ACTA ARITHMETICA
LXI.2 (1992)

Generating linear spans over finite fields

by

Wun-Seng Chou (Taipei) and
Gary L. Mullen* (University Park, PA)

1. Introduction. In [1] Fitzgerald and Yucas defined the notion of an n-dimensional generating pattern over $\mathbb{F}_p$. In particular an n-tuple $(a_0, \ldots, a_{n-1})$ with $a_i \in \mathbb{F}_p$ was called an *n-dimensional generating pattern over* $\mathbb{F}_p$ if for every n-dimensional vector space V over $\mathbb{F}_p$ and every basis $v_1, \ldots, v_n$ of V, the recursive sequence $\{s_k\}$ defined by

$$s_k = \begin{cases} v_k & \text{if } k \le n\,, \\ \sum_{i=0}^{n-1} a_i s_{k-n+i} & \text{if } k > n\,, \end{cases} \tag{1}$$

consists of all nonzero elements of V for $k = 1, \ldots, p^n - 1$. Such generating patterns are of interest because they provide simple algorithms for generating the linear span of independent subsets of vector spaces over $\mathbb{F}_p$ (see [1] for details).

In this paper we generalize a number of the results from [1] by working over $\mathbb{F}_q$ where $\mathbb{F}_q$ is the finite field of order q and by showing that if $a_0 \ne 0$, $(a_0, \ldots, a_{n-1})$ is an n-dimensional generating pattern over $\mathbb{F}_q$ if and only if $f(x) = x^n - \sum_{i=0}^{n-1} a_i x^i$ is a primitive polynomial over $\mathbb{F}_q$. More generally, we show that the number of distinct elements generated by a linear recurring sequence is related to the order of its characteristic polynomial. For $q = p^n < 10^{50}$ with $p \le 97$, we indicate when one can find an optimal n-dimensional generating pattern over $\mathbb{F}_p$ with weight two, i.e. with two nonzero a_i's (in [1] the length is defined to be the number of nonzero a_i's but a more natural term is Hamming weight).

If V is an n-dimensional vector space over $\mathbb{F}_q$ then V is isomorphic to $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$. Consequently, instead of considering vectors in V as in [1], we may assume that the elements of the sequence are in $\mathbb{F}_{q^n}$. We will make this identification throughout the remainder of the paper.

* This author would like to thank the National Security Agency for partial support under grant agreement #MDA904-87-H-2023.

From (1) it is easily seen that the recursive sequence $\{s_k\}$ is really a linear recurring sequence. If n is a positive integer and $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_q$, a sequence $s_0, s_1, \ldots$ of elements of $\mathbb{F}_q$ satisfying the relation

$$s_{k+n} = a_{n-1}s_{k+n-1} + a_{n-2}s_{k+n-2} + \ldots + a_0 s_k \quad \text{for } k = 0, 1, \ldots \tag{2}$$

is called a *linear recurring sequence* in $\mathbb{F}_q$. The vectors

$$S_i = (s_i, s_{i+1}, \ldots, s_{i+n-1}), \quad i = 0, 1, \ldots,$$

are called the *i-th state vectors*. If $a_0 \neq 0$ in (2) then the sequence $\{s_k\}$ is periodic (see [3, Thm. 8.11]). The polynomial $f(x) = x^n - \sum_{i=0}^{n-1} a_i x^i$ is a characteristic polynomial for the sequence $\{s_k\}$ defined by (2). Hence we note that if $s_0, s_1, \ldots, s_{n-1}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and f is a monic polynomial of degree n with $f(0) \neq 0$, then f corresponds to an n-dimensional generating pattern if and only if the linear recurring sequence with initial state vector $S_0 = (s_0, \ldots, s_{n-1})$ and characteristic polynomial $f(x)$ is uniformly distributed over $\mathbb{F}_{q^n}^*$.

