ACTA ARITHMETICA
LXV.3 (1993)

Values of linear recurring sequences of vectors over finite fields

by

GARY L. MULLEN (University Park, Penn.) and
IGOR SHPARLINSKI (Sydney, N.S.W.)

Consider the finite field $\mathbb{F}_q$ of $q = p^r$ elements where p is a prime, $r \geq 1$. For an n-tuple $(v_1, \ldots, v_n)$ of vectors

$$v_i = (v_{i,1}, \ldots, v_{i,n})^T$$

from the n-dimensional vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$ and a polynomial

$$f(x) = x^n - \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q[x]\,,$$

we consider the linear recurring sequence $S = \{s(k)\}$ defined by

$$s(k) = \begin{cases} v_k & \text{if } k \leq n\,, \\ \sum_{i=0}^{n-1} a_i s(k-n+i) & \text{if } k > n\,. \end{cases} \tag{1}$$

We note that the elements of the sequence S can be considered as elements of the field $\mathbb{F}_{q^n}$ which is an n-dimensional vector space over $\mathbb{F}_q$.

It is easy to see that without loss of generality we can suppose that $f(0) \neq 0$. Thus, it is possible to define the order of f, denoted by τ, as the least positive integer t for which $f(x)$ divides $x^t - 1$. It is known from [4] that the period of the sequence S does not exceed τ. For other details concerning polynomials and linear recurring sequence over $\mathbb{F}_q$, see [4].

In this paper we improve and generalize some results from the papers [1], [2], [6], [7] which are also devoted to studying the distribution of values of linear recurring sequences over finite fields. For some applications of such sequences see [1], [2].

It is easy to check that if $\alpha, \mu \in \mathbb{F}_{q^n}$ then for any fixed basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, the coordinate-vectors $\{c_k\}$ of the powers $\alpha\mu^k$, $k = 1, 2, \ldots$, satisfy such

The first author would like to thank the National Security Agency for partial support under grant agreement #MDA904-92-H-3044.

an equation corresponding to the minimal polynomial of α over $\mathbb{F}_q$. More generally, for an $n \times n$ matrix A and a vector $\mathbf{a}$ over $\mathbb{F}_q$ the sequence $\{\mathbf{a}A^k\}$ satisfies such an equation corresponding to the minimal polynomial of A over $\mathbb{F}_q$.

Thus, results on the distribution of values of such linear recurring sequences are related to the well-known discrete logarithm problem and to the orbit problem in finite fields (see [3] and [5] for background and references).

For an integer $P > 1$ denote by $V(P)$ the set of all possible values which occur among the first P elements $s_1, \ldots, s_P$ of the sequence S, and by V the set of all possible vectors which occur among elements of the sequence S. In [1], some sufficient conditions were stated under which such a sequence consists of all nonzero elements of $\mathbb{F}_q^n$, i.e. when $V = \mathbb{F}_q^n \backslash \{(0, \ldots, 0)\}$ (or $V = \mathbb{F}_{q^n}^*$ if we consider S as a sequence of elements of $\mathbb{F}_{q^n}$).

Denote by m the dimension of the vector space generated by the initial vectors $(v_1, \ldots, v_n)$. It has been shown in [1] that in this case

$$|V| \le \min\{q^m, \tau\},$$

where $|V|$ denotes the cardinality of the set V.

It is clear that the $n \times n$ matrix $(v_1, \ldots, v_n)$ contains $m \le n$ linearly independent rows which we denote by $w_i = (w_{i,1}, \ldots, w_{i,n})$, $i = 1, \ldots, m$. Thus we can define m linear recurring sequences $W_i = \{w_i(k)\}$ by

$$w_i(k) = \begin{cases} w_{i,k} & \text{if } k \le n, \\ \sum_{j=0}^{n-1} a_j w_i(k-n+j) & \text{if } k > n \end{cases}$$

(with the same characteristic polynomial $f(x)$) which are linearly independent over $\mathbb{F}_q$.

