ORBITS AND PERIODS FOR LINEAR ACTIONS ON $GF[2]^n$

S. A. Amitsur and E. Shamir

Institute of Mathematics
Hebrew University, Jerusalem

Preprint No. 11

1997/98

§0 Introduction[1]

Let A be a linear operator in the vector space $V = GF[2]^n$. The set $\{\alpha, A\alpha, A^2\alpha, \dots\}$ is the orbit of α under A. The period of α is the minimal m such that for some s_0 $A^{s+m} = A^s$ for all $s \geq s_0$.

Questions of periods and behavior of orbits were treated quite extensively in the context of "linear recurring sequences" [2,3]. Such sequences figure in various applications in Mathematics and Engineering (e.g. in coding theory), and implemented by shift-register circuits [2].

In the case of a linear recurring sequence, the operator is represented by the matrix

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ a_0 & a_1 & a_2 & \dots & a_{n-1} \end{bmatrix}.$$

Partially supported by the Edmund Landau Center for research in Mathematical Analysis and Related Areas, sponsored by the Minerva Foundation (Germany).

[1] The original manuscript was written circa 1963. The present version is minimally revised, in view of later publications. Extensive references are given in [3].

This is easily seen to be a canonical form of a *cyclic* linear transformation in V, for which the minimal polynomial is of degree $n = \dim V$.

In this note[1] we study the orbits of a cyclic linear transformation directly, without using a canonical form. The main result is a detailed structure of V with respect to orbits and periods, counting numbers of periods of various sizes and some related counts.

Realizations of general operators on $V = (GF[2])^n$ by circuits (and vice versa) are quite important in circuit design, verification and various uses of automata [1]. Operators on $(GF[2])^n$ represent "symbolically" any finite state transformation. The periods of orbits are relevant for many issues in automata application, such as re-initialization, synchronization, pseudo-random character of orbits. These applications motivated the original manuscript [1] and its restriction to the field $GF[2]$. However it is easy to see that results and proofs carry over to $GF[p]$ with obvious adjustments.

§1. Irreducible minimal polynomial

Let $f(x)$, the minimal polynomial of A, be an irreducible polynomial of degree $n = \dim V$.

Claim 1a. *There is a integer m dividing $2^n - 1$ such that all $0 \neq \alpha \in V$ have period of length m.*

Claim 1b. *Given m dividing $2^n - 1$, there are $\varphi(m)/n$ irreducible polynomials satisfying 1a, where $\varphi(m)$ is the number of integers m and relatively prime to m.*

Proof. Since f is irreducible, the set of polynomial in A

$$\{p(A) = p_0 + p_1 A + p_2 A^2 \dots\} \equiv \{p(x) \mod f(x)\}$$

is a finite extension field of degree n over $GF[2]$. Thus it is isomorphic to $GF[2^n]$. The non-zero elements in this field form a cyclic group of order $2^n - 1$. The powers $\{A^i\}$ form a cyclic subgroup of order m and clearly $m|(2^n - 1)$. Thus $A^m - 1 = 0$ and $(A^m - 1)\alpha = 0$ for all $\alpha \in V$.

Now let $\alpha \neq 0$ be such that $A^t\alpha = A^s\alpha$, $s < t$. Then $A^s(A^{t-s} - 1)\alpha = 0$. The elements $p(A)$ of the field are either 0 or non-singular, which is the case for the

powers of A. Thus $A^r = 1$ where $r = t - s$, and so $m|r$. This proves that the period of any $\alpha \neq 0$ is exactly m. Moreover already $A^m\alpha = \alpha$.

1b is ascribed by [3] to Pellet in 1870[4]. We outline the proof. Period m for x implies $x^m - 1 = 0$ in $GF[2^n]$. Each group of n primitive roots of $x^m - 1 = 0$ form the set of roots of an irreducible polynomial of degree n and period m. There are $\varphi(m)/n$ disjoint groups. (A primitive element is a cyclic generator of the group $GF[2^n] - 0$).