Let

$$A = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & 0 & \ldots & 0 & a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & a_{n-1} \end{pmatrix} \tag{3}$$

be the companion matrix of $f(x)$. Then we have $S_k = S_0 A^k$, for $k \geq 0$. Moreover, if $a_0 \neq 0$ and $s_0, s_1, \ldots, s_{n-1}$ are linearly independent over $\mathbb{F}_q$ then for any k, $s_k, s_{k+1}, \ldots, s_{k+n-1}$ is a basis since A is nonsingular. We also note that if $a_0 = 0$ then the sequence is ultimately periodic with a preperiod of length h where $f(x) = x^h g(x)$ with $g(0) \neq 0$. We shall hence consider only linear recurring sequences for which $a_0 \neq 0$. For further details and many other properties of linear recurring sequences over $\mathbb{F}_q$, see [3, Ch. 8].

If $f(x)$ is a polynomial over $\mathbb{F}_q$ with $f(0) \neq 0$ then the *order* of f, denoted by $\mathrm{ord}(f)$, is the least positive integer e for which $f(x)$ divides $x^e - 1$. We note that if f is irreducible of degree n over $\mathbb{F}_q$ then $\mathrm{ord}(f)$ divides $q^n - 1$ (see [3, Cor. 3.4]). If f is reducible, such a result does not hold in general but Theorems 3.8 and 3.11 of [3] provide a method for the calculation of orders. For numerous other details concerning polynomials and their orders over $\mathbb{F}_q$, see [3, Ch. 3, Sec. 1].

2. Basic properties. The following result generalizes Proposition 1 of [1].

THEOREM 2.1. *Let $f(x) = x^n - \sum_{i=0}^{n-1} a_i x^i$ with $a_0 \neq 0$ be a polynomial of degree n over $\mathbb{F}_q$. Let $s_0, s_1, \ldots, s_{n-1} \in \mathbb{F}_{q^n}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

Let $s_0, s_1, \ldots$ be the linear recurring sequence with initial state vector $S_0 = (s_0, s_1, \ldots, s_{n-1})$ and characteristic polynomial $f(x)$. If $\mathrm{ord}(f) = e$ then the elements $s_0, s_1, \ldots, s_{e-1}$ are distinct and the least period of this sequence is e.

P r o o f. If A is the companion matrix of $f(x)$ from (3) then $S_i = S_0 A^i$ for $i \geq 0$ and $\{s_i, s_{i+1}, \ldots, s_{i+n-1}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let t be the smallest positive integer so that $s_t = s_i$ for some $0 \leq i \leq t-1$. We note that $n \leq t \leq e$ and without loss of generality, we can assume $s_t = s_0$ for otherwise, if $s_t = s_i$ we may consider the sequence $s_i, s_{i+1}, \ldots$ Now $S_t = S_0 A^t$ and since $\{s_0, s_1, \ldots, s_{n-1}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $A \in \mathrm{GL}(n, q)$, the general linear group of all nonsingular $n \times n$ matrices over $\mathbb{F}_q$, the first column of A^t has entry 1 in the (1, 1) position and 0 elsewhere.

Note that $A^{2t} = A^t A^t$ also has first column of the form $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.

Let $1 \leq k \leq n-1$. From the definition of A, it is easy to see that the $(k+1)$-st columns of both A^{t-k} and A^{2t-k} are of the form $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.

Let $A^t = (a_{ij})$ for $1 \leq i, j \leq n$. Since $A^{2t-k} = A^{t-k} A^t$,

$$A^{t-k} \begin{pmatrix} a_{1,k+1} \\ \vdots \\ a_{n,k+1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Let B be the $(n-1) \times (n-1)$ matrix obtained from A^{t-k} by deleting the first row and $(k+1)$-st column. Then we have

$$B \begin{pmatrix} a_{1,k+1} \\ \vdots \\ a_{k,k+1} \\ a_{k+2,k+1} \\ \vdots \\ a_{n,k+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \\ \vdots \\ \\ 0 \end{pmatrix}.$$

Since A^{t-k} is nonsingular, B is nonsingular and so $a_{i,k+1} = 0$ for $i \neq k+1$.

