modulo v, and let $M(E)$ be expressed as follows:

$$M(E) = f_0(E^v) + f_1(E^v)E + \dots + f_{v-1}(E^v)E^{v-1}$$

where each $f_i(x)$ is a polynomial of degree d_i. The constant term 1 must appear in $M(E)$ and so $f_0(x) \neq 0$. We shall show that $f_i(x) = 0$ for all $i = 1, \dots, v-1$.

LEMMA 5. *If $f_0(E)s(\Sigma) = 0$, then $M(E) = m(E^v)$.*

PROOF.

$$\begin{aligned} f_0(E)s = 0 &\Rightarrow m(E)|f_0(E) \\ &\Rightarrow \text{degree } m(E) \leq \text{degree } f_0(E) \\ &\Rightarrow \text{degree } m(E^v) \leq \text{degree } f_0(E^v) \leq \text{degree } M(E) \end{aligned}$$

By theorem 4, $M(E)|m(E^v)$, so $M(E) = m(E^v)$. ∎

To show that the upper bound on theorem 4 is attained, we need to show that $f_0(E)s = 0$. Involved in the proof are properties of the shift sequence $e = (e_0, e_1, \dots, e_{q^n-2})$ introduced in section 4.

THEOREM 6. *Let $e = (e_0, e_1, \dots, e_{q^n-2})$ be the shift sequence associated with the primitive polynomial $f(x)$ which generates a q-ary m-sequence R of span n. Then any v consecutive terms of e contain exactly $(q^{n-1} - 1)/(q - 1)$ ∞ terms.*

PROOF. This is the number of zeros in any v consecutive terms of R. ∎

COROLLARY 7. *There are exactly q^{n-1} finite terms in $(e_0, e_1, \dots, e_{v-1})$.*

PROOF. $v - (q^{n-1} - 1)/(q - 1) = q^{n-1}$. ∎

In the following theorem, the elements $\{0, 1, \dots, q-2\}$ are identified with the elements of $Z(q-1)$, the integers modulo $q-1$. We use the convention that if $e_i \in Z(q-1)$, then $e_i - \infty = \infty - e_i = \infty$.

THEOREM 8. *Let e be the shift sequence associated with the primitive polynomial $f(x)$ which generates a q-ary m-sequence R of span n. For fixed $k \in \{1,2,...,v-1\}$, the list of differences $(e_{i+k} - e_i \mod (q-1) : i \in \{0,1,...,v-1\})$ contains each element of $\mathbb{Z}(q-1)$ exactly q^{n-2} times.*

PROOF. See [6, theorem 2, but with $m = 1$]. The results in [6] are stated for the case $q = 2$, however, the proofs remain valid for any prime power q. ▮

Recall that

$$M(E) = f_0(E^v) + f_1(E^v)E + ... + f_{v-1}(E^v)E^{v-1}.$$

The next lemma establishes a relationship between the polynomials $f_i(x)$ and the sequence s.

LEMMA 9. $f_0(E)s = (f_1(E) + f_2(E) + ... + f_{v-1}(E))(E^0 + E + ... + E^{q-2})s$.

PROOF. For a polynomial $f(E)$, applying $f(E^v)$ to S is equivalent to applying $f(E)$ to every v^{th} term of S, that is, applying $f(E)$ to columns of $A(S)$. Since the i^{th} column of $A(S)$ is $E^{e_i}s$, the i^{th} column of $A(f(E^v)S)$ is given by $f(E)E^{e_i}s$. Recall the convention that $E^{\infty}s = 0$.