Note that the sequence of vectors $(w_1(k), \ldots, w_m(k))^T$, $k = 1, 2, \ldots$, is periodic with the minimal period T dividing τ. Moreover, if $f(x)$ is an irreducible polynomial then $T = \tau$.

Denote by $M_m(P)$ the number of different vectors which occur among

$$(w_1(k), \ldots, w_m(k))^T, \quad k = 1, \ldots, P,$$

so that $|V(P)| = M_m(P)$.

Let us set for brevity

$$M_m = M_m(\tau), \quad M(P) = M_1(P), \quad M = M(\tau).$$

Then it has been shown in Theorem 3.2 of [1] that if $f(x)$ is a primitive polynomial of degree n (i.e. $\tau = q^n - 1$) and $m < n$ then $M_m = q^m$. Furthermore, when $m = 1$ it has been noted in [1] that there is an asymptotic formula for the number of solutions of certain equations with a linear recurring sequence which enables the authors to prove that $M = q$ whenever $\tau > (q-1)q^{n/2}$.

Now we are going to show that the result of [6] for systems of equations with linear recurring sequences allows us to extend this result to any $m \ge 1$.

Set $t = \tau / \gcd(\tau, q-1)$.

THEOREM 1. *Let the dimension of the vector space generated by the initial vectors $(v_1, \ldots, v_n)$ be m and let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of order τ. Then there exists an absolute constant $C > 0$ such that if $P > C\, q^{m+(n-1)/2} \log \tau$ then $M_m(P) = M_m$.*

Proof. For $\theta_1, \ldots, \theta_m \in \mathbb{F}_q$ denote by $N_P(\theta_1, \ldots, \theta_m)$ the number of solutions of the system of equations

$$w_i(k) = \theta_i, \quad i = 1, \ldots, m,\ 1 \le k \le P\,.$$

It follows from [6] that

$$N_P(0, \ldots, 0) = P/q^m + O(q^{n/2-1} \log \tau) \tag{2}$$

for $P \le t$ and that

$$N_P(\theta_1, \ldots, \theta_m) = P/q^m + O(q^{(n-1)/2} \log \tau) \tag{3}$$

for $P \le \tau$, for any non-zero tuple $(\theta_1, \ldots, \theta_m)$, with absolute implied constants in the O-symbol (see Theorems 1 and 2 of [6], respectively). From (2) and (3) we get that

$$N_P(\theta_1, \ldots, \theta_m) = \frac{P}{\tau} N_\tau(\theta_1, \ldots, \theta_m) + O(q^{(n-1)/2} \log \tau)$$

for any P and any tuple $(\theta_1, \ldots, \theta_m)$.

It has been noted in [6] that in the cases $P = t$ and $P = \tau$ the logarithmic factor in the error terms of (2) and (3) respectively can be omitted. Thus, there is some absolute constant $C > 0$ such that if $t > Cq^{m+n/2-1}$ and $\tau > Cq^{m+(n-1)/2}$ then $M_m = q^m$. This result together with Theorem 1 allows us to easily formulate conditions under which $M_m(P) = q^m$. If we do not consider the zero tuple $(0, \ldots, 0)$, then similarly we get $M_m(P) \ge q^m - 1$ and $M_m \ge q^m - 1$ for $\tau \ge P > Cnq^{m+(n-1)/2} \log q$ and $\tau > Cnq^{m+(n-1)/2}$, respectively.

Moreover, it is an easy matter to explicitly compute constants in all of the above mentioned bounds (in fact, they are quite reasonable, about 1).

Since $t \ge \tau/q$ the condition $\tau > Cnq^{m+n/2}$ guarantees that $M_m = q^m$. This is a generalization (up to the constant C) of the above mentioned result concerning the case $m = 1$. An evident deficiency of Theorem 1 is that it can be utilized only if the period is sufficiently large.