Hence

$$A^{t-k}\begin{pmatrix}0\\ \vdots\\ a_{k+1,k+1}\\ 0\\ \vdots\\ 0\end{pmatrix}=\begin{pmatrix}1\\ 0\\ \vdots\\ 0\end{pmatrix}.$$

Since the first row of A^{t-k} has entry 1 at the $(k+1)$-st place, we have $a_{k+1,k+1}=1$. Hence for $1\le k\le n-1$,

$$a_{i,k+1}=\begin{cases}1 & \text{if } i=k+1,\\ 0 & \text{otherwise.}\end{cases}$$

Combining this with the fact that A^t has first column of the form $\begin{pmatrix}1\\ 0\\ \vdots\\ 0\end{pmatrix}$, we have $A^t=I_n$, the $n\times n$ identity matrix.

Since the order of $A\in \mathrm{GL}(n,q)$ is equal to $\mathrm{ord}(f)=e$, we have $e\,|\,t$ but since $n\le t\le e$, we have $t=e$. Thus $s_0,s_1,\ldots,s_{e-1}$ are distinct and so the least period of this sequence is e since $S_e=S_0A^e=S_0I_n=S_0$.

The following corollary generalizes Proposition 1 of [1].

Corollary 2.2. *Let $s_0,s_1,\ldots,s_{n-1}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The monic polynomial $f(x)$ of degree n over $\mathbb{F}_q$ with $f(0)\ne 0$ corresponds to an n-dimensional generating pattern if and only if $f(x)$ is a primitive polynomial.*

Proof. If $f(x)$ is a primitive polynomial then $\mathrm{ord}(f)=q^n-1$. It follows from the theorem that the linear recurring sequence with initial state vector $(s_0,s_1,\ldots,s_{n-1})$ and characteristic polynomial $f(x)$ has period q^n-1 and $s_0,s_1,\ldots,s_{q^n-2}$ are distinct so $f(x)$ corresponds to an n-dimensional generating pattern.

Conversely, if $f(x)$ corresponds to an n-dimensional generating pattern, the linear recurring sequence with initial vector $(s_0,s_1,\ldots,s_{n-1})$ and characteristic polynomial $f(x)$ has least period q^n-1. Since f is monic and $f(0)\ne 0$, f is primitive by [3, Thm. 3.16].

Since the number of primitive polynomials of degree n over $\mathbb{F}_q$ is known to be $\phi(q^n-1)/n$ where ϕ is Euler's function (see [3, Thm. 3.5]), we have

Corollary 2.3. *The number of distinct n-dimensional generating patterns $(a_0,\ldots,a_{n-1})$ over $\mathbb{F}_q$ with $a_0\ne 0$ is $\phi(q^n-1)/n$.*

Theorem 2.1 explains why the 5-tuple $(1,1,0,0,0)$ over $\mathbb{F}_2$ from [1, p. 55] is not a 5-dimensional generating pattern over $\mathbb{F}_2$ but instead the corresponding sequence has exactly 21 distinct elements. We have $x^5+x+1=(x^2+x+1)(x^3+x^2+1)$ and the order is $3\cdot 7=21$ corresponding to the 21 distinct elements.

3. A more general setting. In this section we relax the condition that the initial state vector $S_0=(s_0,s_1,\ldots,s_{n-1})$ consists of a basis and instead assume that the subspace of $\mathbb{F}_{q^n}$ generated by $s_0,s_1,\ldots,s_{n-1}$ has dimension $m\le n$. Our first result is

THEOREM 3.1. *Let $f(x)=x^n-\sum_{i=0}^{n-1}a_ix^i$ be a monic polynomial of degree n over $\mathbb{F}_q$ with $f(0)\neq 0$. Assume that the subspace generated by $s_0,s_1,\ldots,s_{n-1}$ has dimension $0<m\le n$. Consider the linear recurring sequence which has initial state vector $S_0=(s_0,s_1,\ldots,s_{n-1})$ and characteristic polynomial f. Let N be the number of distinct elements in the sequence. Then $N\le\min\{q^m,\operatorname{ord}(f)\}$.*