Now, for each $k, 0 \leq k \leq v-1$, consider the sequence E^kS as represented by the array $A(E^kS)$. Every column i of the array now has a leading term S_{i+k}. Hence, every column i of the array $A(f_k(E^v)E^kS)$ is given by $f_k(E)E^{e_{i+k}}s$. Now, $M(E)S = 0$ implies that every column i in $A(M(E)S)$ is 0, that is, for $i \in \{0,1,...,v-1\}$,

$$(f_0(E)E^{e_i} + f_1(E)E^{e_{i+1}} + ... + f_{v-1}(E)E^{e_{i+v-1}})s = 0.$$

For every i, with $e_i \neq \infty$

$$E^{e_i}(f_0(E) + f_1(E)E^{e_{i+1}-e_i} + ... + f_{v-1}(E)E^{e_{i+v-1}-e_i})s = 0$$

if and only if

$$(f_0(E) + f_1(E)E^{e_{i+1}-e_i} + ... + f_{v-1}(E)E^{e_{i+v-1}-e_i})s = 0.$$

Summing over $i, 0 \leq i \leq v-1$, such that $e_i \neq \infty$, we have

$$(\sum_{e_i \neq \infty} f_0(E) + \sum_{e_i \neq \infty} (f_1(E)E^{e_{i+1}-e_i} + ... + f_{v-1}(E)E^{e_{i+v-1}-e_i}))s = 0.$$

By corollary 7, the first sum contains q^{n-1} terms, which is odd, thus

$$\sum_{e_i \neq \infty} f_0(E) \equiv f_0(E) \pmod 2.$$

By theorem 8 and since q^{n-2} is odd, for each $k \in \{1, 2, ..., v-1\}$,

$$\sum_{e_i \neq \infty} f_k(E) E^{e_{i+k}-e_i} \equiv f_k(E)(E^0 + E + ... + E^{q-2}) \pmod 2$$

where terms of the form $E^{\infty - e_i}$ are ignored because $E^{\infty - e_i} s = 0$. Combining the above observations, we have

$$f_0(E)s = (f_1(E) + f_2(E) + ... + f_{v-1}(E))(E^0 + E + ... + E^{q-2})s. \blacksquare$$

THEOREM 10. *$M(E) = m(E^v)$ and so $L(S(\Sigma)) = vL(s(\Sigma))$.*

PROOF. By lemma 5, it is enough to show that $f_0(E)s = 0$, and by lemma 9 this is equivalent to showing $(f_1(E) + ... + f_{v-1}(E))(E^0 + E + ... + E^{q-2})s = 0$.

If Σ consists of an even number of hyperplanes, then $wt(s) \equiv 0 \pmod 2$; hence

$$(E^0 + E + ... + E^{q-2})s = (wt(s) \pmod 2) = 0$$

and

$$f_0(E)s = 0.$$

If the number of hyperplanes in Σ is odd, then $wt(s) \equiv 1 \pmod 2$. By lemma 9,

$$\begin{aligned}(E+1)f_0(E)s &= (f_1(E) + f_2(E) + ... + f_{v-1}(E))(E+1)(wt(s) \pmod 2)) \\ &= (f_1(E) + f_2(E) + ... + f_{v-1}(E))0 \\ &= 0;\end{aligned}$$

that is, $m(E) | (E+1) f_0(E)$.

By corollary 3, $(E+1)^2 | m(E)$and so $(E+1) | f_0(E)$ and $f_0(E)$ has an even number of terms. Similarly, theorem 2 states that $(E+1) | M(E)$, so $M(E)$ has an even number of terms, and this number is given by the sum of the number of terms in $f_0(E)$ and the number of terms in $f_1(E) + f_2(E) + ... + f_{v-1}(E)$(before mod 2 cancellation). At any rate, this implies that $f_1(E) + f_2(E) + ... + f_{v-1}(E)$ has an even number of terms and $f_0(E)s = (f_1(E) + f_2(E) + ... + f_{v-1}(E))1 = 0$. $\blacksquare$

6. SPECIAL CASES OF BINARY SEQUENCES.

In this section we consider four particular choices of Σ, and analyze the linear span of each sequence.