The following results give other lower bounds for $M_m(P)$ that are nontrivial for any τ. First we get new lower bounds for the number $M(P)$. It is easy to prove that $M > \tau^{1/n}$ and $M(P) > (P-n)^{1/n}$ (see the proof of Theorem 3 below). We show that for fields $\mathbb{F}_q$ of small characteristic p this bound can be improved.

We need the following refinement of Theorem 1 of [7]:

$$M(P) \geq \min\left\{M, P\binom{n+p-2}{p-1}^{-l}\right\} \tag{4}$$

where l is the least integer with $M(P) \leq p^l$.

In order to obtain this result we can replace the trivial bound $M(P) \leq q = p^r$ in the proof of Theorem 1 of [7] with the inequality $M(P) \leq p^l$.

THEOREM 2. *We have the bound*

$$M(P) \geq \min\{M, p^{-1}P^{\log p/(\log p + p\log n)}\}\,.$$

Proof. It follows from (4) that $M(P) < M$ implies

$$P \leq M(P)\binom{n+p-2}{p-1}^{l} \leq M(P)n^{pl} = M(P)p^{lp\log n/\log p}$$
$$< (pM(P))^{p\log n/\log p + 1}$$

since, by definition, $p^{l-1} < M(P)$.

The next theorem generalizes the above result to the m-dimensional case.

THEOREM 3. *Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of order τ. Then we have the bounds*

$$M_m(P) \geq (P - n + m)^{1/(n-m+1)}$$

and

$$M_m(P) \geq \min\{\tau^{1/(n-m+1)}, p^{-1}P^{\log p/(\log p + p\log(n-m+1))}\}\,.$$

Proof. Let $\lambda_1, \ldots, \lambda_n$ be the roots of $f(x)$ (lying in $\mathbb{F}_{q^n}$). Then we have the representations

$$w_i(k) = \sum_{j=1}^{n} \alpha_{i,j}\lambda_j^k, \qquad i = 1, \ldots, m,\ k = 1, 2, \ldots,$$

for some $\alpha_{i,j} \in \mathbb{F}_{q^n}, i = 1, \ldots, m,\ j = 1, \ldots, n$.

Let $\beta_1, \ldots, \beta_m \in \mathbb{F}_{q^n}$ be any nonzero solution of the following system of $m-1$ linear homogeneous equations

$$\sum_{i=1}^{m} \alpha_{i,j}\beta_i = 0, \qquad j = n-m+2, \ldots, n\,.$$

Define the sequence

$$\omega(k) = \sum_{i=1}^{m} \beta_i w_i(k)\,.$$

Then for some γ_j, $j = 1, \ldots, n-m+1$, we have

$$\omega(k) = \sum_{j=1}^{n-m+1} \gamma_j \lambda_j^k, \qquad k = 1, 2, \ldots$$

It is evident that the sequences W_i, $i = 1, \ldots, m$ are linearly independent over $\mathbb{F}_{q^n}$ as well. Thus $\Omega = \{\omega(k)\}$ is a nonzero linear recurring sequence of elements of the field $\mathbb{F}_{q^n}$ of order at most $n-m+1$. Now we are going to show that the period of the sequence Ω equals τ.

Since $f(x)$ is irreducible, the condition $f(x) \mid (x^\tau - 1)$ is equivalent to $\lambda_j^\tau - 1 = 0$, $j = 1, \ldots, n$, and moreover all of these equalities are equivalent. Therefore, if $\omega(k+T) = \omega(k)$, $k = 1, 2, \ldots$, and $\lambda_j^T - 1 \neq 0$, $j = 1, \ldots, n$ then we see that the system

$$\sum_{j=1}^{n-m+1} \psi_j \lambda_j^k = 0, \qquad k = 1, \ldots, n-m+1\,,$$

has a nonzero solution $\psi_j = \gamma_j(\lambda_j^T - 1)$, $j = 1, \ldots, n-m+1$, which is impossible.