Proof. From [3, Thm. 8.27] the least period of the sequence is at most $\operatorname{ord}(f)$ and so $N\le\operatorname{ord}(f)$. We will show that the subspace V_k of $\mathbb{F}_{q^n}$ generated by $s_k,s_{k+1},\ldots,s_{k+n-1}$ is the same as the subspace V_{k+1} generated by $s_{k+1},s_{k+2},\ldots,s_{k+n}$. Since s_{k+n} is a linear combination of $s_k,\ldots,s_{k+n-1}$, we have $V_{k+1}\subseteq V_k$. Let T be the subspace of $\mathbb{F}_{q^n}$ generated by $s_{k+1},\ldots,s_{k+n-1}$ over $\mathbb{F}_q$. If $T=V_k$ then $s_k\in T$ and so $s_{k+n}\in T$ and thus $V_{k+1}=T=V_k$. If $T\neq V_k$ then $s_k\notin T$. Since $a_0\neq 0$ and $s_{k+n}=a_{n-1}s_{k+n-1}+\ldots+a_0s_k$, $s_k\notin T$ implies $s_{k+n}\notin T$. Hence $T\subsetneq V_{k+1}$, $\dim V_{k+1}=1+\dim T=\dim V_k$. But $V_{k+1}\subseteq V_k$ and so $V_{k+1}=V_k$.

We have shown that for any k, $V_k=V_0$, the subspace generated by $s_0,s_1,\ldots,s_{n-1}$. Every element of the sequence is in V_0 so that $N\le q^m$. Since $N\le\operatorname{ord}(f)$ we have $N\le\min\{q^m,\operatorname{ord}(f)\}$.

The following example shows that equality may not hold in Theorem 3.1. Let $f(x)=x^3+x+1$ be a polynomial over $\mathbb{F}_4$ so that f is irreducible and $\operatorname{ord}(f)=7$. Let $\alpha\in\mathbb{F}_{4^3}$, $\alpha\neq 0$ and set $s_0=\alpha$, $s_1=s_2=0$. Then the linear recurring sequence with initial state vector $(\alpha,0,0)$ and characteristic polynomial f consists of only two distinct elements and $2<\min\{4,7\}$.

We do note, however, that from Theorem 2.1 equality holds when $m=n$, i.e. when the initial state vector consists of a basis. We now consider another special case in which equality holds in Theorem 3.1.

THEOREM 3.2. *Let f be a primitive polynomial of degree n over $\mathbb{F}_q$. Let $s_0,s_1,\ldots,s_{n-1}\in\mathbb{F}_{q^n}$ and let $m<n$ be the largest number of linearly independent elements among $s_0,s_1,\ldots,s_{n-1}$. If N is the number of distinct elements in the linear recurring sequence with initial state vector $(s_0,s_1,\ldots,s_{n-1})$ and characteristic polynomial f, then $N=q^m$.*

Proof. If S denotes the sequence and its least period is r, then $r \mid \mathrm{ord}(f)$. Consider any basis $\{t_0, t_1, \ldots, t_{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let T be the linear recurring sequence with initial state vector $t_0, t_1, \ldots, t_{n-1}$ and characteristic polynomial f. Then T has least period $\mathrm{ord}(f) = q^n - 1$ and the elements $t_0, t_1, \ldots, t_{q^n-2}$ are distinct by Theorem 2.1. Hence $\{t_i \mid 0 \le i \le q^n - 2\} = \mathbb{F}_{q^n}^*$.

Let σ be the linear transformation of $\mathbb{F}_{q^n}$ into itself defined by $\sigma(t_i) = s_i$, $0 \le i \le n-1$. Let $\overline{T}$ be the sequence so that for each $i \ge 0$, the ith term $\bar{t}_i$ of $\overline{T}$ is $\bar{t}_i = \sigma(t_i)$. We will show that the sequences $\overline{T}$ and S are identical.

From the construction of $\overline{T}$, $\bar{t}_i = s_i$ for $0 \le i \le n-1$. Write

$$f(x) = x^n - \sum_{i=0}^{n-1} a_i x^i \,.$$

For any $k \ge 0$, $t_{k+n} = a_{n-1}t_{k+n-1} + \ldots + a_0 t_k$ so that for any $k \ge 0$

$$\begin{aligned}\bar{t}_{k+n} = \sigma(t_{k+n}) &= a_{n-1}\sigma(t_{k+n-1}) + \ldots + a_0\sigma(t_k) \\ &= a_{n-1}\bar{t}_{k+n-1} + \ldots + a_0\bar{t}_k \,.\end{aligned}$$

Hence f is a characteristic polynomial of $\overline{T}$. Since $\overline{T}$ and S have the same initial state vector and the same characteristic polynomial, $\overline{T}$ and S are identical.