§2. Minimal polynomial - power of irreducible one

Let the minimal polynomial of A be $f(x) = g(x)^r$ where $\deg[g(x)] = k$, $g(x)$ irreducible and $n = k \cdot r$. Let m be the period (by claim 1a) of $g(x)$. As we know $x^m - 1 = h(x)g(x)$. Since m divides $x^m - 1$, it is odd an the m'th roots of unity - the solutions of $x^m - 1 = 0$ - are distinct. Hence g.c.d$[h(x), g(x)] = 1$.

Consider the descending scale of spaces

$$
\begin{aligned}
&V = V_0 \supset V_1 \supset V_2 \cdots \supset V_1 = 0 \quad \text{where} \\
&V_i = g(A)^i V = \{g(A)^i\alpha,\ \alpha \in V\}.
\end{aligned} \tag{2.1}
$$

Claim 2a. $\dim V_i/V_{i+1} = k$ *over* $GF[2]$*;* A *induced on this quotient has* $g(x)$ *as its minimal polynomial.*

Claim 2b.

$$
\begin{aligned}
&g(A)^i\alpha \in V_j \quad \textit{iff} \quad \alpha \in V_{i-j},\ 0 \leq j < i \leq r; \\
&\textit{if} \quad g(A)\alpha \notin V_i \quad \textit{then} \quad \alpha \notin V_{i-1}.
\end{aligned}
$$

Proof. We define also an ascending scale

$$V^i = \ker[g(A)^i] = \{\alpha \in V,\ g(A)^i\alpha = 0\};$$

we'll show $V^i = V_{r-i}$.

$$g(A)^r V = 0 \quad \textit{implies} \quad V^i \supseteq g(A)^{r-i}V = V_{r-i}, \tag{2.2}$$

however $g(A)^{r-1}V = V_{r-1} \neq 0$ since the minimal polynomial of A is $g(x)^r$. The space V^i is invariant under A and $g(A)V^i \subseteq V^{i-1}$, hence the action of A is well-defined on the quotient V^{i-1}/V^i, and the minimal polynomial of this action is

$g(A)$ (it clearly annihilates, and it is irreducible). Thus *if* $V^i \neq V^{i+1}$, the quotient-dimension is $\geqq k$, *else* (if equality holds)

$$g(A)^i\alpha = 0 \quad \textit{implies} \quad g(A)^{i-1}\alpha = 0;$$

using this for $\alpha = g(A)^{r-i}\beta$, it readily implies $g(A)^{r-1}\beta = 0$ for all $\beta \in V$, contrary to the definition of r.

Thus $V^{r-i} \supsetneqq V^i$, and now by induction $\dim V^i \geqq ik$. Since $V^r = V$ is of dimension $r \cdot k = n$, it must be that $\dim V^i = ik$ for all i. In a similar way, we prove $\dim V_{r-i} = ik$ and in view of the inclusion (2.2), $V_{r-i} = V^i$ and all the successive quotient are of dimension k. Now

$$g(A)^i\alpha \in V_i \quad \textit{iff} \quad g(A)^{i+r-j}\alpha = 0, \quad \textit{so} \quad \alpha \in V^{r-(j-i)} = V_{j-i}$$

as claimed in (2.1). The second claim follows easily.

Computation of the periods.

Let

$$(A^M - 1)\alpha = 0, \quad \alpha \in V_i - V_{i+1}.$$

Then in V_i/V_{i+1} the induced $\alpha \neq 0$ and $\bar{A}$ satisfies $(\bar{A}^M - 1)\bar{\alpha} = 0$. By claim 1a, m divides M.

Claim 2c. *Let* $t = \operatorname{argmin}_s[2^s \geqq r - i]$. *Then the period of* $\alpha \in V_i - V_{i+1}$ *is* $m2^t$.

The maximum period in $V - V_1$ is $m2^T$, where $2^T \geqq r$ (So between mr and $2mr$).

Proof.

$$\alpha = g(A)^i\alpha_0,\ \alpha_0 \in V_0 - V_1,\ 2^t + i \geq r > 2^{t-1} + i$$
$$A^{m2^t} = [1 + h(A)g(A)]^{2^t} = 1 + h(A)^{2^t}g(A)^{2^t}$$
$$(A^{m2^t} - 1)\alpha = h(A)^{2^t}g(A)^{2^t}g(A)^i\alpha_0 \in g(A)^{2^t+i}V \subseteq g(A)^rV = 0,$$

hence $A^{2^t m}\alpha = \alpha$.