If Σ consists of all nonzero hyperplanes, that is, $\Sigma = \Pi^{\star} = \{H_a : a \neq 0\}$, then the sequence $S(\Pi^{\star})$ has period v and corresponds to the anti-incidence vector of a hyperplane in an $(n-1)$-dimensional projective space $PG(n-1,q)$. In this case $s = (1)$ and has $L(s) = 1$, so theorem 10 states that the linear span of $S(\Pi^{\star})$ is v. It is easy to see that the linear spans of a binary sequence X and its complement $\bar{X}$ differ by at most one. Since $S(\Pi^{\star})$ has period v and $L(\bar{S}(\Pi^{\star}))$ must divide v, $L(\bar{S}(\Pi^{\star})) = L(S(\Pi^{\star})) = v$.

The complement of $S(\Pi^{\star})$ corresponds to the incidence vector of projective hyperplane in $PG(n-1,q)$. Projective codes with the incidence matrix of points and hyperplanes as parity check rules have been studied by coding theorists, and the rank of this incidence matrix over $GF(p)$, where $q = p^r$, has been obtained.

THEOREM 11 [7], [8], [9]. *For $q = p^r$, the $GF(p)$ rank of the incidence matrix of points and hyperplanes in $PG(n-1,q)$ is $1 + \binom{n-1+p-1}{p-1}^r$.*

Each row of the incidence matrix is a shift of the sequence $\bar{S}(\Pi^{\star})$. It is not hard to see that the rank of this incidence matrix over $GF(2)$ is precisely the linear span over $GF(2)$ of the sequence $\bar{S}(\Pi^{\star})$. In the case when $q = 2^r$, the linear span (over $GF(2)$) of a projective hyperplane sequence can be obtained from theorem 11. Combining these observations we have the following theorem.

THEOREM 12. *The linear span of a projective hyperplane sequence of $PG(n-1,q)$ is given by $(q^n - 1)/(q-1)$ if q is odd and $1 + n^r$ if $q = 2^r$.*

On the other hand, if Σ consists of only a single affine hyperplane H in $\Pi^{\star}$, then the sequence $S(H)$ corresponds to the incidence vector of an affine hyperplane and has period $q^n - 1$. The sequence $s(H)$ corresponds to a sequence of all 0's except one 1 and has full linear span $q-1$. Thus, by theorem 10, an affine hyperplane sequence of an affine space of odd order has full linear span. For affine spaces of even order results on the incidence matrix of points and hyperplanes of $EG(n,q)$ apply.

THEOREM 13 [7]. *For $q = p^r$, the $GF(p)$ rank of the incidence matrix of points and hyperplanes in $EG(n,q)$ is $\binom{n+p-1}{p-1}^r$.*

Combining these facts, we have the following theorem.

THEOREM 14. *The linear span of an affine hyperplane sequence of $EG(n,q)$ is given by (q^n-1) if q is odd and $(n+1)^r$ if $q=2^r$.*

If Σ consists of half of the hyperplanes in Π^*, say, $\Sigma = \{H_{\beta^i} : i = 0,1,\ldots,(q-3)/2\}$, then the sequence $s(\Sigma)$ is a binary sequence with $(q-1)/2$ ones followed by $(q-1)/2$ zeros, which has linear span $(q+1)/2$. Thus, by theorem 10, the sequence $s(\Sigma)$ has period q^n-1 and linear span $v(q+1)/2$.

More generally, we can consider choices of Σ with the first half of the sequence $s(\Sigma)$ the complement of the second half. The next lemma gives an upper bound on the linear span of $s(\Sigma)$.