We have shown that $s_i = \sigma(t_i)$ for $i \ge 0$. Since $\{t_i \mid 0 \le i \le q^n - 2\} = \mathbb{F}_{q^n}^*$, $\{s_i \mid 0 \le i \le q^n - 2\} = \sigma(\mathbb{F}_{q^n}^*)$. Since $\sigma(\mathbb{F}_{q^n}^*)$ is a subspace of $\mathbb{F}_{q^n}$ of dimension m over $\mathbb{F}_q, \{s_i \mid 0 \le i \le q^n - 2\}$ consists of exactly q^m distinct elements. This completes the proof.

Remark. We would like to thank Harald Niederreiter for the following argument which provides, in the $m = 1$ case, a sufficient condition in order that $N = q$. The condition is that $r\,\mathrm{ord}(f) > (q-1)^2 q^n$ where r is the least period length of the sequence. If $f(x)$ is the minimal polynomial of the sequence so that $r = \mathrm{ord}(f)$, the condition simplifies to $\mathrm{ord}(f) > (q-1)q^{n/2}$. By [3, Thm. 8.82] we have

$$\left|\mathbb{Z}(b) - \frac{r}{q}\right| \le \left(1 - \frac{1}{q}\right)\left(\frac{r}{\mathrm{ord}(f)}\right)^{1/2} q^{n/2} \,,$$

where $\mathbb{Z}(b)$ denotes the number of n with $0 \le n < r$, with $s_n = b$. Thus

$$\mathbb{Z}(b) \ge \frac{r}{q} - \left(1 - \frac{1}{q}\right)\left(\frac{r}{\mathrm{ord}(f)}\right)^{1/2} q^{n/2} > 0$$

for all $b \in \mathbb{F}_q$ so that every $b \in \mathbb{F}_q$ occurs in the sequence and hence $N = q$.

A periodic sequence is said to be *weakly equidistributed* in $\mathbb{F}_q$ if every element of $\mathbb{F}_q^*$ appears equally often in a period of the sequence. Since we can embed $\mathbb{F}_{q^k}$ as a subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if $k \le n$, then from the proof of

Theorem 3.2 each nonzero element of $\mathbb{F}_{q^k}$ appears exactly q^{n-k} times and so we may state

COROLLARY 3.3. *Let f be a primitive polynomial of degree n over $\mathbb{F}_q$. Let $s_0, s_1, \ldots, s_{n-1} \in \mathbb{F}_{q^k}$, where $1 \le k \le n$. Let $s_0, s_1, \ldots$ be the linear recurring sequence on $\mathbb{F}_{q^k}$ with initial state vector $(s_0, s_1, \ldots, s_{n-1})$ and characteristic polynomial $f(x)$. Then the sequence is weakly equidistributed on $\mathbb{F}_{q^k}$ if and only if the subspace of $\mathbb{F}_{q^k}$ generated by $s_0, s_1, \ldots, s_{n-1}$ over $\mathbb{F}_q$ equals $\mathbb{F}_{q^k}$, or equivalently, there are exactly k linearly independent elements over $\mathbb{F}_q$ among $s_0, s_1, \ldots, s_{n-1}$.*

The result of Corollary 3.3 is related to [4, Cor. 1]. We close this section with the following:

PROBLEM. Find an exact formula for the number N of distinct elements given in Theorem 3.1 where the elements of the initial state vector generate a subspace of dimension $m \le n$ and f is any monic polynomial of degree n over $\mathbb{F}_q$ with $f(0) \ne 0$.