For $\nu < m2^t$, let $\nu = m2^sN$, $s < t$, N odd. Then

$$A^\nu = (1 + h(A)g(A))^{2^sN} = (1 + h(A)^{2^s}g(A)^{2^s})^N$$
$$= 1 + \binom{N}{1}h(A)^{2^s}g(A)^{2^s} + Bg(A)^{2^s+1}.$$

If $(A^\nu - 1)\alpha = 0$, the sum of the last two terms will annihilate α

$$[C + Bg(A)]\beta = 0, \quad \beta = g(A)^{2^s}\alpha, \quad C = \binom{N}{1} h(A)^{2^s}.$$

The vector β is in $V_{i+2^s} - V_{i+2^s-1}$ by claim 2b and

$$C\beta = -Bg(A)\beta \in V_{i+1+2^s} \text{ (if } i + 2^s < r),$$

but $\binom{N}{1} = 1$ since N is odd and g.c.d$(h, g) = 1$ so $h(A)$ is a non-singular matrix in the quotient $V_{i+2^s} - V_{i+2^s-1}$ and so is $\binom{N}{1} h(A)^{2^s}$. So $\beta = -C^{-1}Bg(A)\beta \in V_{i+2^s-1}$, which is a contradiction. Thus the period cannot be less then $2^t m$.QED

Count. *For a fixed t, the number of orbits with period $2^t \cdot m$ is*

$$\sum_{r-2^t \leqq i < r-2^{t-1}} 2^{n-(i+1)k} \cdot (2^k - 1)/2^t m. \tag{2.3}$$

Indeed the first factor counts the size of the vector space V_{i+1} whose dimension is $n-(i+1)k$; note that each equivalence class in the quotient V_i/V_{i+1} also has this size, and $(2^k - 1)$ is the number of classes. Thus the counting formula follows from claim 2c. There are two extreme cases. For orbits of minimal period m ($t = 0$), $i = r - 1$ and their total number is $(2^k - 1)/m$. For orbits of maximum period $2^T m$, the number of orbits is obtained from (2.3) by setting $t = T$ and summing from $i = 0$ to $r - 2^{T-1} - 1$.

§3 A general minimal polynomial of degree n

$f(x) = \prod_{j=1}^{\ell} g_j x)^{r_j}$, g_j irreducible, of degree k_j and pairwise relatively prime. The space V decomposes into a direct sum $\sum_{\oplus} V_j$, with $\alpha = \sum \alpha_j$ correspondingly. A induces linear transformations on V_j with minimal polynomials $g_j(x)^{r_j}$ of degree $n_j = k_j \cdot r_j$. Moreover

$$A^q\alpha = \alpha \text{ iff } A^q\alpha_j = \alpha_j, \quad 1 \leq j \leq \ell.$$

So if $\alpha_j \neq 0$ its period is $2^{t_j} m_j$, t_i defined as in claim 2c, thus $2^{t_j} m_j$ divides the exponent q and the period of α is

$$m = \text{l.c.m.}(2^{t_j} m_j | 1 \leq j \leq \ell, \alpha_j \neq 0). \tag{3.1}$$

Conversely given a vector of partial periods as in (3.1), there is a vector $v \in V$ with the period m, namely $\alpha = \sum \alpha_j$ where $\alpha_j \in V_j$ has period $2^{t_j} m_j$ (if α_j is taken $\neq 0$). The number of such vectors is the product

$$\prod_{\substack{j \\ a_j \neq 0}} \sum_{r-2^{t_j} \leq i < r-2^{t_j-1}} 2^{n_j-(i+1)k_j}(2^{k_j}-1) = b$$

and the total number of orbits in this set is b/m.

References

[1] Booth, T.L. *Sequential Machines and Automata*, Theory. Wiley, New York 1968.

[2] Golumb, S.W. *Shift Register Sequences*, Holden-Day, San-Francisco, 1967.

[3] Lidle, R. and Niederreiter, H. *Finite Fields*, Encyclopedia of Mathematics and its Applications, Vol. 20, Addision Wesley, Reading Mass. 1983.

[4] Pellet, A.E. *Sur les function irreducibles...*, C.R. Acad. Sci. Paris **70**, 328–330, 1870.