LEMMA 15. *If Σ is chosen so that the first half of the sequence $s(\Sigma)$ is the complement of the second half of the sequence, then*

$$L(s(\Sigma)) \leq (q+1)/2.$$

PROOF. Let $d = (q-1)/2$ and consider the sequence $h = (E^d+1)s$. Since $s_i = s_{i+d}$ for all $i \in \{0,1,\ldots,(q-3)/2\}$, the sequence h consists of all 1's and $(E+1)h = 0$. Thus,

$$m(E) | (E^d+1)(E+1)$$

and

$$L(s) \leq 1 + (q-1)/2 = (q+1)/2. \quad \blacksquare$$

Finally, if q is an odd prime ($q = p$) and Σ consists of all the "odd hyperplanes," that is, $\Sigma = \{H_a : a \equiv 1 \pmod 2\}$, the sequence $S(\Sigma)$, called the *parity sequence* of order n, has period p^n-1 and linear span that depends on the linear span of the parity sequence $s(\Sigma)$ of order 1. For all $i \in \{0,1,\ldots,p-2\}$, $\beta^{i+(p-1)/2} = p - \beta^i$, and since p is odd, β^i and $\beta^{i+(p-1)/2}$ have different parities. Thus the parity sequence of order 1 has the property stated in lemma 15, and $L(s(\Sigma)) \leq (p+1)/2$.

For all but 14 primes less than 500, $L(s(\Sigma)) = (p+1)/2$, that is, usually $L(S(\Sigma)) = v(p+1)/2 = (p^n-1)/2 + (p^n-1)/(p-1)$. For instance the parity sequence in example 2 has linear span $(31)(3) = 93$. The 14 primes with $L(s(\Sigma)) < (p+1)/2$ are listed in table 1, together with the linear spans of the corresponding parity sequences of order 1. The determination of a closed form expression of the linear span of the parity sequences of order 1 is an interesting (and probably difficult) open problem.

TABLE 1

PRIMES < 500 WITH $L(s) < (p+1)/2$

p	$L(s)$	$(p+1)/2 - L(S)$
29	12	3
113	54	3
163	80	2
197	96	3
239	117	3
277	135	4
311	146	10
337	163	6
349	171	4
373	182	5
397	195	4
421	207	4
463	229	3
491	240	6

7. CONCLUSION.

We have presented general results on the linear spans of a class of binary sequences that are obtained from q-ary m-sequences (q odd) by mapping the elements of $GF(q)$ to 0 and 1. The linear span and minimal polynomial for these sequences are determined by considering a binary sequence of much shorter period $q-1$. The results imply that the binary sequences under consideration have linear spans that are comparable to their periods, which can be made very long.

ACKNOWLEDGEMENT

We would like to thank E.L. Key for introducing this problem area and for helpful and stimulating discussions.

REFERENCES

1. S.W. GOLOMB, "Shift Register Sequences," Aegean Park Press, Laguna Hills, 1982.
2. J.L. MASSEY, Shift-Register Synthesis and BCH Decoding, *IEEE Trans. Info Theory* **IT–15** (1969), 122–127.
3. E.L. KEY, An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators, *IEEE Trans. Info Theory* **IT–22** (1976), 732–736.
4. R. A. RUPPEL, "New Approaches to Stream Ciphers," Ph.D. Thesis, Swiss Federal Institute of Technology, 1984.
5. N. ZIELER, Linear Recurring Sequences, *J. Soc. Indust. Appl. Math.* **7** (1959), 31–48.
6. R. A. GAMES, Crosscorrelation of M-sequences and GMW-sequences with the same primitive polynomial, *Discrete Applied Math.* **12** (1985), 139–146.
7. J.M. GOETHALS AND P. DELSARTE, On a Class of Majority-logic Decodable Cyclic Codes, *IEEE Trans. Info Theory* **IT–14** (1968), 182–188.
8. F.J. MACWILLIAMS AND H.B. MANN, On the p-rank of the Design Matrix of a Difference Set, *Info. Control* **12** (1968), 474–488.
9. K.J.C SMITH, On the p-rank of the Incidence Matrix of Points and Hyperplanes in a Finite Projective Geometry, *J. Combinatorial Theory* **7** (1969), 122–129.