4. An application. In [1], parts 2 and 3 of Corollary 2 are incorrectly stated. The modulus should be $p^n - 1$ rather than p^n. This error also occurs in the proof of Proposition 4 of [1]. For a corrected and generalized version over $\mathbb{F}_q$ we prove

COROLLARY 4.1. *Let $f(x) = x^n - \sum_{i=0}^{n-1} a_i x^i$ with $a_0 \ne 0$ be a polynomial of degree n over $\mathbb{F}_q$. Let $s_0, s_1, \ldots, s_{n-1} \in \mathbb{F}_{q^n}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $s_0, s_1, \ldots$ be the linear recurring sequence with initial state vector $S_0 = (s_0, s_1, \ldots, s_{n-1})$ and characteristic polynomial $f(x)$. Then for any k and j*

(1) *$s_k, s_{k+1}, \ldots, s_{k+n-1}$ is a basis of $\mathbb{F}_{q^n}$.*

(2) *$s_k = s_{k+j}$ if and only if $j \equiv 0 \pmod{\operatorname{ord}(f)}$.*

(3) *Let $f(x) = (f_1(x))^{e_1} \ldots (f_r(x))^{e_r}$ where $f_1(x), \ldots, f_r(x) \in \mathbb{F}_q[x]$ are irreducible and $e_1, \ldots, e_r \ge 1$. Then $\{s_j - s_k, s_{j+1} - s_{k+1}, \ldots, s_{j+n-1} - s_{k+n-1}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $j \not\equiv k \pmod{\operatorname{ord} f_i(x)}$ for all $1 \le i \le r$.*

Proof. Let A be the companion matrix of $f(x)$. Then (1) holds since $a_0 \ne 0$ and the companion matrix of f is nonsingular, (2) follows from Theorem 2.1, and for (3)

$$
\begin{aligned}
&(s_j - s_k, s_{j+1} - s_{k+1}, \ldots, s_{j+n-1} - s_{k+n-1}) \\
&\qquad = S_j - S_k = S_0 A^j - S_0 A^k = S_0 A^k (A^{j-k} - I)\,.
\end{aligned}
$$

So $\{s_j - s_k, s_{j+1} - s_{k+1}, \ldots, s_{j+n-1} - s_{k+n-1}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $A^{j-k} - I$ is nonsingular. The last statement is equivalent to that 1 is not an eigenvalue of A^{j-k}, or equivalently, $j \not\equiv k \pmod{\operatorname{ord} f_i(x)}$, for all $1 \le i \le r$.

Let $W \subseteq \mathbb{F}_{q^n}$. By an *m-spread* of W is meant a collection $\{U_i\}_{i=1}^k$ of m-dimensional subspaces of $\mathbb{F}_{q^n}$ satisfying $U_i \cap U_j = \{0\}$ for $i \neq j$ and $W = \bigcup U_i$. While we can consider W a subset of $\mathbb{F}_{q^n}$, we will restrict our attention to the case when W is a subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

THEOREM 4.2. *Let W be a subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ with $\dim W = k$. Let m be a positive integer. Then W has an m-spread if and only if $m \mid k$. Furthermore, if $m \mid k$, and if $\{w_1, \ldots, w_k\}$ is a basis of W over $\mathbb{F}_q$, then we can find an m-spread of W in the following way: Fix a primitive polynomial $f(x) \in \mathbb{F}_q[x]$ of degree m. Write $k = mh$ for some positive integer h. For $1 \leq i \leq h$, let $S_{i,j}$ be the j-th state vector of the linear recurring sequence which has characteristic polynomial $f(x)$ and initial state vector $S_{i,1} = (w_{(i-1)m+1}, \ldots, w_{im})$. Moreover, let $S_{i,0} = (0, \ldots, 0)$ for all $1 \leq i \leq h$. Then the collection of all subspaces of W spanned by all possible sums $S_{i,1} + S_{i-1,j_1} + \ldots + S_{1,j_{i-1}}$, where $1 \leq i \leq h$ and $0 \leq j_t \leq q^m - 1$ for each $1 \leq t \leq i-1$, is an m-spread of W.*

Proof. For necessity, we have $(q^m - 1) \mid (q^k - 1)$ from the definition of m-spread and so $m \mid k$. For sufficiency, we just need to prove the second assertion.