Evidently, $M_m(P)$ is greater than or equal to the number of different values which occur among $\omega(1), \ldots, \omega(P)$. On the other hand, taking into account that Ω is a linear recurring sequence of order $n-m+1$ and of period τ, we conclude that for $P \le \tau$ all tuples

$$(\omega(k), \ldots, \omega(k+n-m)), \qquad k = 1, \ldots, P-n+m\,,$$

are pairwise different. Thus $M_m(P)^{n-m+1} \ge P$ and we obtain the first bound.

It is easy to note that for $P = \tau$ we could consider τ pairwise different tuples

$$(\omega(k), \ldots, \omega(k+n-m)), \qquad k = 1, \ldots, \tau\,,$$

rather than $\tau - n + m$. Then the sequence Ω takes at least $\tau^{1/(n-m+1)}$ different values. Hence

$$M_m \ge \tau^{1/(n-m+1)}\,,$$

and applying Theorem 2 we get the second bound.

The following theorem is a generalization and an improvement of Theorem 1 of [7]. It is nontrivial for all q but is especially effective when p is a fixed prime.

THEOREM 4. *For $P > (pM_m)^{p \log n/\log p+1}$ we have $M_m(P) = M_m$.*

P r o o f. Let $\theta_1, \ldots, \theta_m$ be a basis of the field $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Applying Theorem 2 to the linear recurring sequence

$$u(k) = \theta_1 w_1(k) + \ldots + \theta_m w_m(k), \qquad k = 1, 2, \ldots,$$

over $\mathbb{F}_{q^m}$ we get

$$M_m(P) \geq \min\{M_m, p^{-1} P^{\log p/(\log p + p\log n)}\},$$

and the result follows.

Since $M_m \leq q^m$ the statement of the theorem holds for

$$P > (pq)^{m(p\log n/\log p+1)}.$$

Thus, for p fixed, $M_m(P) = M_m$ for some $P = \exp(O(m\log q\log n))$. In particular, if m and q are fixed, then the number of vectors $(w_1(k), \ldots, w_m(k))$ that we need to compute in order to determine the set of all possible distinct values, is bounded by $n^{O(1)}$, i.e. the computation can be done in polynomial time.

In fact, when q is fixed, for an arbitrary m the number of vectors which we need to compute can be estimated by $\exp(O(\log M_m \log n))$ which is a quasi-polynomial function $\exp(\log^2 L)$ in the total size $L = L_i + L_o$ of the input $L_i = O(n)$ and of the output $L_o = O(mM_m)$. However, we do not know any upper bounds for M_m (excepting $M_m \leq q^m$).

Acknowledgement. We would like to thank the referee for several helpful comments.

References

[1] W.-S. Chou and G. L. Mullen, *Generating linear spans over finite fields*, Acta Arith. 61 (1992), 183–191.

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

[3] R. Kannan and R. J. Lipton, *Polynomial-time algorithm for the orbit problem*, J. Assoc. Comput. Mach. 33 (1986), 808–821.

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

[5] K. S. McCurley, *The discrete logarithm problem*, in: Cryptology and Computational Number Theory, C. Pomerance (ed.), Proc. Sympos. Appl. Math. 42, Amer. Math. Soc., 1990, 49–74.

[6] I. Shparlinski, *On the distribution of recurring sequences*, Problemy Peredachi Informatsii 25 (2) (1989), 46–53 (in Russian).

[7] —, *On the distribution of values of recurring sequences and the Bell numbers in finite fields*, European J. Combin. 12 (1991), 81–87.

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

SCHOOL OF MPCE
MACQUARIE UNIVERSITY
SYDNEY, NEW SOUTH WALES 2109
AUSTRALIA
E-mail: IGOR@MACADAM.MPCE.MQ.EDU.AU

Received on 10.9.1992
and in revised form on 15.4.1993 (2302)