Take any two distinct vectors $S_{i,1} + S_{i-1,r_1} + \ldots + S_{1,r_{i-1}}$ and $S_{j,1} + S_{j-1,t_1} + \ldots + S_{1,t_{j-1}}$. Let U, V be subspaces of W spanned by these two vectors, respectively. If $i \neq j$, it is easy to see $U \cap V = \{0\}$. So, consider $i = j$. Let $a \in U \cap V$. There are two column vectors $B_1, B_2 \in \mathbb{F}_{q^m}$ so that $(S_{i,1} + S_{i-1,r_1} + \ldots + S_{1,r_{i-1}})B_1 = a = (S_{i,1} + S_{i-1,t_1} + \ldots + S_{1,t_{i-1}})B_2$. So, $S_{i,1}B_1 = S_{i,1}B_2$. Since all elements in $S_{i,1}$ are linearly independent we have $B_1 = B_2 = B$. Let c be the smallest integer so that $r_c \neq t_c$. Without loss of generality, let $r_c < t_c$. Since $0 \leq r_c < t_c \leq q^m - 1$ and $S_{c,0} = 0$, all elements in $S_{i-c,t_c} - S_{i-c,r_c}$ are linearly independent by Corollary 4.1(3). So,

$$\begin{aligned}(S_{i-c,t_c} - S_{i-c,r_c})B \\ = [(S_{i-c-1,r_{c+1}} - S_{i-c-1,t_{c+1}}) + \ldots + (S_{1,r_{i-1}} - S_{1,t_{i-1}})]B = 0\end{aligned}$$

implies that B is the zero vector. So $a = 0$ and thus $U \cap V = \{0\}$.

Note that there are exactly $q^{(h-1)m} + \ldots + q^m + 1$ vectors of the form $S_{i,1} + S_{i-1,j_1} + \ldots + S_{1,j_{i-1}}$. From the second paragraph, the total number of distinct elements in the union of subspaces of W spanned by all such vectors $S_{i,1} + S_{i-1,j_1} + \ldots + S_{i,j_{i-1}}$ is $(q^m - 1)(q^{(h-1)m} + \ldots + q^m + 1) + 1 = q^{hm} = q^k$.

Hence W is the union of all such subspaces. This completes the proof.

We note that the first assertion of our theorem was proved by induction for $\mathbb{F}_p$ by Fitzgerald and Yucas [1]. The first assertion is quite well known. We, however, give a constructive proof using the second assertion.

5. Optimal n-dimensional generating patterns. In [2] for each $p^n < 10^{50}$ with $p \leq 97$, Hansen and Mullen have obtained a primitive polynomial of degree n over $\mathbb{F}_p$. Moreover, the given polynomial has minimal weight, i.e. the minimal number of nonzero coefficients among all primitive polynomials of degree n over $\mathbb{F}_p$. From their tables, with the exception of 234 values of p^n in the above range, there is always a primitive trinomial of degree n over $\mathbb{F}_p$ and hence always an optimal n-dimensional generating pattern with weight two. Of the exceptions, 90 occur in the $p = 2$ case and 144 occur for odd p. Tables of primitive polynomials from [2] are available upon request from the second author.

References

[1] R. Fitzgerald and J. Yucas, *On generating linear spans over* GF(p), Congr. Numer. 69 (1989), 55–60.

[2] T. Hansen and G. L. Mullen, *Tables of primitive polynomials over finite fields*, Math. Comp., to appear.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Addison-Wesley (now distributed by Cambridge Univ. Press), 1983.

[4] H. Niederreiter and J.-S. Shiue, *Weak equidistribution of sequences in finite fields*, in: Contributions to General Algebra, B. G. Teubner, Stuttgart, 6 (1988), 203–212.

INSTITUTE OF MATHEMATICS
ACADEMIA SINICA
NANKANG, TAIPEI 11529
TAIWAN
REPUBLIC OF CHINA
E-mail: MACWS@TWNAS886.BITNET

MATHEMATICS DEPARTMENT
THE PENNSYLVANIA STATE UNIVERSITY
UNIVERSITY PARK, PENNSYLVANIA 16802
U.S.A.
E-mail: MULLEN@MATH.PSU.EDU

Received on 2.1.1991 (2108)